



**HAL**  
open science

# Multimode Quantum Communications and Hybrid Cryptography

Francesco Mazzoncini

► **To cite this version:**

Francesco Mazzoncini. Multimode Quantum Communications and Hybrid Cryptography. Computer Science [cs]. Institut Polytechnique de Paris, 2024. English. NNT : 2024IPPAT018 . tel-04656723

**HAL Id: tel-04656723**

**<https://theses.hal.science/tel-04656723>**

Submitted on 22 Jul 2024

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

NNT : 2024IPPAT018

Thèse de doctorat



INSTITUT  
POLYTECHNIQUE  
DE PARIS



# Multimode Quantum Communications and Hybrid Cryptography

Thèse de doctorat de l'Institut Polytechnique de Paris  
préparée à Télécom Paris

École doctorale n°626 École doctorale de l'Institut Polytechnique de Paris (ED IP  
Paris)  
Spécialité de doctorat : Physique

Thèse présentée et soutenue à Palaiseau, le 18/06/2024, par

**FRANCESCO MAZZONCINI**

Composition du Jury :

|   |                         |
|---|-------------------------|
| Eleni Diamanti<br>Directrice de recherche CNRS, LIP6, Sorbonne Université                 | Présidente/Examinatrice |
| Norbert Lütkenhaus<br>Professeur, Institute for Quantum Computing, University of Waterloo | Rapporteur              |
| Renato Renner<br>Professeur, Institute for Theoretical Physics, ETH Zürich                | Rapporteur              |
| Hugo Defienne<br>Chargé de recherche CNRS, INSP, Sorbonne Université                      | Examineur               |
| Sophie Laplante<br>Professeure, IRIF, Université Paris Cité                               | Examinatrice            |
| Romain Alléaume<br>Professeur, Télécom Paris, Institut Polytechnique de Paris             | Directeur de thèse      |
| Sylvain Gigan<br>Professeur, Laboratoire Kastler-Brossel, Sorbonne Université             | Co-directeur de thèse   |



---

# ACKNOWLEDGMENTS

I would like to start by expressing my deepest gratitude to my two amazing supervisors, Romain and Sylvain. To Romain, thank you for allowing me the freedom to explore my own path while always being there when I needed guidance. Your support and trust have been invaluable throughout this journey. To Sylvain, your positivity and optimism have been a constant source of encouragement. When I joined the lab as a theoretician with zero hands-on experience, you celebrated every (often very small) achievement with me, making me believe in myself and my abilities. Thank you both for your incredible support.

I would also like to express my gratitude to my jury for carefully reading my thesis and providing valuable feedback on the future directions of my work. In particular, I would like to thank my examiners, Sophie and Hugo. Sophie, for her interest in my work from the very beginning, for welcoming me into her group at IRIF, and for introducing me to Balthazar, whom I also thank for our collaboration filled with math equations and discussions about French cinema. Hugo, for being an exceptional mentor at LKB and a truly fun, genuine person; seeing you smiling among the jury members made me feel much more relaxed during my defense.

I cannot believe how lucky I have been to be part of not just one, but two wonderful research groups: the Curiosity group at Télécom and the Comedia group at LKB. I want to thank you all for making my PhD experience so lovely: Adrian, Alexandra, Amol, Augustin, Bernhard, Caio, Cambyse, Clémence, Fei, Fernando, Filippo, Guilhelm, Hankun, Hao, Hilton, Jan, Jianqi, Julien, Lea, Lei, Lorenzo, Louis, Louisiane, Marco, Michal, Peter, Raj, Raphael, Shupeng, Sara, Tengfei, Thomas, Tristan, Vivek, Yoonseok, Yuan, Ziao and all those that I might forget to mention. Among these, a few people deserve special mention for their exceptional support and company. From Télécom, I want to thank my office mates and friends, Guillaume and Nilesh, for sharing all the ups and downs of the PhD journey with me, always with a smile. Then I cannot avoid mentioning Pierre: most of my French language skills are thanks to your inability to speak English after a few beers. From LKB, I must mention Baptiste and Malo, with whom I spent numerous hours trying to make our setup work. You managed to make even the usually boring procedure of realigning the setup **almost** fun. An extra mention goes to my fellow compatriot Gianni, for his unique way of offering crucial advice on my work while never stopping with the jokes. I forgive you for calling me Franco for most of my PhD.

Outside the office, some people truly made my four years in Paris unforgettable. I must highlight my roommate and dear friend Aviman, who promised to do the dishes if I mentioned him in my thesis. Beyond your impressive dishwashing skills, you have been an incredible

roommate and a wonderful friend. From the very beginning of my adventure in France, I want to extend a big thank you to the entire Kley crew at Palaiseau. Special shoutouts go to Carmine, Shivank, and Akhila for sharing this Parisian experience with me right from day one. Together, we faced a pandemic in the post-apocalyptic Plateau de Saclay, numerous strikes, and the infamous French administration. I also want to thank all my friends from the Cité Universitaire, and in particular, Giulia, Nupur, and Eric. Our time together, filled with delicious Italian and Indian dinners, movie nights, and karaoke sessions, has been truly unforgettable. Thanks for the laughter, the fun, and the fabulous memories!

Infine, voglio ringraziare la mia famiglia per essere sempre stati i fan più accaniti del mio lavoro e aver cercato di comprendere cosa volesse dire questo benedetto "quantum". Non ce l'avrei mai fatta senza di voi.

---

# RESUMÉ DE LA THÈSE EN FRANÇAIS

La cryptographie quantique a été définie comme une nouvelle forme de cryptographie qui ne reposerait sur aucune hypothèse de difficulté calculatoire [1]. Cependant, à mesure que le domaine progresse, et en particulier à mesure que la Quantum Key Distribution (QKD) atteint des niveaux élevés de maturité technologique, il semble qu'un équilibre critique peut être trouvé. D'une part, nous avons la quête du plus haut niveau de sécurité théorique. D'autre part, une seconde direction consisterait à optimiser la sécurité et la performance pour une utilisation dans le monde réel, tout en offrant un avantage par rapport à la cryptographie classique. Dans cette thèse, nous avons exploré de nouvelles voies vers cette seconde direction, c'est-à-dire l'application de la cryptographie quantique dans des contextes pratiques.

## Analyse de la vulnérabilité de la QKD

Notre première approche consiste à adapter une méthode traditionnelle d'analyse de vulnérabilité, connue sous le nom de Common Criteria, à la cryptographie quantique. Cette méthode fournit un cadre pour évaluer les caractéristiques de sécurité et les capacités des produits hardware et software de technologie de l'information. La principale idée de notre travail est d'évaluer, à l'aide d'un cadre standardisé, la faisabilité d'attaques possibles contre un dispositif QKD, de prioriser les attaques les plus dangereuses et d'aider à guider la conception et l'ingénierie des systèmes QKD vers les normes de sécurité les plus élevées possibles. La faisabilité d'une attaque est évaluée en utilisant une métrique déjà définie dans le cadre des Common Criteria pour les dispositifs classiques, appelée *attack potential*, qui vise à évaluer l'effort total nécessaire pour mener à bien une attaque contre les systèmes QKD.

En particulier, nous avons réalisé une évaluation de la vulnérabilité d'un dispositif de système Continuous-Variable Quantum Key Distribution (CV-QKD). En exploitant la réponse non linéaire du détecteur homodyne près de sa limite de détection, un adversaire, Eve, peut lancer une attaque contre les dispositifs CV-QKD appelée *saturation attack*. Elle consiste à biaiser l'estimation du bruit en induisant activement la saturation des détecteurs homodynes. Nous avons identifié deux stratégies différentes pour exploiter cette vulnérabilité. La première et la plus difficile est la stratégie d'attaque cohérente, où Eve renvoie un signal cohérent translaté pour induire la saturation du détecteur. Notre seconde stratégie d'attaque consiste en l'attaque par saturation incohérente, où nous dirigeons un laser additionnel vers le récepteur cohérent de Bob. La mise en œuvre de cette attaque est considérablement plus simple et constitue une menace sérieuse pour les systèmes CV-QKD.

L'introduction d'une méthodologie de notation des attaques dans le contexte de la QKD ouvre de nouvelles perspectives pour la conception de matériels cryptographiques quantiques: la recherche d'une haute sécurité théorique doit être équilibrée avec le besoin pratique de maintenir la complexité de mise en œuvre gérable et de réduire la présence de failles potentielles. Cette approche dialectique est susceptible de déclencher l'exploration de nouveaux compromis dans la conception des systèmes cryptographiques.

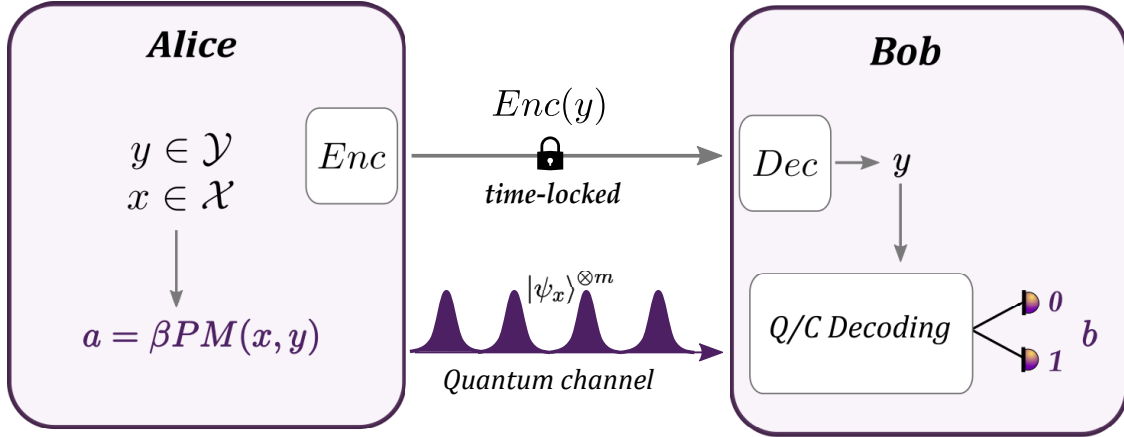
## Cryptographie hybride basée sur la complexité de communication

Dans la seconde approche, nous envisageons un modèle de sécurité hybride, nommé Quantum Computational Time-lock (QCT), où nous opérons sous l'hypothèse réaliste que le décryptage d'un chiffrement sécurisé par calcul nécessiterait une période bien supérieure au temps de cohérence des mémoires quantiques actuelles. En délaissant la quête du niveau de sécurité le plus élevé, nous pouvons alors proposer des protocoles de distribution de clés qui dépassent les benchmarks standard de la QKD. Ces protocoles offrent non seulement des taux de clés améliorés et une meilleure tolérance aux pertes, mais garantissent également une sécurité prouvée, selon les critères de sécurité standard de la QKD, face à des adversaires disposant d'une puissance de calcul infinie après la décohérence du stockage quantique, ce qui confère une *sécurité éternelle* [2]. Une direction spécifique explorée a été la construction de protocoles de distribution de clés basés sur des problèmes de complexité de communication quantique, pour lesquels il existe un gap exponentiel entre les stratégies classiques et quantiques. La complexité de communication est un cadre de communication général, impliquant deux parties, Alice et Bob, qui cherchent à calculer une fonction  $f(x, y)$  à partir de leurs entrées respectives  $x$  et  $y$ , en utilisant une communication classique ou quantique.

### Protocole HM-QCT

Nous introduisons une construction explicite pour un nouveau protocole de distribution de clés appelé Hidden Matching Quantum Computational Time-lock (HM-QCT). Il est basé sur le problème de complexité de communication unidirectionnelle  $\beta$ -Partial Matching ( $\beta$ PM) [3], pour lequel  $\Omega(\sqrt{n})$  bits de communication d'Alice à Bob sont nécessaires, contre seulement  $\mathcal{O}(\log(n))$  qubits, avec  $n$  la longueur de l'entrée  $x$ . Dans chaque round du protocole HM-QCT, Alice génère les deux entrées  $x$  et  $y$  et partage la seconde avec Bob en utilisant un schéma de chiffrement sécurisé à court terme. Alice et Bob peuvent alors résoudre le protocole  $\beta$ PM avec une stratégie quantique pour extraire un bit, en envoyant  $m$  copies du même état quantique de dimension  $n$ . Voir la Figure 1 pour une illustration graphique.

Enfin, en effectuant un post-traitement classique standard sur leur chaîne de bits, ils peuvent distiller une clé secrète. Nous prouvons sa sécurité contre un adversaire qui se comporte de manière indépendante et identique à chaque tour du protocole en établissant une réduction aux stratégies classiques pour ce problème de complexité de communication, reliant effectivement les domaines de la complexité de communication et de la cryptographie quantique. Ce que nous obtenons au final est un schéma de distribution de clés hybride avec les caractéristiques suivantes :



**Figure 1:** Un round du protocole HM-QCT.

- **Taux de clés boostés :** La sécurité peut être atteinte tout en envoyant jusqu'à  $\mathcal{O}\left(\frac{\sqrt{n}}{\log(n)}\right)$  photons par utilisation de canal, dépassant la limite standard d'un photon par utilisation de canal. Le protocole HM-QCT, basé sur le problème  $\beta PM$ , peut être mis en œuvre avec deux détecteurs de seuil monomode, et la performance peut donc être évaluée avec des protocoles à 2 modes de sortie. Le fait que la sécurité puisse être atteinte avec de nombreux photons par utilisation de canal conduit à des taux de clés secrètes asymptotiquement réalisables qui peuvent être augmentés d'un facteur  $\mathcal{O}\left(\frac{\sqrt{n}}{\log(n)}\right)$  par rapport à la QKD standard.
- **Fonctionnalités améliorées :** La possibilité d'atteindre constamment la capacité classique d'un bit par utilisation de canal sur des distances relativement courtes, un exploit inédit dans la QKD standard. De plus, plusieurs photons offrent non seulement une efficacité améliorée mais aussi la possibilité d'une distribution de clés en multicast avec jusqu'à  $\mathcal{O}\left(\frac{\sqrt{n}}{\log(n)}\right)$  Bobs autorisés simultanément.
- **Sécurité avec des "untrusted detectors" :** L'information d'un attaquant peut être limitée supérieurement en ne considérant que l'état que Alice introduit et ne nécessite pas (comme dans la QKD standard) d'information sur les résultats de mesure de Bob. Par conséquent, il n'est pas nécessaire de faire confiance à la mise en œuvre du dispositif de mesure de Bob.

## Plateforme expérimentale pour la complexité de la communication quantique

S'appuyant sur nos travaux théoriques concernant l'établissement de clés, notre dernier projet expérimental examine la faisabilité de démontrer un avantage quantique en complexité de communication. En particulier, nous exploitons le mélange de modes inhérent aux fibres multimodes en employant des techniques de *wavefront shaping* [4, 5], pour aborder les problèmes de complexité de la communication quantique. L'approche du wavefront shaping consiste à ajuster la phase et l'amplitude des ondes lumineuses pendant leur propagation, permettant ainsi le contrôle et la focalisation de la lumière à travers des milieux complexes, tels que les fibres optiques. Notre approche offre les avantages suivants :



- **Flexibilité** : Notre méthode permet la mise en œuvre de la phase de détection de Bob pour tout problème de complexité de communication quantique unidirectionnelle. Elle permet la construction d'opérateurs linéaires reconfigurables, autorisant une manipulation précise de l'amplitude et de la phase de chaque composante.
- **Scalabilité** : Contrairement aux conceptions de réseaux reconfigurables traditionnels qui dépendent d'interféromètres en cascade et subissent une augmentation quadratique des composants comme les diviseurs de faisceau et les déphaseurs avec la taille du circuit, notre méthode surmonte ces défis. En concevant simplement des fibres multimodes de plus grand diamètre, nous gagnons la capacité de contrôler davantage de modes physiques, nous permettant de configurer des réseaux optiques linéaires pouvant augmenter en taille.

Nous avons appliqué notre méthode à la partie de détection du protocole quantique  $\beta$ PM, évaluant son efficacité et discutant de la manière dont elle peut être mise à l'échelle pour des opérateurs linéaires plus importants en augmentant le nombre de modes pris en charge par la fibre. Finalement, nous avons remarqué que notre plateforme de détection reconfigurable est particulièrement efficace pour les problèmes nécessitant le codage d'un large éventail d'opérateurs linéaires quantiques. Ici, nous constatons que l'augmentation du nombre de modes contrôlables et la réduction du bruit externe pourraient potentiellement conduire à surpasser son équivalent classique.

---

# CONTENTS

|          |   |           |
|----------|---|-----------|
| <b>1</b> | <b>Introduction</b>                                       | <b>1</b>  |
| <b>I</b> | <b>Background</b>   | <b>13</b> |
| <b>2</b> | <b>Preliminaries</b>                                      | <b>15</b> |
| 2.1      | Introduction to quantum mechanics . . . . .               | 16        |
| 2.1.1    | Quantum states . . . . .                                  | 16        |
| 2.1.2    | Quantum measurements . . . . .                            | 18        |
| 2.1.3    | Quantum channels . . . . .                                | 19        |
| 2.1.4    | Distance measures among states and channels . . . . .     | 19        |
| 2.2      | Quantum continuous variables . . . . .                    | 20        |
| 2.2.1    | Canonical quantization . . . . .                          | 20        |
| 2.2.2    | Coherent states . . . . .                                 | 21        |
| 2.2.3    | Coherent detection . . . . .                              | 23        |
| 2.3      | Information theory . . . . .                              | 24        |
| 2.3.1    | Classical information theory . . . . .                    | 25        |
| 2.3.2    | Quantum information theory . . . . .                      | 26        |
| <b>3</b> | <b>Introduction to quantum key distribution</b>           | <b>29</b> |
| 3.1      | Modern cryptography . . . . .                             | 30        |
| 3.1.1    | Encryption schemes . . . . .                              | 30        |
| 3.1.2    | Basic principles in modern cryptography . . . . .         | 31        |
| 3.2      | General QKD protocol . . . . .                            | 32        |
| 3.2.1    | Structure of the protocol . . . . .                       | 33        |
| 3.2.2    | Foundational assumptions and trust requirements . . . . . | 34        |
| 3.3      | Explicit protocols . . . . .                              | 36        |
| 3.3.1    | Example 1: BB84 . . . . .                                 | 36        |
| 3.3.2    | Example 2: GG02 protocol . . . . .                        | 37        |
| 3.4      | Secure quantum key distribution . . . . .                 | 39        |
| 3.4.1    | Security definitions . . . . .                            | 39        |
| 3.4.2    | Security analysis . . . . .                               | 40        |
| 3.5      | Practical quantum key distribution . . . . .              | 43        |

|            |  |           |
|------------|--|-----------|
| 3.5.1      | Experimental implementations . . . . .                               | 43        |
| 3.5.2      | Quantum hacking . . . . .  | 44        |
| <b>II</b>  | <b>QKD vulnerability analysis</b>                                    | <b>47</b> |
| <b>4</b>   | <b>QKD attack rating</b>   | <b>49</b> |
| 4.1        | Introduction . . . . .   | 50        |
| 4.1.1      | Road to certified quantum infrastructures . . . . .                  | 50        |
| 4.1.2      | Attack rating methodology . . . . .                                  | 51        |
| 4.2        | CV-QKD vulnerability assessment against saturation attacks . . . . . | 53        |
| 4.2.1      | The saturation attack principle . . . . .                            | 54        |
| 4.2.2      | Attack implementation and rating . . . . .                           | 55        |
| 4.3        | Conclusion . . . . .   | 60        |
| <b>III</b> | <b>Hybrid quantum cryptography from communication complexity</b>     | <b>63</b> |
| <b>5</b>   | <b>From classical to quantum communication complexity</b>            | <b>65</b> |
| 5.1        | Communication Complexity . . . . .                                   | 66        |
| 5.1.1      | Deterministic protocols . . . . .                                    | 66        |
| 5.1.2      | Randomized protocols . . . . .                                       | 67        |
| 5.2        | Information Complexity . . . . .                                     | 70        |
| 5.2.1      | External and internal information . . . . .                          | 70        |
| 5.2.2      | Compression schemes in one-way setting . . . . .                     | 72        |
| 5.3        | Quantum Communication Complexity . . . . .                           | 74        |
| 5.3.1      | $\beta$ -Partial Matching Problem . . . . .                          | 74        |
| 5.3.2      | Vector in a Subspace Problem . . . . .                               | 77        |
| 5.3.3      | Comparison between the two problems . . . . .                        | 79        |
| <b>6</b>   | <b>Quantum cryptography against a bounded adversary</b>              | <b>81</b> |
| 6.1        | Introduction . . . . .   | 82        |
| 6.2        | Quantum data locking . . . . .                                       | 82        |
| 6.2.1      | General protocol . . . . .   | 82        |
| 6.2.2      | Security with accessible information . . . . .                       | 84        |
| 6.2.3      | Practical quantum data locking . . . . .                             | 85        |
| 6.3        | Noisy-storage model . . . . .  | 86        |
| 6.3.1      | Physical assumption . . . . .  | 86        |
| 6.3.2      | Quantifying adversarial information . . . . .                        | 86        |
| 6.4        | Quantum computational time-lock security model . . . . .             | 90        |
| 6.4.1      | Computational and physical assumptions . . . . .                     | 90        |
| 6.4.2      | Validity of QCT model . . . . .                                      | 91        |
| 6.4.3      | Rationale of the QCT model . . . . .                                 | 92        |
| 6.4.4      | Quantifying adversarial information . . . . .                        | 93        |

|          |   |            |
|----------|---|------------|
| 6.5      | Conclusion . . . . .  | 95         |
| <b>7</b> | <b>HM-QCT protocol</b>  | <b>97</b>  |
| 7.1      | Introduction . . . . .  | 98         |
| 7.2      | HM-QCT key distribution scheme . . . . .                                      | 99         |
| 7.2.1    | Protocol description . . . . .  | 99         |
| 7.2.2    | Achievable key rate in the i.i.d. setting . . . . .                           | 100        |
| 7.2.3    | Exploiting the complexity gap . . . . .                                       | 101        |
| 7.2.4    | Everlasting secure key expansion . . . . .                                    | 103        |
| 7.3      | Performance analysis and functionalities . . . . .                            | 103        |
| 7.3.1    | Key rate analysis . . . . .   | 103        |
| 7.3.2    | Multicast key distribution . . . . .  | 105        |
| 7.3.3    | Security with untrusted detectors . . . . .                                   | 106        |
| <b>8</b> | <b>Platform for one-way quantum communication complexity</b>                  | <b>109</b> |
| 8.1      | Introduction . . . . .  | 110        |
| 8.2      | Light propagation through disordered media . . . . .                          | 110        |
| 8.2.1    | Scattering theory . . . . .   | 110        |
| 8.2.2    | Multimode fibers as complex media . . . . .                                   | 111        |
| 8.2.3    | Introduction to wavefront shaping . . . . .                                   | 113        |
| 8.2.4    | Applications of wavefront shaping . . . . .                                   | 116        |
| 8.3      | Reconfigurable optical network for quantum communication complexity . . . . . | 119        |
| 8.3.1    | Experimental setup . . . . .  | 120        |
| 8.3.2    | Acquisition of transmission matrix . . . . .                                  | 121        |
| 8.3.3    | Construction of reconfigurable detection system . . . . .                     | 123        |
| 8.3.4    | Scalability and flexibility of the optical network . . . . .                  | 125        |
| 8.3.5    | Experimental analysis . . . . .   | 127        |
| 8.4      | Conclusion . . . . .  | 132        |
| <b>9</b> | <b>Perspectives</b>   | <b>133</b> |
| <b>A</b> | <b>Methods for saturation attacks</b>   | <b>137</b> |
| A.1      | Experimental setup . . . . .  | 138        |
| A.1.1    | Bob's homodyne detector . . . . .   | 138        |
| A.1.2    | Setup for incoherent attack strategy . . . . .                                | 139        |
| A.2      | Estimation of channel parameters . . . . .                                    | 140        |
| A.3      | Noise model and attack tuning . . . . .                                       | 140        |
| A.4      | Asymptotic secret key rate for GG02 . . . . .                                 | 141        |
| <b>B</b> | <b>One-way compression scheme</b>   | <b>143</b> |
| B.1      | Derivation of Theorem 5.2.1 . . . . .   | 143        |
| <b>C</b> | <b>Quantum Communication Complexity</b>                                       | <b>145</b> |
| C.1      | $\beta$ -Partial Matching problem . . . . .                                   | 146        |
| C.1.1    | Detection linear operator for quantum protocol . . . . .                      | 146        |
| C.1.2    | Derivation of Theorem 5.3.1 . . . . .   | 147        |

|          |   |            |
|----------|---|------------|
| C.1.3    | Best known classical protocol . . . . .                   | 148        |
| C.2      | Vector in a Subspace problem . . . . .                    | 150        |
| C.2.1    | Best known classical protocol . . . . .                   | 150        |
| C.3      | General practical quantum protocol . . . . .              | 154        |
| C.3.1    | QBER and $p_{\text{abort}}$ derivation . . . . .          | 154        |
| <b>D</b> | <b>Methods for reconfigurable optical linear operator</b> | <b>157</b> |
| D.1      | Input ports calibrations . . . . .                        | 158        |
| D.1.1    | Active zone of the SLM . . . . .                          | 158        |
| D.1.2    | Dividing the SLM in slices . . . . .                      | 158        |

---

# LIST OF FIGURES

|     |  |     |
|-----|--|-----|
| 1   | Un round du protocole HM-QCT. . . . .  | vii |
| 2.1 | Homodyne detection scheme. . . . .   | 24  |
| 3.1 | Hardware trust requirements for QKD protocols. . . . .   | 35  |
| 3.2 | BB84 illustration. . . . .   | 37  |
| 3.3 | Attack categories for QKD. . . . .   | 41  |
| 3.4 | Illustration of the detection of Eve's resent pulsed in the blinding attack. . . . .                               | 45  |
| 4.1 | Illustration of the space-ground integrated quantum network in China . . . . .                                     | 50  |
| 4.2 | Pictorial representation of how to characterize the linearity range of a homodyne detector. . . . .                | 54  |
| 4.3 | Scheme for saturation attack. . . . .  | 56  |
| 4.4 | Response of homodyne output due to displacement. . . . .   | 57  |
| 4.5 | Results of the incoherent attack. . . . .  | 58  |
| 4.6 | Schematic of both a coherent attack and an incoherent attack against a CV-QKD protocol. . . . .                    | 58  |
| 4.7 | Pictorial representation of the possible divergence between theoretical and practical QKD security. . . . .        | 61  |
| 5.1 | Illustration of an execution of a two-way deterministic protocol. . . . .  | 67  |
| 5.2 | Illustration of a set of perfect matchings for size $n = 4$ . . . . .  | 75  |
| 5.3 | Illustration of a possible implementation of Bob's decoding with $n = 6$ spatial modes and $\beta = 1/3$ . . . . . | 76  |
| 5.4 | Comparison between transmitted bits/qubits for classical and quantum upper bounds . . . . .                        | 80  |
| 6.1 | QDL protocol's circuit layout. . . . .   | 83  |
| 6.2 | General encoding attack. . . . .   | 87  |
| 6.3 | Overview of the assumptions in the QCT Model. . . . .  | 92  |
| 7.1 | One round of the HM-QCT protocol. . . . .  | 98  |
| 7.2 | Key rate comparison for the HM-QCT protocol. . . . .   | 104 |
| 7.3 | Key rate over short distances for the HM-QCT protocol. . . . .   | 105 |
| 7.4 | One round of the multicast HM-QCT protocol. . . . .  | 106 |

|      |   |     |
|------|---|-----|
| 7.5  | Comparison of hardware trust requirements between QCT and conventional trust models. . . . .  | 107 |
| 8.1  | Model of light scattering in a complex medium. . . . .  | 111 |
| 8.2  | Illustration of an optical fiber . . . . .  | 112 |
| 8.3  | Wavefront shaping with the optimization method. . . . .   | 115 |
| 8.4  | Illustration of a QSA. . . . .  | 117 |
| 8.5  | Secure data transmission over a MMF in the presence of an eavesdropper. . .   | 118 |
| 8.6  | Setup configuration to solve a one-way boolean quantum communication complexity problem. . . . .  | 120 |
| 8.7  | Pictorial representation of the construction of a $4 \times 4$ linear operator. . . . .   | 123 |
| 8.8  | Alice's methods to encode input vectors for a $4 \times 4$ linear operator. . . . .   | 124 |
| 8.9  | Numerical simulation for the visibility of $\beta$ PM and VS protocols. . . . .   | 126 |
| 8.10 | Plot of the transmitted number of qubits vs. the input size $n$ for solving the $\beta$ PM problem. . . . .                                   | 129 |
| 8.11 | Experimental transmission of a binary classical fingerprint image with $6 \cdot 10^3$ pixels solving the $\beta$ PM quantum protocol. . . . . | 131 |
| 8.12 | Plot of error probabilities of the experimental transmission of a binary classical fingerprint solving the $\beta$ PM problem. . . . .        | 131 |
| A.1  | Balanced homodyne detection at Bob's side. . . . .  | 138 |
| A.2  | Experimental setup for generating displaced coherent state. . . . .   | 139 |
| A.3  | Excess noise due to displacement in the saturation attack. . . . .  | 141 |
| C.1  | Error analysis for the best-known protocol of the $\beta$ PM problem. . . . .   | 150 |
| C.2  | Error analysis for the best-known protocol of the VS problem. . . . .   | 154 |
| D.1  | Analysis of the active zone of the SLM. . . . .   | 159 |
| D.2  | Illustration of the division of the SLM into $m = 4$ different ports. . . . .   | 159 |

---

# LIST OF TABLES

|     |   |     |
|-----|---|-----|
| 4.1 | Table for the evaluation of the Attack Potential used in the thesis. . . . .    | 52  |
| 4.2 | Semi-qualitative scale for attack rating. . . . .                               | 53  |
| 4.3 | Summary of the analysis on the two attacks to the homodyne detection. . . .     | 59  |
| 5.1 | Comparison of the lower and upper bounds of the VS and $\beta$ PM problems. . . | 79  |
| 6.1 | Comparison of cryptographic models: QDL, NSM, and QCT. . . . .                  | 95  |
| 8.1 | Comparison of different types of SLM technologies. . . . .                      | 114 |
| 8.2 | Summary of the efficiency parameters measured in the implementations. . . .     | 128 |





---

# LIST OF ACRONYMS

|            |   |
|------------|---|
| $\beta$ PM | $\beta$ -Partial Matching                               |
| AES        | Advanced Encryption Standard                            |
| AP         | Attack Potential  |
| BB84       | Bennet-Brassard-1984                                    |
| BQSM       | Bounded-Quantum-Storage Model                           |
| BS         | Beam Splitter   |
| CAC        | Classical Authenticated Channel                         |
| CP         | Complete Positive                                       |
| CPTP       | Complete Positive Trace Preserving                      |
| CV         | Continuous Variable                                     |
| CV-QKD     | Continuous-Variable Quantum Key Distribution            |
| DD-QKD     | Device-Dependent Quantum Key Distribution               |
| DI-QKD     | Device-Independent Quantum Key Distribution             |
| DMD        | Digital Micromirror Device                              |
| DMPK       | Dorokhov-Mello-Pereira-Kumar                            |
| DV-QKD     | Discrete-Variable Quantum Key Distribution              |
| EB         | Entangled-Based   |
| EMCCD      | Electron-Multiplying Charge-Coupled Device              |
| EPR        | Einstein-Podolsky-Rosen                                 |
| GG02       | Grosshans-Grangier-2002                                 |
| HM-QCT     | Hidden Matching Quantum Computational Time-lock         |
| IEC        | International Electrotechnical Commission               |
| ISG        | Industry Specification Group                            |
| ISO        | International Organization for Standardization          |
| IT         | Information Technology                                  |
| LO         | Local Oscillator  |
| MDI-QKD    | Measurement-Device-Independent Quantum Key Distribution |
| MEMS       | Micro Electro-Mechanical System                         |
| MMF        | MultiMode Fiber   |
| NA         | Numerical Aperture                                      |
| NSM        | Noisy-Storage Model                                     |
| PBS        | Polarization Beam Splitter                              |
| PLOB       | Pirandola-Laurenza-Ottaviani-Bianchi                    |

|        |   |
|--------|---|
| PLS    | <b>Physical Layer Security</b>                          |
| PM     | <b>Prepare and Measure</b>                              |
| PNS    | <b>Photon-Number-Splitting</b>                          |
| POVM   | <b>Positive Operator-Valued Measure</b>                 |
| POWF   | <b>Physical One-Way Function</b>                        |
| PQC    | <b>Post-Quantum Cryptography</b>                        |
| PUF    | <b>Physical Unclonable Function</b>                     |
| QBER   | <b>Quantum Bit Error Rate</b>                           |
| QCT    | <b>Quantum Computational Time-lock</b>                  |
| QDL    | <b>Quantum Data Locking</b>                             |
| QKD    | <b>Quantum Key Distribution</b>                         |
| QSA    | <b>Quantum-Secure Authentication</b>                    |
| RMT    | <b>Random Matrix Theory</b>                             |
| RNG    | <b>Random Number Generator</b>                          |
| RSA    | <b>Rivest-Shamir-Adleman</b>                            |
| SKC    | <b>Secret Key Capacity</b>                              |
| SLM    | <b>Spatial Light Modulator</b>                          |
| SNSPDs | <b>Superconducting Nanowire Single-Photon Detectors</b> |
| SVD    | <b>Singular Value Decomposition</b>                     |
| TF-QKD | <b>Twin-Field Quantum Key Distribution</b>              |
| TM     | <b>Transmission Matrix</b>                              |
| TOE    | <b>Target Of Evaluation</b>                             |
| VBS    | <b>Variable Beam Splitter</b>                           |
| VS     | <b>Vector in a Subspace</b>                             |

---

# INTRODUCTION

## Advent of quantum cryptography

The advent of quantum cryptography represents a paradigm shift in cryptography, the science and the art of secrets, as it promoted the idea that some cryptographic mechanisms could rely on the laws of quantum physics, and not on mathematical hardness assumptions. It can be traced back to the late 60s or early 70s, when a young graduate student Stephen Wiesner, then at Columbia University in New York, introduced the concept of "quantum conjugate coding" to his friend from their undergraduate days, Charles Bennett [6]. Wiesner's innovative proposal included the use of quantum states encoded into "conjugate observables," like linear and circular polarization of light, to create banknotes that couldn't be counterfeited. These early concepts, though initially overlooked by the academic world, eventually seeded the development of quantum cryptography.

A decade later, Charles Bennett together with Gilles Brassard, a cryptologist from the University of Montreal, proposed the very first Quantum Key Distribution (QKD) scheme based on Wiesner's conjugate observables [1]. At its core, QKD is a quantum-based primitive designed for the secure exchange of a secret—a key—between two parties. Its security is rooted solely in the fundamental principles of quantum mechanics, ensuring resilience against future technological advancements or discoveries. Right from the introduction of their seminal paper, Bennet and Brassard make it clear that their objective is to challenge classical cryptography, whose security relies on assumptions about the complexity of certain mathematical problems.

Meanwhile, during the historical Physics of Computation Conference of 1981 [7], Richard Feynman observed that classical computers fall short in effectively modeling the complex nature of quantum states involving numerous particles, and suggested the development of a new kind of computer based on the principle of quantum mechanics—a quantum computer. Then, in 1994, Peter Shor made another revolutionary discovery, showing that quantum computers could not only simulate quantum phenomena but also offer significant benefits in tackling classical computational problems [8]. He showed that problems like integer factorization and

the discrete logarithm problem, traditionally viewed as challenging for classical computers, could actually be solved efficiently in polynomial time with a quantum computer. Such a breakthrough inevitably limited the security of vastly used protocols like the Diffie–Hellman key exchange [9] and Rivest-Shamir-Adleman (RSA) encryption [10] and led cryptographers to ominously dub the advent of quantum computing as the "quantum cryptocalypse".

## Practical quantum-safe cryptography

With the potential rise of technologies like fault-tolerant quantum computers on the horizon [11–14], both the well-established classical cryptography community and the emergent quantum cryptography community were united in one belief: "we must act now before it's too late" [15]. As a matter of fact, classical communications can be fully cloned or copied, leaving the possibility for harvesting attacks (store now, attack later) as a generic vulnerability.

Two distinct paths, yet not quite mutually exclusive (as will be revealed later—a little spoiler), have been envisioned. On one side we have the deployment of quantum cryptography as a future-proof alternative, vigorously promoted by the quantum community. On the other side, advocated by the classical cryptography community, there is the idea of replacing the vulnerable cryptographic protocols with new protocols based on problems that would remain difficult to solve even for quantum computers [16]. This approach is known as Post-Quantum Cryptography (PQC).

Over the last three decades, the dynamic rivalry between quantum and post-quantum cryptography has been extremely stimulating for both parts, fueling outstanding developments. From a theoretical standpoint, there's been a fervent push to formalize the security proofs of QKD protocols [17–20], highlighting the profound distinction between the foundational principles of QKD and the security assurances offered by PQC. Meanwhile, on the practical front, we have witnessed remarkable strides at the implementation level, such as the debut of commercial QKD devices [21–28], the deployment of QKD networks both solely fiber-based [29–31] and supported by ground-satellites free space links [32, 33], or the development of compact on-chip systems [34, 35].

The post-quantum community has also witnessed significant progress, proposing different approaches such as code-based cryptography [36], lattice-based cryptography [37], multivariate cryptography [38], and hash-based cryptography [39], culminating in the famous NIST PQC standardization challenge announced at PQCrypto 2016 [40]. This challenge consisted of four rounds, where several protocols were proposed and analyzed, to select the PQC schemes that would eventually become industry standards. Surprisingly, some of those protocols were broken even in the final rounds of the challenge [41, 42], casting doubts about the reliability of these new approaches. However, to prevent dramatic security issues, the hybridization of PQC with traditional cryptographic schemes has been promoted [43, 44]. Furthermore, there has been a development of strategies centered around the concept of "crypto-agility" [45, 46], a methodology for rapidly updating cryptographic standards without significant alterations to the existing infrastructure.

## Crypto crossroads

The relationship between QKD (as well as quantum cryptography at large) and PQC is complex. While it is undeniable that this competition between QKD and PQC has stimulated research and development and triggered progress on both sides, there is also a risk it could evolve into systematic opposition, potentially hindering the advantages that a collaborative environment could foster.

For instance, national security entities, traditionally aligned with the PQC paradigm, have pinpointed various challenges in QKD that currently impede its mainstream adoption [47–50]. While some critiques, such as the supposed lack of authentication, or the risk of denial of service, have been adequately addressed [50, 51], many remain pertinent, casting shadows on the immediate applicability of QKD. A pressing concern is the need to enhance performance while minimizing the cost and complexity of the hardware. Therefore, cost-efficiency is expected to be a central criterion that should guide the design of future QKD systems, aiming to broaden their applicability. Another important challenge in the field consists in addressing the discrepancy between the theoretical unconditional security, sometimes referred to as "absolute security" [52–54], and the more limited security that can be achieved in practice using current hardware and engineering designs.

This conundrum between the security and practicality of QKD was rightly boiled down in [55] to the following statement: *absolute security implies infinite costs, which in turn implies zero practical interest*. Here, we find ourselves at a crossroads, already identified a decade ago by Valerio Scarani and Christian Kurtsiefer in their "black paper on quantum cryptography" [56]: either to keep pursuing the quest for absolute security, while giving up on any real-world application of quantum cryptography, or to reconsider the absolute security claims and adopt a balanced viewpoint.

## Our approach: building bridges

Naturally, it should come as no surprise that we strongly believe that the quantum cryptography community should not give up on the aspiration of seeing quantum technologies actively contribute to the world of cybersecurity. Instead, what we propose in this thesis are two different approaches to bridge the gaps with the classical cryptography community and avoid the perpetuation of antagonistic positions.

Our first approach consists of adapting a traditional method for vulnerability analysis, known as Common Criteria [57], to quantum cryptography. This method provides a framework for evaluating the security features and capabilities of information technology products. The main idea behind our work is to evaluate with a standardized framework the possible attacks to a QKD device, to prioritize the most dangerous attacks, and to help guide the design and engineering of practical QKD systems towards the highest possible security standards. This initiative aligns with international efforts toward standardizing security certification for quantum technologies [58–62], aiming to reduce the gap between theoretical and practical security.

In the second approach, we consider a *hybrid security model*, called Quantum Computational Time-lock (QCT), where we operate under the realistic assumption that breaking

computationally secure encryption would take a time span far exceeding the coherence time of current quantum memories. By shifting away from the pursuit of absolute security, we can then propose key distribution protocols that surpass standard QKD benchmarks. Moreover, these protocols not only offer improved key rates and loss tolerance but are also provably secure, as per standard QKD security criteria [17], against adversaries with unbounded computational power after quantum storage decoherence, offering what is called *everlasting security* [2]. Notably, unlike in PQC and traditional cryptography, the security remains robust against any future technological advancements made by potential attackers.

## Outline of the manuscript and main contributions

In the following, we give an outline of the manuscript and briefly discuss our contributions.

### Part I: Background

To facilitate the understanding of this thesis, the first part offers an exploration of preliminary concepts within classical and quantum information theory and cryptography, with a particular emphasis on quantum key distribution.

**Chapter 2 – Preliminaries.** We start by introducing the notation and the basic notions of finite-dimensional quantum mechanics in Section 2.1, followed by the necessary background on Continuous-Variable systems in Section 2.2. Here in particular, we talk about coherent state mapping [63], an abstract mapping scheme to map the prepare-and-measure qubit protocols to more practical coherent states protocols, which will be used to make the experiment described in Chapter 8 more practical. Moreover, we describe in detail methods for measuring the quadrature components of a coherent state, usually called *coherent detection*. Finally in Section 2.3 we introduce basic tools of classical and quantum information theory to quantify the information exchanged between Alice and Bob in communication protocols such as QKD. In particular the concept of *conditional min-entropy* will be crucial to quantify the amount of information that might have leaked to an eavesdropper in our quantum key distribution protocol presented in Chapter 7.

**Chapter 3 – Introduction to quantum key distribution.** In this chapter, we take a closer look at quantum key distribution from various angles, including its practical implementation and security aspects, offering a broad overview. We start in Section 3.1 with a general introduction to modern cryptography, focusing on its basic principles.

Section 3.2 then presents the general structure of a QKD protocol, and the different assumptions that must be made to prove security in a rigorous manner. In particular, we distinguish between the foundational assumptions of QKD, necessary for any type of protocol, and the more specific trust assumptions on the implementation of the protocol. In Section 3.3 we present two explicit protocols: the BB84 protocol [1], whose presentation is essential in any introduction to QKD, and the GG02 protocol [64], a Continuous-Variable Quantum Key Distribution (CV-QKD) protocol for which we will identify some security loopholes in Chapter 4.

Section 3.4 focuses on presenting clear definitions of security for QKD and the general structure of a security proof. We conclude this section with the asymptotic key rate given by the Devetak-Winter formula [65] in Eq. (3.10), which will be used to compute the key rate for our quantum key distribution protocol presented in Chapter 7.

Finally, Section 3.5 is devoted to practical implementations of QKD and the possible vulnerabilities that could arise from imperfect implementations of a protocol. In particular, we introduce the *blinding attack* [66], an attack strategy that comprises manipulating Bob’s single-photon detectors by shining intense light on them. This attack strategy is similar to the one that we discuss in Chapter 4, this time directed at a homodyne detector—a device designed for coherent detection of a single quadrature of an electromagnetic field used for CV-QKD protocols.

## Part II: QKD vulnerability analysis

The second part of the manuscript is devoted to presenting my first research project as an early PhD student, which focused on the certification of QKD devices. Exploiting the non-linear response of the homodyne detector near its detection limit, an eavesdropper, Eve, can launch an attack against CV-QKD devices called *saturation attack* [67]. It consists of biasing the noise estimation by actively inducing the saturation of the homodyne detectors. In this project, we report the first experimental demonstration of a saturation attack against a running CV-QKD system, ultimately leading to a full security breach. We go beyond that by explicitly demonstrating the benefits of using well-established methodology from classical security—Common Criteria, in the context of QKD system security evaluations. This research led to a journal article [68], a collaborative effort with my former colleagues at Télécom Paris. Specifically, R. Kumar was responsible for the experimental realizations of two different variants of the saturation attack. H. Qin and R. Alléaume contributed by developing the theoretical model for the attack. Meanwhile, I focused on adapting the Common Criteria general framework to QKD and conducted the attack rating analysis and evaluation.

**Chapter 4 – QKD attack rating.** We begin in Section 4.1 with an introduction to the collective effort at the international level that has been made towards the development of a standardized approach for security certification. We then proceed by describing in detail the concept of *attack potential*—a metric already defined in the Common Criteria framework for classical devices. This metric aims to evaluate the total effort required by a malicious hacker to successfully mount an attack against QKD systems. The rating procedure consists of attributing a numeric value to the attack potential, by summing the contributions from the different factors shown in Table 4.1. These factors span from the level of technical expertise required to mount the attack, to the level of sophistication of the equipment used.

Section 4.2 starts with an explanation of the general principle behind a saturation attack, focusing then on the experimental analysis of two possible implementations using the attack potential metric. The first and most challenging one is the coherent attack strategy [67] where Eve resends a coherent displaced signal to induce the detector saturation. Our second attack strategy consists of the incoherent saturation attack [69], where we shine an independent laser toward Bob’s coherent receiver. The implementation of this attack is considerably simpler



and it constitutes a dangerous threat to practical CV-QKD systems, resulting in a lower attack potential.

Finally, in Section 4.3 we summarize our main take-home message: we should tackle the challenge of reducing the gap between practical and theoretical security by rating feasible attacks and prioritizing accordingly the greatest threats.

## Part III: Hybrid quantum cryptography from communication complexity

The core of my thesis unfolds in the third section, starting with a quest for new theoretical quantum cryptographic constructions, developed in partnership with the Institute on the Foundations of Computer Science (IRIF), at Paris Cité University. Our primary goal is to propose a key distribution protocol that could surpass standard QKD benchmarks in terms of both performance and functionalities, basing its security on the QCT security model.

The starting point was to identify some communication problems that would show a performance gap between classical and quantum strategies. Leveraging the QCT model we aimed to provide a key distribution scheme that allowed Alice and Bob to exchange a key performing the corresponding quantum strategy, while an eavesdropper would be reduced only to classical strategies. Such communication problems have been identified in the general framework of *communication complexity* [70] and thoroughly analyzed in Chapter 5. Once introduced the general framework of communication complexity, we examine in Chapter 6 alternative security models in quantum cryptography, where potential adversaries may have some additional limitations compared to standard QKD. The last model that we consider is precisely the QCT model. Finally, in Chapter 7 we propose our final key distribution scheme. The work described in Chapters 5, 6 and 7 led to an arXiv publication [71] and has been submitted for journal review.

**Chapter 5 – From classical to quantum communication complexity.** Section 5.1 introduces the concept of communication complexity in both a deterministic and a randomized setting. It involves two parties, Alice and Bob, aiming to compute a function  $f(x, y)$  based on their respective inputs from sets  $\mathcal{X}$  and  $\mathcal{Y}$ , using classical or quantum communication. The communication complexity of a problem is defined as the *communication cost* of the optimal protocol, i.e. the amount of bits/qubits necessary to solve a communication complexity problem with a fixed probability.

Section 5.2 presents an alternative quantity, called *information complexity* [72] which is a measure of the minimum amount of information that two parties need to exchange about their respective inputs to compute a function of both inputs. As it turns out in Chapter 7, simply having a gap between quantum and classical communication complexity is insufficient for cryptographic applications within the QCT model. Instead, what is crucial is the presence of a gap between quantum communication complexity and classical information complexity. Consequently, we discuss how to link classical information and communication complexity using compression schemes. In particular, our first original contribution in this chapter has been to derive the explicit constants in the one-way compression scheme in Lemma 5.2.4, crucial to derive an explicit key rate formula in our key distribution protocol.

Finally, Section 5.3 focuses on quantum communication complexity problems that show

an exponential gap between classical and quantum strategies. In particular, we thoroughly study two different one-way quantum communication complexity problems: the  $\beta$ -Partial Matching ( $\beta$ PM) problem [3] and the *Vector in a Subspace (VS)* problem [73]. Our original contributions in this section consist in the derivation of the explicit prefactors of the classical lower bound for the  $\beta$ PM problem in Theorem 5.3.1, and the analysis of the best-known classical protocol for both problems, leading to Theorems 5.3.2 and 5.3.3 respectively.

**Chapter 6 – Quantum cryptography against a bounded adversary.** After a brief introduction in Section 6.1, we present in Section 6.2 a first alternative security model, called *Quantum Data Locking (QDL)* [74], where one assumes in the security proof that an adversary can perfectly store an unlimited number of qubits in a quantum memory, but only for a finite period of time. In particular, in this section we introduce the security framework called *strong QDL*, where an adversary is assumed to have access to a perfect copy of Alice’s quantum state.

In Section 6.3 we then introduce the *Noisy-Storage Model (NSM)*, which accounts for limited and noisy quantum storage resources available to adversaries. Here we discuss different definitions of a "noisy quantum memory", starting from memories only bounded in size [75], then considering memories with limited classical [76] and quantum [77] capacities, and how one can prove security under each definition. In particular, in this section we introduce a general theoretical attack called the *encoding attack* depicted in Figure 6.2. Here, an adversary has immediate access to some quantum information, and after a time  $t$  obtains some additional classical information. What they can do is to first prepare the initial quantum information for storage while extracting some classical information. Subsequently, the adversary stores the quantum state using a noisy quantum memory until they have access to the additional classical information.

In Section 6.4, we then describe the QCT model, introduced in [78]. Alice and Bob are assumed to have access to a public authenticated classical channel and to an encryption scheme that provides computational security against any unauthorized (and assumed computationally-bounded) attacker, but only for a duration  $t_{comp}$  after a ciphertext is exchanged on the classical channel. The second assumption is that Eve cannot reliably store a quantum state during a time larger than  $t_{comp}$ . In particular we assume that she has access to what we call a  $(t_{comp}, \delta)$ -noisy quantum memory, i.e. a time-dependent quantum memory  $\Phi_t$  such that after time  $t_{comp}$  we have  $\|\Phi_{t_{comp}} - \mathcal{F}\|_{\diamond} \leq \delta$ , where  $\mathcal{F}$  is a completely mixing channel and  $\|\cdot\|_{\diamond}$  is the diamond norm [79]. In other words, it is a quantum memory that is hard to distinguish (parametrized by a parameter  $\delta$ ) from a completely mixing channel, when it stores a quantum state for a time  $t_{comp}$  or longer.

Our original contribution in this chapter consists in proving Theorem 6.4.1. We show that the general encoding attack within the QCT model can be simplified to a scenario where the adversary employs no quantum storage, referred to as the *immediate measurement strategy*. Section 6.5 concludes the chapter by summarizing the similarities and differences between the different security models.

**Chapter 7 – HM-QCT protocol.** Now that we have described all the ingredients necessary to construct a key distribution scheme, in Chapter 7 we introduce an explicit construction for a new key distribution protocol called *Hidden Matching Quantum Computational Time-lock (HM-QCT)*. It is based on the  $\beta$ PM problem analyzed in Chapter 5, a boolean version of the Hidden Matching problem [80]. In this one-way communication problem,  $\Omega(\sqrt{n})$  bits of communication from Alice to Bob are required, against only  $\mathcal{O}(\log(n))$  qubits, with  $n$  the length of the binary string  $x$  that constitutes Alice’s input. In particular, we unlock the possibility of sending multiple copies of the same state to perform key establishment with *everlasting security* [2] with performances that go beyond standard QKD.

Section 7.1 provides a high-level overview of a single round of the HM-QCT protocol, illustrated in Figure 7.1. Following this, Section 7.2 delves into a more detailed explanation of how the protocol works, followed by a security analysis in the i.i.d. setting, i.e. a restricted scenario where the adversary performs the same strategy independently every round. Once we reduce to an immediate measurement strategy thanks to Theorem 6.4.1, a central result of our work is the exploitation of the communication gap between quantum and classical strategies to build a secure key distribution protocol. In particular, the security reduction to the communication complexity of the  $\beta$ PM problem cannot be done directly. First, since Alice is sending  $m$  copies of the same  $n$ -dimensional quantum state, the amount of information that she is leaking to Eve about the input  $x$  is at most  $m \log(n)$  bits thanks to the Holevo bound. This simply reduces the security proof to the study of the information complexity of the classical  $\beta$ PM problem. In particular, through mapping communication complexity to information complexity in the one-way setting in Lemma 5.2.4, we demonstrate in Theorem 7.2.1 that Eve’s one-round guessing probability is safely bounded away from 1 when Alice sends  $\mathcal{O}\left(\frac{\sqrt{n}}{\log(n)}\right)$  copies of the quantum state.

Finally, in Section 7.3 we discuss the performance and functionalities of our protocol. Our results illustrate that the QCT hybrid security model constitutes a promising route to enhance the capabilities and effectiveness of quantum cryptography, while retaining some core advantage against classical cryptography: the possibility of providing everlasting security. In particular, our protocol offers the following benefits.

- **Boosted key rates:** Security can be achieved while sending up to  $\mathcal{O}\left(\frac{\sqrt{n}}{\log(n)}\right)$  photons per channel use, overcoming the standard limit of one photon per channel use. The HM-QCT protocol, based on the  $\beta$ PM problem, can be implemented with two single-mode threshold detectors, and performance can hence be benchmarked with 2-output-mode protocols. The fact that security can be achieved with many photons per channel use leads to asymptotic achievable secret key rates that can be boosted by a factor  $\mathcal{O}\left(\frac{\sqrt{n}}{\log(n)}\right)$  with respect to BB84 QKD. As illustrated in Figure 7.2, HM-QCT could moreover overcome the fundamental secret key capacity [81].
- **Improved functionalities:** A fascinating advantage of enabling multiple copies per channel use is the potential to consistently hit the classical capacity of one bit per channel use over relatively short distances, as illustrated in Figure 7.3 — a feat unseen in standard QKD. Moreover, multiple photons not only offer improved efficiency but also enable multicast key distribution with up to  $\mathcal{O}\left(\frac{\sqrt{n}}{\log(n)}\right)$  authorized Bobs simultaneously.

- **Security with untrusted detectors:** Eve’s information can be upper bounded by only considering the state that Alice inputs and does not require (as in standard QKD) any information about Bob’s measurement results, as discussed in Section 7.3.3. Consequently, the implementation of Bob’s measurement device is not required to be trusted, a property analog to measurement-device independent security [82].

Building on our theoretical work on key establishment, whose security and effectiveness hinge on the ability of two parties to address a one-way quantum communication complexity problem more efficiently than is possible classically, I performed a (quite challenging) transition to a hands-on experiment within the walls of the Laboratoire Kastler Brossel (LKB), at Ecole Normale Supérieure. Here, I had complete access to an experimental platform that had already been used to simulate two-photon linear networks [83, 84].

In this last experimental project, detailed in Chapter 8, we investigate the feasibility of demonstrating a quantum advantage in communication complexity. We leverage the intricate mode mixing inherent in multimode fibers by employing *wavefront shaping techniques* [4, 5] to tackle quantum communication complexity problems. An article detailing this work is currently under development.

**Chapter 8 – Platform for one-way quantum communication complexity.** After a brief introduction (Section 8.1) on our work, Section 8.2 gives a broad overview of light propagation through disordered media, such as a multimode fiber. First, we provide a description of speckle phenomena, mixing properties of a multimode fiber, and wavefront control of light propagating through complex optical systems. Second, we describe the impact that wavefront shaping has had on cryptography and quantum information processing, discussing some pioneering approaches in both worlds: from the use of complex media as unclonable physical functions [85, 86], to their use in QKD [87–89] and in programmable optical networks [83, 84, 90, 91].

Next, Section 8.3 starts with detailing the experimental setup and its application in addressing one-way quantum communication complexity problems like the  $\beta$ PM and VS problem. Following this, we present a theoretical framework and conduct a numerical study to assess the flexibility and scalability of our optical network.

- **Flexibility:** Our method enables the implementation of Bob’s detection phase for any one-way quantum communication complexity problem. It enables the construction of reconfigurable linear operators, allowing for precise manipulation of both amplitude and phase of each component, a pictorial representation of our method is presented in Figure 8.7.
- **Scalability:** Unlike traditional reconfigurable network designs that rely on cascade interferometers and suffer from a quadratic increase in components like beamsplitters and phase shifters with circuit size, our method overcomes these challenges. By simply engineering multimode fibers with larger diameters, we gain the ability to control more physical modes, enabling us to configure linear optical networks that can scale in size.

In the last part of this section, we report the experimental realization of the  $\beta$ PM quantum protocol up to dimension  $n = 8$ . In particular, a clear example of how well our platform

performs the  $\beta$ PM protocol is given in Figure 8.11, where we showcase how a fingerprint can be transmitted while tracking the number of photons sent. While the results are still far from being able to show quantum advantage, we further discuss in Section 8.4 directions to extend this approach to different quantum communication complexity problems, such as the VS problem, and how we can scale in practice this approach to higher dimensions, to finally reach a quantum advantage.

**Chapter 9 – Perspectives.** We conclude our manuscript in this final chapter. Here we explore some possible future directions stemming from my PhD research. We start by examining the potential impacts of our new security certification method introduced in Chapter 4. Next, we consider ways to extend and improve our security proof for the HM-QCT protocol. Our focus then shifts to the opportunities the QCT could open in the field of quantum cryptography, exploring potential routes for novel cryptographic methods. We wrap up with ideas on developing cryptographic constructions with provable security, leveraging the isotropic mode mixing in complex media such as multimode fibers.

# List of publications and activities done during the PhD

## Articles

1. **F. Mazzoncini**, H. Defienne, M. Dąbrowski, R. Alléaume, and S. Gigan, in preparation.
2. **F. Mazzoncini**, B. Bauer, P. Brown, and R. Alléaume, "Hybrid Quantum Cryptography from Communication Complexity." arXiv, Nov. 27, 2023. [Link](#)
3. R. Kumar, **F. Mazzoncini**, H. Qin, and R. Alléaume, "Experimental vulnerability analysis of QKD based on attack ratings." Sci Rep 11, 9564 (2021). [Link](#)

## Contributed talks and seminars

1. QSNP Workshop "Quantum meets Classical Cryptography" (WP4 & WP6). 10-12 January 2024, Paris, France.
2. "Saclay Quantum Seminar", 22 May 2023, Gif-sur-Yvette, France.
3. "Journées Informatique Quantique 2022 (JIQ'22)", 14-15 November 2022, Paris, France.
4. "Journée IDIA IP Paris (département informatique, données, intelligence artificielle)". 28 June 2022, Palaiseau, France.
5. "IRIF research seminar", algorithms and complexity, 7 June 2022, Paris, France.
6. "The International Conference on Quantum Communication (ICQOM)", 18-22 October 2021, Paris, France.
7. "Qcrypt21", 23-27 August 2021 (Online). [Video](#)

## Poster presentations

1. "GDR IQFA 13th Colloquium", 16-18 November 2022, Palaiseau, France.
2. "Journée de la recherche du LTCI", 14 October 2022, Palaiseau, France.
3. "Qcrypt22", 29 August - 2 September 2022 (Hybrid).
4. "International Conference on Quantum Communication, Measurement and Computing (QCMC)", 11-15 July 2022, Lisbon, Portugal.
5. "SPIE Photonics Europe 2022", 03-07 April 2022, Strasbourg, France.
6. "European Quantum Technologies Conference (EQTC)", 29 November - 2 December, 2021 (Online).
7. "GDR IQFA 11th Colloquium", December 2 - 4, 2020, (Online).

## Extra activities

During my PhD, I also completed the research I had initiated during my master's thesis on quantum batteries, and this work was successfully published in Phys. Rev. A.

- **F. Mazzoncini**, V. Cavina, G.M. Andolina, P.A. Erdman, and V. Giovannetti, "Optimal control methods for quantum batteries." Phys. Rev. A 107, 032218 (2023). [Link](#)

In addition to my research accomplishments, I dedicated two consecutive years to teaching. I conducted intensive two-week projects on quantum information, with each year totaling 9 hours of teaching. During these projects, students gained practical experience in quantum information by actively engaging in coding exercises on the IBM quantum computer.

- Programming a real quantum computer, 2-weeks intensive project, Project Application Final (PAF), L3 at Télécom Paris (2022-2023).

# Part I

## Background





# PRELIMINARIES

## Contents

|            |   |           |
|------------|---|-----------|
| <b>2.1</b> | <b>Introduction to quantum mechanics . . . . .</b>    | <b>16</b> |
| 2.1.1      | Quantum states . . . . .                              | 16        |
| 2.1.2      | Quantum measurements . . . . .                        | 18        |
| 2.1.3      | Quantum channels . . . . .                            | 19        |
| 2.1.4      | Distance measures among states and channels . . . . . | 19        |
| <b>2.2</b> | <b>Quantum continuous variables . . . . .</b>         | <b>20</b> |
| 2.2.1      | Canonical quantization . . . . .                      | 20        |
| 2.2.2      | Coherent states . . . . .                             | 21        |
| 2.2.3      | Coherent detection . . . . .                          | 23        |
| <b>2.3</b> | <b>Information theory . . . . .</b>                   | <b>24</b> |
| 2.3.1      | Classical information theory . . . . .                | 25        |
| 2.3.2      | Quantum information theory . . . . .                  | 26        |

This chapter begins with an overview of finite-dimensional quantum mechanics and continuous-variable systems, setting the notations that we will use across the manuscript. Additionally, we touch upon key concepts from classical and quantum information theory.

## 2.1 Introduction to quantum mechanics

Let's start with an overview of the mathematical framework of quantum mechanics. For those interested in a deeper exploration, we recommend consulting [92].

### 2.1.1 Quantum states

A quantum state is the state of a specific physical system. All possible quantum states of the system belong to a so-called *Hilbert space*, a complete, complex vector space endowed with an inner product. A *pure state*, represented by  $|\psi\rangle$ , is defined as a unit vector within the Hilbert space  $\mathcal{H}$  of the quantum system. The term "pure" indicates that this state encapsulates the maximum amount of information possible about the system's quantum state. In other words, a pure state represents a quantum system with a precisely defined state, with no ambiguity or uncertainty. An important example is the *qubit* Hilbert space. This space is spanned by the basis  $\{|0\rangle, |1\rangle\}$ , consisting of two orthonormal vectors. A general qubit pure state can be expressed as

$$|\psi\rangle = \alpha |0\rangle + \beta |1\rangle, \quad (2.1)$$

where  $\alpha, \beta \in \mathbb{C}$  and  $|\alpha|^2 + |\beta|^2 = 1$ . In addition to  $|0\rangle$  and  $|1\rangle$ , Two other important qubit orthonormal states are  $|+\rangle := \frac{|0\rangle + |1\rangle}{\sqrt{2}}$  and  $|-\rangle := \frac{|0\rangle - |1\rangle}{\sqrt{2}}$ . In the literature the basis  $\{|0\rangle, |1\rangle\}$  is often called "z basis" or "computational basis" while  $\{|+\rangle, |-\rangle\}$  is called "x basis" or "Hadamard basis".

### Mixed states and density matrices

There are situations where the exact state of a quantum system might not be fully known. For instance, a quantum system might exist in a statistical mixture—not a superposition—of several possible states  $|\psi_i\rangle$ , each with a certain probability  $p_i$ . This scenario doesn't correspond to a pure state, but rather to what's known as a *mixed state*. The conventional representation using state vectors isn't the most efficient way to describe a mixed state. Instead, quantum mechanics employs an alternative, yet mathematically equivalent, formulation known as the *density matrix*.

#### Density matrix formalism

A density matrix  $\rho \in \mathcal{D}(\mathcal{H})$  for a quantum system is defined through the following convex sum of projectors

$$\rho := \sum_i p_i |\psi_i\rangle\langle\psi_i|, \quad (2.2)$$

where  $p_i$  is the probability that the system is in the pure state  $|\psi_i\rangle \in \mathcal{H}$ , and  $\mathcal{D}(\mathcal{H})$  denotes the set of density operators acting on a finite-dimensional Hilbert space  $\mathcal{H}$ .

#### Properties:

- i)  $\text{Tr}[\rho] = 1$ ,

- ii)  $\rho$  is a positive-semidefinite operator<sup>a</sup>,
- iii)  $\rho$  represents a pure state if and only if  $\rho^2 = \rho$ .

<sup>a</sup>A linear operator  $M \in \mathcal{L}(\mathcal{H})$  is called positive-semidefinite if  $\langle \psi | M | \psi \rangle \geq 0$  for all  $|\psi\rangle \in \mathcal{H}$ . The set of positive-semidefinite operators acting on a finite-dimensional Hilbert space  $\mathcal{H}$  is denoted by  $\mathcal{P}(\mathcal{H})$ .

It is important to highlight that various probability distributions can describe the same mixed state, implying that the states they depict are physically indistinguishable. This equivalence occurs exclusively when the corresponding density matrices are identical. For instance, the completely mixed state  $\frac{1}{2} |0\rangle\langle 0| + \frac{1}{2} |1\rangle\langle 1|$  is equivalent to  $\frac{1}{2} |+\rangle\langle +| + \frac{1}{2} |-\rangle\langle -|$ , with both density matrices being identical. An analogous point is that a global phase factor  $e^{i\theta}$  in pure states lacks physical relevance; indeed, the pure states  $|\psi\rangle$  and  $e^{i\theta} |\psi\rangle$  are described by the same density matrix,  $\rho = |\psi\rangle\langle \psi|$ .

## Multipartite states

To analyze complex quantum systems, it is often convenient to consider a partition into different subsystems. Mathematically, if we have a collection of  $n \in \mathbb{N}$  subsystems with the Hilbert space of the  $i$ -th quantum system being  $\mathcal{H}_i$ , then the Hilbert space of the entire joint system is given by the tensor product of the individual Hilbert spaces  $\mathcal{H}_{\text{joint}} := \bigotimes_{i=1}^n \mathcal{H}_i$ . We say a state  $\rho_{\text{sep}} \in \mathcal{D}(\mathcal{H}_{\text{joint}})$  is *separable* if it can be written as a convex combination of tensor products of states from the individual subsystems, that is

$$\rho_{\text{sep}} = \sum_i p_i \rho_1^{(i)} \otimes \cdots \otimes \rho_n^{(i)} \quad (2.3)$$

with  $\sum_i p_i = 1$ ,  $p_i \geq 0$  and  $\rho_j^{(i)} \in \mathcal{D}(\mathcal{H}_j)$  for every  $i, j$ . On the other hand, a state that is not separable is called *entangled*.

There are instances where we are interested in determining the quantum state of a particular subsystem, disregarding the states of other subsystems. Consider, for instance, a bipartite quantum state  $\rho_{AE}$ , involving two parties - Alice (A) and Eve (E). In such scenarios, we might choose to overlook the subsystems associated with A, focusing solely on the quantum state pertinent to Eve's subsystem E. The mathematical operation for focusing on a specific subsystem's quantum state, while disregarding others, is called the *partial trace*. For a bipartite state  $\rho_{AE}$ , taking the partial trace over subsystem A is defined as

$$\rho_E = \text{Tr}_A[\rho_{AE}] := \sum_{a \in \mathcal{A}} (\langle a | \otimes \mathbf{1}_E) \rho_{AE} (|a\rangle \otimes \mathbf{1}_E), \quad (2.4)$$

where  $\mathcal{A}$  constitutes a complete orthonormal basis set for subsystem A.

## Classical-quantum states

Consider a classical random variable  $A$  with distribution  $P_A$  on some set  $\mathcal{A}$ . Since we are going to treat classical and quantum variables with the same formalism, it is useful to view  $A$  as a particular case of a quantum system. We shall identify the classical values  $a \in \mathcal{A}$

with some fixed orthonormal basis  $|a\rangle$  on some Hilbert space  $\mathcal{H}_A$ . The random variable  $A$  can then be identified with the density matrix

$$\rho_A = \sum_{a \in \mathcal{A}} P_A(a) |a\rangle\langle a|. \quad (2.5)$$

We can extend this representation to hybrid settings where the state  $\rho_Q^{(a)}$  of a quantum system  $\mathcal{H}_Q$  depends on the value  $a$  of a classical random variable  $A$ . Such a state is called a *classical-quantum state*, or simply *cq-state*, and takes the form

$$\rho_{AQ} = \sum_{a \in \mathcal{A}} P_A(a) |a\rangle\langle a| \otimes \rho_Q^{(a)}. \quad (2.6)$$

In the context of cryptography, the symbol  $a$  typically denotes some (partially secret) classical string that Alice generates during a quantum protocol [93]. Meanwhile,  $\rho_Q^{(a)}$  represents the quantum information that an eavesdropper might collect during the protocol. This quantum information could potentially be correlated to the string  $a$ .

### 2.1.2 Quantum measurements

A measurement  $M$  with outcomes in the set  $\mathcal{M}$  is a process in which information about the state of a physical system is acquired by an observer. Mathematically, quantum measurements are defined by a set of measurement operators, denoted as  $\{M_m\}_{m \in \mathcal{M}}$  acting on some Hilbert space  $\mathcal{H}$ . For a system in state  $\rho \in \mathcal{D}(\mathcal{H})$  just before a measurement, the probability of obtaining the outcome  $m \in \mathcal{M}$  is expressed by

$$p(m) = \text{Tr} [M_m^\dagger M_m \rho], \quad (2.7)$$

where the measurement operators satisfy  $\sum_m M_m^\dagger M_m = \mathbf{1}$ . If the outcome  $m$  is observed, the quantum system's state transforms to

$$\rho_m = \frac{M_m \rho M_m^\dagger}{\text{Tr}[M_m^\dagger M_m \rho]}. \quad (2.8)$$

### POVM measurements

If we are only interested in calculating the probabilities of various measurement outcomes, without needing to fully understand the changes to the quantum state post-measurement, the most comprehensive description of quantum measurements is provided by the Positive Operator-Valued Measure (POVM) formalism. Defining the measurement as a map  $\Pi : \mathcal{M} \rightarrow \mathcal{P}(\mathcal{H})$  one can simply rewrite Eq. (2.7) as

$$p(m) = \text{Tr} [\Pi(m) \rho], \quad (2.9)$$

where now the map  $\Pi$  satisfies  $\sum_{m \in \mathcal{M}} \Pi(m) = \mathbf{1}$ . *Projective measurements* are special class of measurements where in addition we have  $\Pi(m)^2 = \Pi(m)$  for all  $m \in \mathcal{M}$ .

### 2.1.3 Quantum channels

A measurement is just one possible operation that can be performed on a quantum state. What then constitutes the most general operation that a quantum device is capable of executing? Mathematically it is described by a linear mapping  $\mathcal{E} : \mathcal{L}(\mathcal{H}_A) \rightarrow \mathcal{L}(\mathcal{H}_B)$  which satisfy the following two properties.

- i)  $\mathcal{E}$  is trace preserving, i.e. for any  $\rho_A \in \mathcal{L}(\mathcal{H}_A)$  we have  $\text{Tr}[\rho_A] = \text{Tr}[\mathcal{E}(\rho_A)]$
- ii)  $\mathcal{E}$  is Complete Positive (CP), i.e. for any positive-semidefinite operator  $\rho_{AC}$  the output state  $(\mathcal{E} \otimes \mathcal{I}_C)(\rho_{AC})$  is also a positive-semidefinite operator, where  $\mathcal{I}_C$  denotes the identity channel on some auxiliary system  $C$ .

These two conditions ensure that all quantum states are mapped to quantum states. We refer to such operations as Complete Positive Trace Preserving (CPTP) maps or more generally as *quantum channels*. A definition similar to the one for cq-states can be used to describe quantum channels whose outcomes are partially classical. The quantum channel  $\mathcal{E}_{\text{classic}} : \mathcal{L}(\mathcal{H}_1) \rightarrow \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_2)$  is said to be *classical on  $\mathcal{H}_A$*  if it can be written as

$$\mathcal{E}_{\text{classic}}(\rho) = \sum_a |a\rangle\langle a| \otimes \mathcal{E}^{(a)}(\rho), \quad (2.10)$$

where for any  $a \in \mathcal{A}$ ,  $\mathcal{E}^{(a)}$  is a trace non-increasing complete positive map from  $\mathcal{L}(\mathcal{H}_1)$  to  $\mathcal{L}(\mathcal{H}_2)$ , with the additional condition that  $\sum_{a \in \mathcal{A}} \mathcal{E}^{(a)}$  is trace-preserving. Finally, one should observe that a measurement on  $\mathcal{H}_1$  with outcomes in  $\mathcal{A}$  can be seen as a CPTP map from  $\mathcal{L}(\mathcal{H}_1)$  to  $\mathcal{L}(\mathcal{H}_A)$  classical in  $\mathcal{H}_A$ .

### 2.1.4 Distance measures among states and channels

It is a natural question to ask how well a given collection of quantum states can be discriminated by means of a measurement. We start to tackle this problem by introducing the notion of distance between quantum states.

**Definition 2.1.1** (Trace Distance). *Let  $\rho$  and  $\sigma$  be linear operators in a Hilbert space  $\mathcal{H}$ . The trace distance between  $\rho$  and  $\sigma$  is defined as*

$$D(\rho, \sigma) := \frac{1}{2} \|\rho - \sigma\|_1, \quad (2.11)$$

where  $\|\cdot\|_1$  denotes the trace norm, given by  $\|A\|_1 = \text{Tr}[\sqrt{A^\dagger A}]$  for any linear operator  $A$ .

As a matter of fact, the trace distance has a clear operational interpretation as it measures how distinguishable two quantum states are. Consider a scenario where Alice sends one of two quantum states,  $\rho$  or  $\sigma$  to Bob, with probabilities  $\lambda$  and  $1 - \lambda$ , respectively. Upon receipt, Bob performs a measurement on the received state to infer whether he was sent  $\rho$  or  $\sigma$ . The maximum probability  $P_{\text{guess}}$  with which Bob can guess correctly is achieved by a projective measurement and it is given by

$$P_{\text{guess}} = \frac{1}{2} + \frac{1}{2} \|\lambda\rho - (1 - \lambda)\sigma\|_1. \quad (2.12)$$

This result is known as *Holevo-Helstrom theorem* [94, 95].

Similarly, one can define a notion of distance between quantum channels, called the *diamond norm*, offering an analog to the Holevo-Helstrom theorem when it comes to distinguishing between pairs of quantum channels [79]:

**Definition 2.1.2.** Let  $\Phi : \mathcal{L}(\mathcal{H}_A) \rightarrow \mathcal{L}(\mathcal{H}_B)$ . The diamond norm is defined as

$$\|\Phi\|_{\diamond} := \max_{\rho \in \mathcal{P}(\mathcal{H}_A \otimes \mathcal{H}_A) : \|\rho\|_1 \leq 1} \|(\Phi \otimes \mathcal{I}_A)(\rho)\|_1, \quad (2.13)$$

where  $\mathcal{I}_A$  denotes the identity channel on the Hilbert space  $\mathcal{H}_A$ .

Let us consider a one-shot discrimination task equivalent to the one for quantum states. The optimal guessing probability  $P_{\text{guess}}$  in distinguishing two quantum channels  $\Phi$  and  $\Psi$  is now

$$P_{\text{guess}} = \frac{1}{2} + \frac{1}{2} \|\lambda\Phi - (1 - \lambda)\Psi\|_{\diamond}. \quad (2.14)$$

Specifically, the optimal measurement for this purpose is a projective measurement, and the optimal input state is a pure state [79].

## 2.2 Quantum continuous variables

A quantum system described by observables whose numerical values belong to continuous intervals is said to be a Continuous Variable (CV) system. In this section, we will introduce the formalism necessary to study quantum information with the continuous variables of a bosonic system, such as the electromagnetic field. For an extensive description of CV systems tailored for quantum information processing, we refer the reader to [96].

### 2.2.1 Canonical quantization

Let's consider a continuous variable system as a multimode quantum harmonic oscillator described by the Hamiltonian

$$H = \sum_{k=1}^N \hbar\omega_k \left( \hat{a}_k^\dagger \hat{a}_k + \frac{1}{2} \right), \quad (2.15)$$

Where  $\hbar$  denotes the reduced Planck constant and  $\{\omega_k\}_{k=1}^N$  represents the set of angular frequencies associated with each mode. Considering the bosonic nature of photons,  $\hat{a}$  and  $\hat{a}^\dagger$  are respectively the *annihilation* and *creation operators*, with commutation relations

$$[\hat{a}_k, \hat{a}_{k'}] = [\hat{a}_k^\dagger, \hat{a}_{k'}^\dagger] = 0, \quad [\hat{a}_k, \hat{a}_{k'}^\dagger] = \delta_{kk'}. \quad (2.16)$$

The corresponding *quadrature operators* for each mode are defined as

$$\hat{x}_k := \frac{1}{\sqrt{2}}(\hat{a}_k^\dagger + \hat{a}_k), \quad \hat{p}_k := \frac{i}{\sqrt{2}}(\hat{a}_k^\dagger - \hat{a}_k). \quad (2.17)$$

## Energy eigenstates

The eigenstates  $|n_k\rangle$ , with eigenvalues  $\hbar\omega_k(n_k + \frac{1}{2})$ , where  $n_k$  is an integer ( $n_k = 0, 1, 2, \dots, \infty$ ), of the Hamiltonian (2.15) are known as *Fock states*. They are eigenstates of the number operator  $N_k = \hat{a}_k^\dagger \hat{a}_k$

$$\hat{a}_k^\dagger \hat{a}_k |n_k\rangle = n_k |n_k\rangle . \quad (2.18)$$

The *vacuum state* of the field mode is defined by

$$\hat{a}_k |0\rangle = 0 \quad (2.19)$$

and the state vectors for the higher excited states are given by

$$|n_k\rangle = \frac{(\hat{a}_k^\dagger)^{n_k}}{(n_k!)^{1/2}} |0\rangle , \quad n_k = 0, 1, 2, \dots, \infty . \quad (2.20)$$

The Fock space is an orthogonal and complete set of basis vectors for a Hilbert space and is a very useful representation for systems where the number of photons is not too large.

## 2.2.2 Coherent states

*Coherent states* are states belonging to a complete basis of the Hilbert space of a quantized electromagnetic field, with an indefinite number of photons. Notably, they are the quantum representation of the light emitted by a laser source high above threshold, such as those employed in our experiments. These are quantum states that saturate Heisenberg's uncertainty principle. Hence, they are usually addressed as classical-like states. Mathematically, they are generated by applying the unitary *Displacement operator*

$$D(\alpha) = \exp(\alpha \hat{a}^\dagger - \alpha^* \hat{a}) , \quad (2.21)$$

with  $\alpha$  an arbitrary complex number, on the vacuum state

$$|\alpha\rangle = D(\alpha) |0\rangle . \quad (2.22)$$

Coherent states possess several notable properties that are crucial in quantum information processing. Firstly, they are eigenstates of the annihilation operator  $\hat{a}$ , satisfying the relation

$$\hat{a} |\alpha\rangle = \alpha |\alpha\rangle . \quad (2.23)$$

They can be represented as a superposition of all Fock states

$$|\alpha\rangle = e^{-|\alpha|^2/2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle . \quad (2.24)$$

Consequently, the probability distribution of the number of photons in the state is Poissonian

$$P(n) = |\langle n|\alpha\rangle|^2 = \frac{e^{-\mu} \mu^n}{\sqrt{n!}} \quad (2.25)$$



with the mean photon number  $\mu = \langle \alpha | \hat{a}^\dagger \hat{a} | \alpha \rangle = |\alpha|^2$  and variance  $(\Delta\mu)^2 = |\alpha|^2$ . Furthermore, coherent states form a complete set of states, where the completeness relation for these states is expressed as

$$\frac{1}{\pi} \int |\alpha\rangle \langle \alpha| d^2\alpha = \mathbb{1} . \quad (2.26)$$

For two coherent states  $|\alpha\rangle$  and  $|\beta\rangle$ , the scalar product is given by

$$|\langle \beta | \alpha \rangle| = e^{-\frac{|\alpha - \beta|^2}{2}} . \quad (2.27)$$

This indicates that while coherent states are normalized, that is,  $|\langle \alpha | \alpha \rangle| = 1$ , they differ from Fock states in that they are not orthogonal, as  $|\langle \beta | \alpha \rangle| \neq 0$ . This lack of orthogonality means it is impossible to perfectly distinguish between different coherent states, which is a crucial property for their application in quantum cryptography.

### Coherent state mapping

Let's consider a simple, yet quite general, protocol where Alice prepares an  $n$ -dimensional quantum state

$$|\psi\rangle = \sum_{k=1}^n \lambda_k |k\rangle \quad (2.28)$$

and sends it to a second party, Bob, which applies a unitary transformation and performs a projective measurement on the canonical basis. The pure state  $|\psi\rangle$  can be physically implemented by a single-photon state in superposition over  $n$  modes

$$\hat{a}_\psi^\dagger |0\rangle = \sum_{k=1}^n \lambda_k |1_k\rangle , \quad (2.29)$$

where  $\hat{a}_\psi^\dagger := \sum_{k=1}^n \lambda_k \hat{a}_k^\dagger$  for a collection of creation operators  $\{\hat{a}_1, \hat{a}_2, \dots, \hat{a}_n\}$  corresponding to  $n$  optical modes, and where  $|1_k\rangle$  is the state of a single photon in the  $k$ -th mode.

However, motivated by the difficulty in implementing quantum protocols based on single-photon encoding, an alternative mapping of such protocols was introduced [63], where, instead of the state in Eq. (2.28), one simply implements a sequence of coherent states over  $n$  optical modes

$$|\alpha, \psi\rangle := \bigotimes_{k=1}^n |\alpha \lambda_k\rangle_k . \quad (2.30)$$

The free parameter  $\alpha$  fixes the average number of photons across all the  $n$  optical modes. In particular, the probability distribution of the number of photons in each mode is equivalent to the one obtained by performing the same measurement on many copies of the single-photon state of Eq. (2.28) where the number of copies is drawn from a Poisson distribution with mean  $|\alpha|^2$ .

As we shall see in the next chapters, in this thesis we are interested in quantifying the amount of transmitted information in a given quantum communication protocol. Typically, this is based on counting the number of employed qubits. However, when a protocol uses

physical systems distinct from qubits, one can assess the transmitted information by determining the minimum number of qubits necessary, in principle, to match the protocol's performance. In general, the communication cost  $C$  of a quantum protocol is defined as

$$C = \log[\dim(\mathcal{H})], \quad (2.31)$$

where  $\mathcal{H}$  is the smallest Hilbert space containing all the states that can be sent during the execution of the protocol. While the size of the Hilbert space is easy to calculate in a single-photon protocol, this is more tricky in a coherent-state protocol. Since distinct coherent states are linearly independent, one would need a large Hilbert space to contain all the possible states involved in a protocol. However, it has been proven in [63] that they effectively occupy a Hilbert state of dimension comparable to the single-photon version.

**Theorem 2.2.1.** *For any state  $|\psi\rangle$  in a Hilbert space of dimension  $n$  and for any  $\epsilon > 0$ , there exists a Hilbert space  $H_\alpha$  of dimension  $n_\alpha$  such that*

$$\langle \alpha, \psi | P_{\mathcal{H}_\alpha} | \alpha, \psi \rangle \geq 1 - \epsilon, \quad (2.32)$$

$$\log n_\alpha = \mathcal{O}(\log n), \quad (2.33)$$

and where  $P_{\mathcal{H}_\alpha}$  is the projector onto  $\mathcal{H}_\alpha$ .

### 2.2.3 Coherent detection

Here we describe the methods for measuring the quadrature components of a coherent state. This is usually called *coherent detection* since it requires combining the signal state with a strong reference signal called a Local Oscillator (LO). Coherent detection can be divided into two types of measurements: *homodyne detection*, where only a single quadrature is measured, and *heterodyne detection*, where both quadratures are measured.

The homodyne detection method is represented in Figure 2.1, where the signal mode, denoted by  $S$ , is combined with the LO through a 50/50 beam splitter. The output modes  $+$  and  $-$  of the beam splitter are then measured with two detectors, where the photon number operators for each output mode can be written as

$$\hat{n}_+ = \frac{1}{2}(\hat{a}_S^\dagger + \hat{a}_{\text{LO}}^\dagger)(\hat{a}_S + \hat{a}_{\text{LO}}), \quad (2.34)$$

$$\hat{n}_- = \frac{1}{2}(-\hat{a}_S^\dagger + \hat{a}_{\text{LO}}^\dagger)(-\hat{a}_S + \hat{a}_{\text{LO}}). \quad (2.35)$$

The operator  $\hat{I}_\Delta$ , representing the difference in photocurrents, is then proportional to

$$\hat{I}_\Delta \propto \hat{n}_+ - \hat{n}_- \quad (2.36)$$

$$\propto \hat{a}_S^\dagger \hat{a}_{\text{LO}} + \hat{a}_{\text{LO}}^\dagger \hat{a}_S, \quad (2.37)$$

where the prefactors are determined by the properties of the detectors. Given that the LO is an intense classical field with energy levels significantly exceeding a single quantum unit. This allows us to replace the operators  $\hat{a}_{\text{LO}}$  and  $\hat{a}_{\text{LO}}^\dagger$  with the classical fields  $E_{\text{LO}} e^{\pm i\theta_{\text{LO}}}$ ,

where  $\theta_{\text{LO}}$  represents the phase of the LO. When the signal state is a coherent state  $|\alpha_s\rangle$  the expected value of the operator  $\hat{I}_\Delta$  can thus be described as

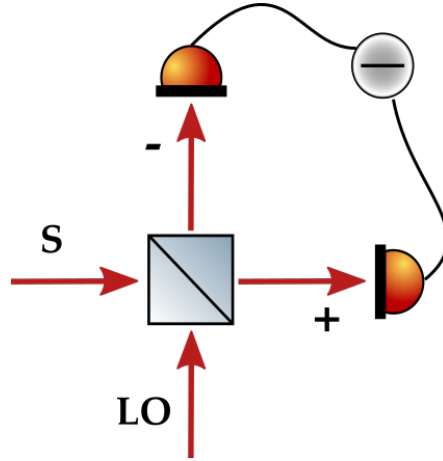
$$\mathbb{E}[\hat{I}_\Delta] \propto E_{\text{LO}} \langle \alpha_S | \hat{a}_S^\dagger e^{i\theta_{\text{LO}}} + \hat{a}_S e^{-i\theta_{\text{LO}}} | \alpha_S \rangle \quad (2.38)$$

$$\propto E_{\text{LO}} \langle \alpha_S | (\hat{x} - i\hat{p}) e^{i\theta_{\text{LO}}} + (\hat{x} + i\hat{p}) e^{-i\theta_{\text{LO}}} | \alpha_S \rangle \quad (2.39)$$

$$\propto E_{\text{LO}} \langle \alpha_S | \hat{x} (e^{i\theta_{\text{LO}}} + e^{-i\theta_{\text{LO}}}) + i\hat{p} (e^{-i\theta_{\text{LO}}} - e^{i\theta_{\text{LO}}}) | \alpha_S \rangle \quad (2.40)$$

$$\propto E_{\text{LO}} (\mathbb{E}[\hat{x}_S] \cos \theta_{\text{LO}} + \mathbb{E}[\hat{p}_S] \sin \theta_{\text{LO}}), \quad (2.41)$$

where in the second line we used the fact that  $\hat{a}_S = \frac{\hat{x}_S + i\hat{p}_S}{2}$  and  $\hat{a}_S^\dagger = \frac{\hat{x}_S - i\hat{p}_S}{2}$ , while in the fourth line we used the trigonometric formulas of the sine and cosine. Therefore by selecting  $\theta_{\text{LO}} = 0, \pi, 2\pi, \dots$ , we can measure the quadrature  $x_s$ , whereas for  $\theta_{\text{LO}} = \frac{\pi}{2}, \frac{3\pi}{2}, \dots$ , we measure the quadrature  $p_s$ .



**Figure 2.1:** Homodyne detection scheme. The signal mode is combined with a strong laser using a 50/50 beamsplitter. The light intensity at each output of the beamsplitter is recorded and the difference between these measurements forms the homodyne detection.

Moreover, we define the *shot noise*  $N_0$  as the variance observed in the quadrature measurements when the signal path is blocked. This represents the inherent noise level of the measurement system, capturing only the noise contributions intrinsic to the detector and the local oscillator. This usually acts as the standard unit for calibration in continuous-variable quantum protocols. Similarly, a heterodyne measurement consists of directing the input signal through a 50/50 beam splitter and performing a double homodyne detection, with one measurement in each output path [96].

## 2.3 Information theory

We will now introduce key concepts from both classical and quantum information theory. Our goal is to provide the necessary tools to measure and understand the information exchanged between Alice and Bob in communication protocols, such as Quantum Key Distribution (QKD), and also to evaluate the amount of information that might be intercepted by an eavesdropper. We refer to [97] for a more in-depth analysis.

### 2.3.1 Classical information theory

In the context of information theory, the concept of entropy was first introduced by Shannon in his groundbreaking paper [98]. Driven by various questions related to information theory, his search for a natural measure of uncertainty for a random variable resulted in the formulation of what is now known as *Shannon entropy*.

**Definition 2.3.1** (Shannon entropy). *Let  $X$  be a random variable distributed over a finite set  $\mathcal{X}$  according to the probability distribution  $P_X$ . Then, the Shannon entropy of  $X$  is*

$$H(X) = - \sum_{x \in \mathcal{X}} P_X(x) \log P_X(x), \quad (2.42)$$

where we also define  $0 \log(0) := 0$ .

Another interesting quantity is the *self-information*, or surprisal, symbolized by  $S$ . It is a function that maps events from the set  $\mathcal{X}$  to  $\mathbb{R} \cup \{-\infty\}$ , defined as

$$S(x) := - \log P_X(x). \quad (2.43)$$

Shannon entropy can be seen as the expected value  $\mathbb{E}[S]$  of the self-information. The latter measures somehow the level of surprise or unexpectedness an observer experiences when an event  $x$  occurs. The function  $-\log(p)$  decreases monotonically, dropping to zero at  $p = 1$  and approaching infinity as  $p \rightarrow 0$ . Thus, events that are certain do not contribute to surprisal, while those deemed impossible are linked with infinite surprisal. Building on Shannon's work, in [99] Rényi proposed a new set of useful entropy definitions that can capture more than the average surprisal.

**Definition 2.3.2** (Rényi entropies). *Let  $X$  be a random variable distributed over a finite set  $\mathcal{X}$  according to the probability distribution  $P_X$  and Let  $\alpha \in [0, 1) \cup (1, \infty)$ . Then, the  $\alpha$ -Rényi entropy of  $X$  is defined as*

$$H_\alpha(X) := \frac{1}{1 - \alpha} \log \sum_{x \in \mathcal{X}} P_X(x)^\alpha, \quad (2.44)$$

Additionally, the case  $\alpha = 0$  and the limiting cases are defined as

- i)  $H_0(X) := \log |\mathcal{X}|$ ,
- ii)  $H_1(X) := H(X)$ ,
- iii)  $H_\infty(X) := \min_{x \in \mathcal{X}} (-\log P_X(x))$ .

The measures  $H_\infty$  and  $H_0$  are known as the *min-entropy* and the *max-entropy*, respectively, and we denote them by  $H_{\min}$  and  $H_{\max}$ . In particular, we have that

$$H_{\max}(X) \geq H(X) \geq H_{\min}(X). \quad (2.45)$$

Furthermore, we can quantify the amount of information shared between two random variables  $X$  and  $Y$ , with distribution  $P_{XY} \in \Delta(\mathcal{X} \times \mathcal{Y})$ <sup>1</sup> and marginal distributions  $P_X$  and  $P_Y$  respectively, by means of the *mutual information*

$$I(X : Y) := H(X) - H(X|Y) , \quad (2.46)$$

where  $H(X|Y) := -\sum_{x,y} P_{XY}(x,y) \log\left(\frac{P_{XY}(x,y)}{P_X(x)}\right)$  is the *conditional entropy*.

### 2.3.2 Quantum information theory

Now we introduce a generalization of Shannon entropy for quantum states, called the *von Neumann entropy*. The von Neumann entropy of  $\rho \in \mathcal{D}(\mathcal{H}_A)$  is

$$H(A)_\rho := -\text{Tr}[\rho \log(\rho)]. \quad (2.47)$$

One can notice that by considering a classical state we recover back the Shannon entropy. For a bipartite state  $\rho_{AB} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_B)$ , we define the *conditional von Neumann entropy* of system  $A$  given system  $B$  when the joint system is in the state  $\rho_{AB}$  by  $H(A|B)_\rho := H(AB)_\rho - H(B)_\rho$ . We can finally define the *quantum mutual information* as

$$I(A : B)_\rho := H(A)_\rho - H(A|B)_\rho \quad (2.48)$$

From this point forward, we will omit the state subscript when the state is evident from the context.

Notably, the quantum mutual information of a classical-quantum state  $\rho_{AQ}$  is an upper bound of the amount of classical information that an adversary can extract about the classical system  $A$  from measuring the quantum system  $Q$ .

**Theorem 2.3.1** (Holevo's Theorem). *Given a cq-state  $\rho_{AQ} = \sum_{a \in \mathcal{A}} P_A(a) |a\rangle\langle a| \otimes \rho_Q^{(a)}$ , then for any measurement  $\Pi : \mathcal{M} \rightarrow \mathcal{P}(\mathcal{H}_Q)$  on the quantum system  $Q$ , the mutual information between the classical input  $A$  and measurement outcome  $M$  is bounded by*

$$I(A : M) \leq I(A : Q) . \quad (2.49)$$

Another useful quantity in quantum cryptography is the probability of guessing the random variable  $A$  for an adversary holding a quantum system  $Q$ , given by

$$P_{\text{guess}}(A|Q) := \max_{\Pi} \sum_{a \in \mathcal{A}} P_A(a) \text{Tr}[\Pi(a) \rho_Q^{(a)}] , \quad (2.50)$$

where we maximize over all POVMs  $\Pi : \mathcal{A} \rightarrow \mathcal{P}(\mathcal{H}_Q)$ . From Eq. (2.50) we can define the *conditional min-entropy* of a classical system given quantum side information, in its operational formulation [100], as

$$H_{\min}(A|Q) := -\log(P_{\text{guess}}(A|Q)) . \quad (2.51)$$

Moreover, the quantum system  $Q$  could be formed by different subsystems, say  $Q_1$  and  $Q_2$ , where  $Q_2$  might not be correlated with the classical variable  $A$ . In this case one can prove the following lemma.

---

<sup>1</sup>Let  $\mathcal{S}$  be a set. We use  $\Delta(\mathcal{S})$  to denote the family of all probability distributions on  $\mathcal{S}$ .

**Lemma 2.3.1.** *Let  $\rho_{AQ_1Q_2} = \sum_{a \in \mathcal{A}} P_A(a) |a\rangle\langle a| \otimes \rho_{Q_1}^{(a)} \otimes \rho_{Q_2}$  be a cq-q-state<sup>2</sup>. Then*

$$P_{\text{guess}}(A|Q_1Q_2) = P_{\text{guess}}(A|Q_1). \quad (2.52)$$

*Proof.* Clearly  $P_{\text{guess}}(A|Q_1Q_2) \geq P_{\text{guess}}(A|Q_1)$ , so we show the opposite inequality. We have

$$P_{\text{guess}}(A|Q_1Q_2) = \max_{\Pi} \sum_{a \in \mathcal{A}} P_A(a) \text{Tr}[\Pi(a)(\rho_{Q_1}^{(a)} \otimes \rho_{Q_2})] \quad (2.53)$$

and

$$P_{\text{guess}}(A|Q_1) = \max_{\tilde{\Pi}} \sum_{a \in \mathcal{A}} P_A(a) \text{Tr}[\tilde{\Pi}(a)\rho_{Q_1}^{(a)}]. \quad (2.54)$$

Take any POVM  $\Pi$  acting on the joint system  $Q_1Q_2$ , which is a feasible point for the optimization defining  $P_{\text{guess}}(A|Q_1Q_2)$ . Now define

$$\tilde{\Pi}(a) := \text{Tr}_{Q_2}[(\mathbf{1}_{Q_1} \otimes \sqrt{\rho_{Q_2}})\Pi(a)(\mathbf{1}_{Q_1} \otimes \sqrt{\rho_{Q_2}})]. \quad (2.55)$$

This defines a POVM on  $Q_1$ . To see this note it is positive-semidefinite as  $(\mathbf{1}_{Q_1} \otimes \sqrt{\rho_{Q_2}})\Pi(a)(\mathbf{1}_{Q_1} \otimes \sqrt{\rho_{Q_2}}) \in \mathcal{P}(\mathcal{H}_{Q_1} \otimes \mathcal{H}_{Q_2})$  and the partial trace is a CP map. Finally we have

$$\begin{aligned} \sum_{a \in \mathcal{A}} \tilde{\Pi}(a) &= \sum_{a \in \mathcal{A}} \text{Tr}_{Q_2}[(\mathbf{1}_{Q_1} \otimes \sqrt{\rho_{Q_2}})\Pi(a)(\mathbf{1}_{Q_1} \otimes \sqrt{\rho_{Q_2}})] \\ &= \text{Tr}_{Q_2}[\mathbf{1}_{Q_1} \otimes \rho_{Q_2}] = \mathbf{1}_{Q_1}. \end{aligned}$$

so  $\tilde{\Pi}$  forms a POVM on  $Q_1$ . Moreover, we have

$$\begin{aligned} \sum_{a \in \mathcal{A}} P_A(a) \text{Tr}[(\Pi(a)(\rho_{Q_1}^{(a)} \otimes \rho_{Q_2}))] &= \sum_{a \in \mathcal{A}} P_A(a) \text{Tr}[(\mathbf{1}_{Q_1} \otimes \sqrt{\rho_{Q_2}})\Pi(a)(\mathbf{1}_{Q_1} \otimes \sqrt{\rho_{Q_2}})(\rho_{Q_1}^{(a)} \otimes \mathbf{1}_{Q_2})] \\ &= \sum_{a \in \mathcal{A}} P_A(a) \text{Tr}[\tilde{\Pi}(a)\rho_{Q_1}^{(a)}]. \end{aligned}$$

Hence, we have  $P_{\text{guess}}(A|Q_1Q_2) \leq P_{\text{guess}}(A|Q_1)$ .  $\square$

A last important quantity in quantum cryptography is the  $\varepsilon$ -smooth conditional min-entropy. For any  $\varepsilon \geq 0$  and a given state cq-state  $\rho_{QE}$  the  $\varepsilon$ -smooth min-entropy,  $H_{\min}^\varepsilon$  is defined as the highest min-entropy among all states that are  $\varepsilon$ -close to  $\rho_{AQ}$

$$H_{\min}^\varepsilon(A|Q)_\rho := \sup_{\sigma \in B^\varepsilon(\rho)} H_{\min}(A|Q)_\sigma, \quad (2.56)$$

where  $B^\varepsilon(\rho)$  is the set of states within an  $\varepsilon$  distance from  $\rho$ , based on the purified distance, an upper bound of the trace distance (see [101] for details).

---

<sup>2</sup>A cq state represents a straightforward extension of a cq state, with a joint system that includes a classical system alongside two quantum systems.



# INTRODUCTION TO QUANTUM KEY DISTRIBUTION

## Contents

|            |   |           |
|------------|---|-----------|
| <b>3.1</b> | <b>Modern cryptography</b> . . . . .                      | <b>30</b> |
| 3.1.1      | Encryption schemes . . . . .                              | 30        |
| 3.1.2      | Basic principles in modern cryptography . . . . .         | 31        |
| <b>3.2</b> | <b>General QKD protocol</b> . . . . .                     | <b>32</b> |
| 3.2.1      | Structure of the protocol . . . . .                       | 33        |
| 3.2.2      | Foundational assumptions and trust requirements . . . . . | 34        |
| <b>3.3</b> | <b>Explicit protocols</b> . . . . .                       | <b>36</b> |
| 3.3.1      | Example 1: BB84 . . . . .                                 | 36        |
| 3.3.2      | Example 2: GG02 protocol . . . . .                        | 37        |
| <b>3.4</b> | <b>Secure quantum key distribution</b> . . . . .          | <b>39</b> |
| 3.4.1      | Security definitions . . . . .                            | 39        |
| 3.4.2      | Security analysis . . . . .                               | 40        |
| <b>3.5</b> | <b>Practical quantum key distribution</b> . . . . .       | <b>43</b> |
| 3.5.1      | Experimental implementations . . . . .                    | 43        |
| 3.5.2      | Quantum hacking . . . . .                                 | 44        |

In this chapter, after a brief introduction to modern cryptography, we cover the process of distributing secret keys through quantum communication. We'll begin by explaining what security means in this quantum context and how to quantify the adversary's knowledge of the key. Following this, we'll transition into examining how these protocols are applied in real-world settings, discussing both their implementation and the practical security challenges that emerge.



## 3.1 Modern cryptography

The 20th century has been a turning point in the history of cryptography. With the advent of the digital revolution, cryptography transitioned from the realm of manual ciphers and mechanical devices to the world of algorithms and computers. This section aims to provide, in a quite informal way, a short overview of how to guarantee secure communication with modern cryptography. We refer to [102] for a more extensive and formal overview.

### 3.1.1 Encryption schemes

Historically, cryptography focused on providing secure communication between two parties who had previously shared some information. This scenario is referred to as *symmetric* or *secret-key cryptography*. In this cryptographic method, a "key" acts as a shared secret between the communicating parties that can be used to transform the original message, called *plaintext*, into an encrypted message, called *ciphertext*, and vice versa. A bit more formally, a *private-key encryption scheme*, or cipher, consists first of a *key-generation algorithm*, followed by an *encryption algorithm*, and finally by a *decryption algorithm*. These algorithms are defined as follows:

1. The key-generation algorithm, denoted as **Gen**, is a probabilistic algorithm that outputs a key  $k$ , chosen according to a specific distribution defined by the scheme.
2. The encryption algorithm, denoted as **Enc**, takes as input a key  $k$  and a plaintext message  $m$ , and outputs a ciphertext  $c$ . The encryption of plaintext  $m$  using key  $k$  is represented as  $\text{Enc}_k(m)$ .
3. The decryption algorithm, denoted as **Dec**, takes as input a key  $k$  and a ciphertext  $c$ , and outputs a plaintext message  $m$ . The decryption of ciphertext  $c$  using key  $k$  is represented as  $\text{Dec}_k(c)$ .

It is clear that if an eavesdropper obtains the decryption key  $k$  and is aware of the decryption algorithm **Dec**, then they can intercept and decrypt all messages between the communicating parties. Therefore, it's crucial for the parties to keep  $k$  confidential. This raises the question: should **Dec** and, by extension, the entire set of cryptographic algorithms (**Gen** and **Enc**) also be kept secret? As explained by *Kerckhoffs' principle*, the answer is negative. In other words, the security of the scheme should rely solely on the secrecy of the key.

Today, Kerckhoffs' principle goes beyond simply suggesting that the security of a cryptographic system shouldn't rest on keeping its algorithms secret. It actively advocates for these algorithms to be public. This openness allows for a broader community to scrutinize and test the cryptographic designs, which not only can strengthen the security of these systems by identifying and addressing vulnerabilities but also pave the way for creating standardized, robust cryptographic practices.

## Public-key cryptography

One of symmetric cryptography's main challenges lies in the distribution of the secret keys between parties. Clearly, they cannot be directly exchanged through an insecure communication channel, since an eavesdropping adversary could easily intercept them and copy them. The initial methods used for key distribution were primarily physical and logistical rather than based on algorithms with provable security. For instance, the most straightforward method simply consisted of a direct physical exchange, where the parties would meet in person to share the secret key or send it via a *trusted courier*. However, this method was logistically challenging, especially for geographically distant parties, where excluding the possibility of interceptions along the way was virtually impossible.

Luckily, the 1970s brought forth a revolutionary solution: *asymmetric* or *public-key cryptography*. Pioneered by Whitfield Diffie and Martin Hellman in their paper called "New Directions in Cryptography" [9], this method introduced a fundamentally different way of looking at cryptography, introducing the concept of *asymmetric cryptography* or *public-key cryptography*. Unlike symmetric cryptography, in asymmetric cryptography, there are two separate keys: a *public key* for encryption and a *private key* for decryption. Anyone could encrypt a message using a public key, but only the recipient, who holds the corresponding private key, could decrypt it.

While this method allows much more flexibility compared to symmetric encryption schemes, allowing safe communication across open networks, it is significantly less efficient in terms of communication speed. A nice solution is therefore not to directly use asymmetric cryptography for secure communication, but to use it as a secure key exchange protocol, in combination with a symmetric encryption scheme. For instance, to encrypt a message  $m$ :

1. The sender encrypts a random secret key  $k$  with the receiver's public key to produce ciphertext  $c_1$ , enabling only the receiver to decrypt  $k$ .
2. The sender then encrypts the message  $m$  using  $k$  through symmetric encryption, resulting in ciphertext  $c_2$  which the receiver decrypts with  $k$ .

### 3.1.2 Basic principles in modern cryptography

Modern cryptography, regardless of its varied techniques or applications, is built upon a set of fundamental principles. These principles not only underscore the scientific rigor inherent in the field but also ensure that cryptographic practices are guided by a consistent and robust framework. In the following, we list the three main principles [102].

1. **Principle 1 — Exact security definitions.** When addressing any cryptographic problem the initial step is to establish a rigorous and clear definition of what constitutes security.
2. **Principle 2 — Reliance on precise assumptions.** If the security of a cryptographic mechanism depends on an unverified assumption, it is crucial to precisely articulate this assumption. Additionally, the assumption ought to be as minimal as possible.

- 3. Principle 3 — Rigorous proof of security.** Cryptographic mechanisms must be presented alongside a thorough proof of security. This proof should align with a security definition outlined in accordance with Principle 1. If any assumption is necessary, it should be identified following Principle 2.

Regarding a standard definition of security, one usually requires that an adversary should not be able to derive any information, even if only partial, about the plaintext from the ciphertext. This is commonly referred to as *semantic security* [103]. Additionally, the security definition always includes the range of attacks an adversary might employ. These can vary from the basic *ciphertext-only attack*—where the adversary has access only to the ciphertext and attempts to infer the corresponding plaintext—to the more advanced *adaptive chosen-ciphertext attack*. Here, the attacker adaptively chooses multiple ciphertexts for decryption, then leverages the outcomes to decrypt a specific target ciphertext without directly querying the oracle about it.

With respect to the possible assumptions used in modern cryptography, the bedrock of both symmetric and asymmetric cryptographic protocols is their reliance on *computational hardness assumptions*. Informally, they refer to the assumption that a particular computational problem cannot be solved efficiently (i.e. in polynomial time) using any known algorithm, given the current state of technology. While this is a standard approach in modern cryptographic protocols, it's important to stress that these are assumptions, not proven facts. While many problems are believed to be hard based on extensive empirical evidence and theoretical analysis, it's still theoretically possible that efficient solutions could be discovered in the future.

This brief introduction to modern cryptography concludes here. In the rest of this chapter, we will focus on QKD, analyzing it under the lens of the three principles outlined earlier.

## 3.2 General QKD protocol

QKD is a quantum communication task that enables two parties, commonly referred to as Alice and Bob, to create a shared secret key. At its core, a QKD protocol aims for Alice and Bob to produce identical keys that remain unknown to any malicious eavesdropper, commonly known as Eve. Before presenting the various steps of a QKD protocol, let's introduce the two communication channels used.

- **Classical Authenticated Channel (CAC):** a classical communication channel with added security that ensures messages sent between Alice and Bob are authenticated and unchanged. While the channel does not conceal the content from Eve, who can read all messages, it guarantees that Eve cannot forge or modify any messages.
- **Quantum channel:** a channel that allows the transmission of quantum information between Alice and Bob. Eve has the capability to fully interact with this channel, potentially affecting the transmitted quantum information.

### 3.2.1 Structure of the protocol

The different steps of a QKD protocol can always be partitioned into two phases. The first one is the *quantum phase*, where Alice prepares the quantum states according to some random variables in her laboratory and sends them to Bob, who subsequently measures them. This is called the Prepare and Measure (PM) scheme<sup>1</sup>. Crucially, both Alice and Bob depend on a trusted Random Number Generator (RNG) to provide the randomness essential for conducting this phase, with the following steps being repeated several times.

1. **Quantum communication:** Based on a classical random variable extracted by a RNG, Alice encodes a quantum state and transmits it to Bob.
2. **Measurement:** Bob then randomly selects one of several possible measurements to perform on the quantum state and extracts a classical outcome.

In the subsequent *classical phase*, Alice and Bob utilize the CAC to perform classical post-processing on their classical variables to generate a pair of identical and secret bit strings, known as *cryptographic keys*. Specifically, they execute the following steps.

3. **Sifting:** They agree on a subset of samples they keep, and discard the rest.
4. **Parameter estimation:** Alice and Bob randomly select a number of rounds and announce their outcomes. This comparison allows them to accurately estimate relevant parameters such as the error rate or the transmittance of the channel, from which they can bound the amount of information an eavesdropper might have acquired. Should the estimated parameters be above some predetermined thresholds, they abort the protocol. If this doesn't happen, the remaining unrevealed variables can be mapped to two partially correlated bit strings, known as *raw keys*.
5. **Error correction:** Alice and Bob now apply a classical error correction protocol [104] to transform their partially correlated strings into identical ones. In this thesis, we will only consider *one-way error correction* where Alice helps Bob (or vice-versa) correct his errors.
6. **Privacy amplification:** In the final step, Alice and Bob use a privacy amplification technique [105], based on a seeded randomness extractor, to eliminate any knowledge Eve might have about the key, resulting in a shorter but secure final key.

After finishing the protocol, there are two main outcomes: if Eve has learned too much information about the key, the protocol aborts. If not, they end up with matching secret keys they can use to send encrypted messages.

---

<sup>1</sup>It turns out that an equivalent Entangled-Based (EB) protocol can always be formulated. In this protocol, an external source distributes entangled states to both Alice and Bob, who then measure them. However, in this thesis we will focus only on PM schemes.

### 3.2.2 Foundational assumptions and trust requirements

Having analyzed the general steps in a QKD protocol, it's essential to clarify the assumptions required to formally prove security. While QKD protocols are frequently touted as offering "unconditional security", this doesn't imply they are assumption-free. Instead, this term contrasts with traditional classical cryptography, highlighting that QKD's security doesn't hinge on any assumptions about the computational capabilities of potential eavesdroppers. Although most of the assumptions ultimately depend on the type of QKD protocol, certain foundational assumptions are universally necessary across all protocols.

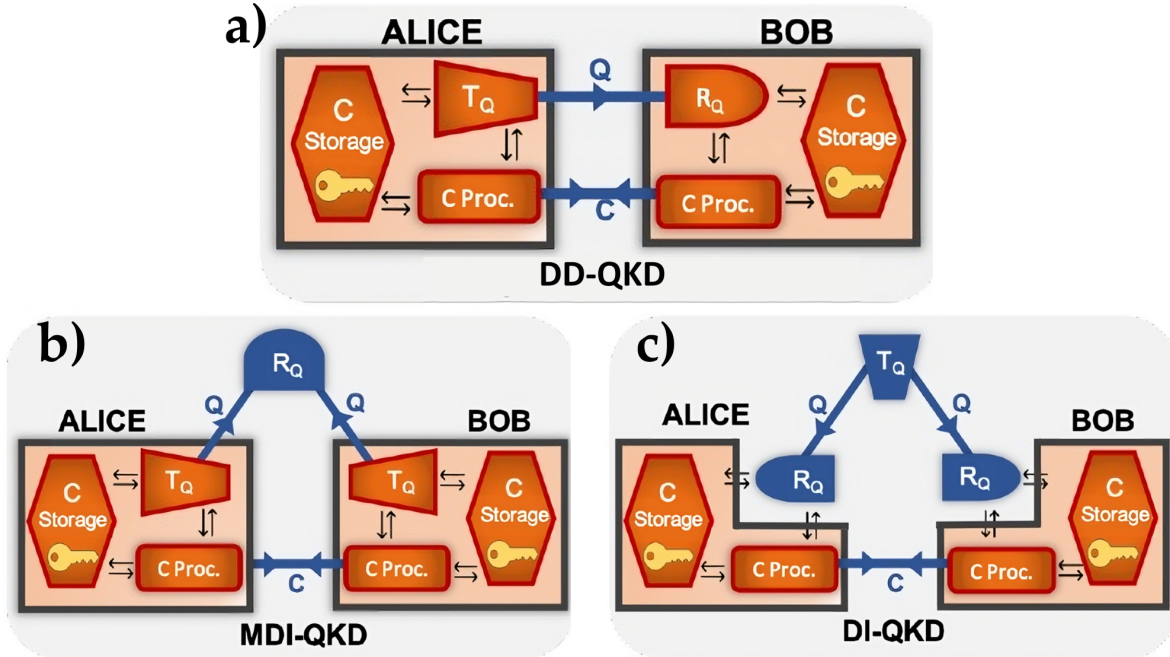
#### Foundational assumptions for QKD [107]

1. **Correctness of quantum theory.** We assume that quantum theory accurately predicts outcomes of physical phenomena. This assumption is strongly supported by a vast array of experimental evidence confirming the reliability of quantum mechanics' predictions.
2. **Existence of free randomness.** The protocol assumes the ability to make truly random number generators. It has been shown in [106] that the existence of free randomness and the correctness of quantum theory guarantee its completeness, i.e. there's no extension of the theory that can provide improved predictions. Notably, an eavesdropper cannot obtain any more information on the generated key than what is predicted by quantum theory.
3. **No device leaks unauthorized information.** We assume that the devices employed in the protocol do not leak sensitive information beyond what is outlined in the protocol. This includes, for example, ensuring that raw keys stored on classical computers are not accessible externally.

Beyond the foundational assumptions discussed, numerous other assumptions regarding the protocol's implementation can be made. The more assumptions introduced, the simpler the security proof becomes, since each known detail about the devices narrows the range of potential eavesdropper attacks. For instance, assuming devices are leak-proof against unauthorized information eliminates the need to consider such leaks in the security analysis. In the literature, we divide the QKD protocols into three main categories based on the assumptions made: Device-Dependent Quantum Key Distribution (DD-QKD), Measurement-Device-Independent Quantum Key Distribution (MDI-QKD) and Device-Independent Quantum Key Distribution (DI-QKD). A pictorial representation of the assumptions made for each category is given in Figure 3.1.

In DD-QKD protocols, all devices within Alice and Bob's labs are considered trusted and shielded to prevent any information leakage. However, as we will see in Section 3.5.2 and, more in detail, in Chapter 4, guaranteeing that the QKD devices behave according to the ideal model is often challenging, opening the way to dangerous side-channel attacks.

A breakthrough in the direction of closing security loopholes at the receiver side was the proposal of MDI-QKD [82]. In this security framework Alice and Bob each send quantum states to a central node, which is in charge of performing the measurements. Here, it is



**Figure 3.1:** Hardware trust requirements for QKD protocols. Hardware components in orange are those that need to be reliable and work as specified for the security proof. In contrast, the blue elements are those where no specific assumptions about their internal functioning and specifications are made. The shield, depicted with a black border, ensures no information leakage from these devices. We use abbreviations such as  $T_Q$  for the quantum transmitter,  $R_Q$  for the quantum receiver, C for classical, and Q for quantum. The trust models are depicted as follows: **a)** for conventional DD-QKD, **b)** for MDI-QKD, and **c)** for DI-QKD. Figure adapted from [78].

assumed that they can flawlessly generate these quantum states within their shielded laboratories, while the central receiving device operates under no such trust assumptions. The receiver, in fact, could potentially be under the control of an eavesdropper, and its integrity is not assumed.

In the pursuit of reducing trust assumptions to the bare minimum, DI-QKD [108] emerges as an ideal solution because it eliminates the need to characterize both the quantum transmitter and receiver. Nonetheless, this approach necessitates the distribution of entanglement between distant observers, who must also be equipped to carry out rapid, random measurements with extremely high efficiency [109]. Consequently, the complexity involved in implementing DI-QKD might be excessively challenging for practical implementations. In the rest of this chapter, we will focus only on DD-QKD protocols.

### 3.3 Explicit protocols

Before reviewing specific protocols, it's important to outline two primary categories defined by their encoding and decoding techniques. The first type of protocol, called Discrete-Variable Quantum Key Distribution (DV-QKD), utilizes single photons as the carriers of information, employing, for instance, varying polarization directions to represent different qubit states. However, in real-world applications, perfect single-photon sources and detectors are not available, which could dramatically impact the security of these protocols if they are not integrated into the security analysis, as discussed later in Section 3.5.2.

This limitation has prompted the development of protocols that encode information in continuous properties of light, such as the electromagnetic field's quadrature components, leading to measurement results with continuous values. These are known as Continuous-Variable Quantum Key Distribution (CV-QKD) protocols [110]. A remarkable advantage of these protocols is that they can be implemented using standard telecommunications technology, the same as what's employed in classical optical communication. However, encoding information in a quantum state within infinite-dimensional Hilbert spaces introduces unique challenges for security analysis in such protocols. This is because many information-theoretic methods are tailored to DV-QKD and are difficult to extend to continuous variables.

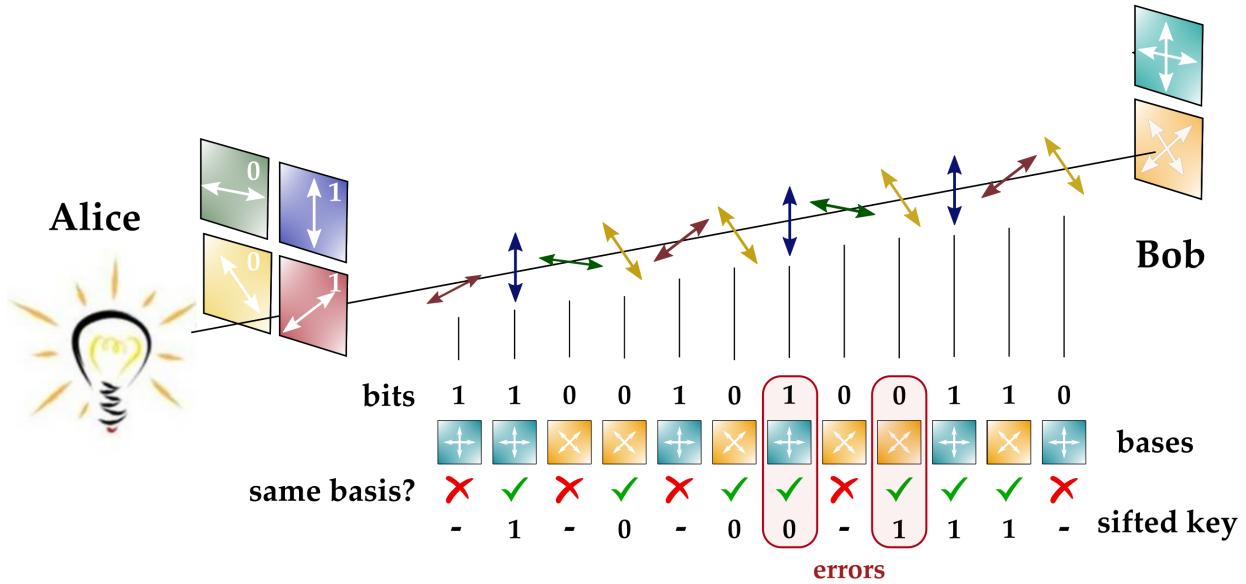
#### 3.3.1 Example 1: BB84

In the 1970s, the entire field of quantum cryptography was only based on one unpublished paper by Wiesner on a quantum money scheme [111]. This protocol used qubits in the states  $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$  to create and verify banknotes, where their unforgeability was based on the no-cloning theorem. While the protocol proposed was too simple and could not guarantee security, the idea of using the computational and Hadamard basis to encode classical information into a qubit inspired the first and arguably most famous QKD protocol, the Brassard-Bennet-1984 (BB84) protocol, named after its creators, Bennet and Brassard [1]. In the following, we give a detailed description of all the steps of the protocol.

1. **Quantum communication:** Alice first generates a uniformly random string  $\mathbf{a} = a_1, \dots, a_n \in \{0, 1\}^n$  and a basis string  $\boldsymbol{\theta} = \theta_1, \dots, \theta_n \in \{0, 1\}^n$ , where  $\theta_j = 0$  represents the computational basis and  $\theta_j = 1$  the Hadamard basis. Then, she encodes each bit  $a_j$  into the quantum state  $|a_j\rangle_{\theta_j} = H^{\theta_j} |a_j\rangle$ , with  $H$  the Hadamard matrix, and sends it to Bob.
2. **Measurement:** Bob chooses a different basis string  $\tilde{\boldsymbol{\theta}} = \tilde{\theta}_1, \dots, \tilde{\theta}_n \in \{0, 1\}^n$  uniformly at random. He then measures each  $j$ -th qubit received from Alice in the basis  $\tilde{\theta}_j$ , obtaining the outcomes  $\mathbf{b} = b_1, \dots, b_n \in \{0, 1\}^n$ .
3. **Sifting:** Let  $S = \{j | \theta_j = \tilde{\theta}_j\}$  denote the indices of the round in which Alice and Bob measured on the same basis. Since only those rounds provide correlated results, they discard the information for all rounds not in  $S$ . An illustration of the protocol up to this step is represented in Figure 3.2.

4. **Parameter estimation:** Alice reveals the substring  $\mathbf{a}_P$  of  $\mathbf{a}$  corresponding to the indices in a random subset  $P \subseteq S$  to Bob. He then reveals the corresponding substring  $\mathbf{b}_P$ . Their goal is to use this data to calculate the Quantum Bit Error Rate (QBER), which measures the fraction of quantum states that produced an incorrect measurement result out of the total sent by Alice. Mathematically, it is estimated as  $\text{QBER} = \frac{1}{|P|} |\{j \in P | a_j \neq b_j\}|$ . Finally, if the QBER exceeds some threshold<sup>2</sup> they abort the protocol, otherwise they set  $\mathbf{a}_{\text{remain}} = \mathbf{a}_{S \setminus P}$  and  $\mathbf{b}_{\text{remain}} = \mathbf{b}_{S \setminus P}$  respectively.

5-6 **Error correction and privacy amplification:** Alice sends some error-correcting information  $c$  across the CAC to Bob, who corrects the error in his string  $\mathbf{b}_{\text{remain}}$  to obtain a corrected string  $\tilde{\mathbf{b}}_{\text{remain}}$ . Finally, Alice and Bob perform privacy amplification to extract the cryptographic keys  $k_A$  and  $k_B$  respectively.



**Figure 3.2:** BB84 illustration. Here the computational basis is represented as  $\{\uparrow, \leftrightarrow\}$ , while the Hadamard basis is  $\{\nearrow, \searrow\}$ . In this example, even after sifting, some errors could still occur. This can be due to some external noise or due to a malicious eavesdropper. Figure inspired by [113].

### 3.3.2 Example 2: GG02 protocol

The Grosshans-Grangier-2002 (GG02) protocol [64], named again after its inventors, Grosshans and Grangier, was the first CV-QKD protocol to employ weak coherent states. In this protocol, Alice prepares a coherent state  $|\alpha\rangle$  for each transmission, where the state follows a complex Gaussian distribution with each quadrature characterized by a variance  $V_A$ . Bob then randomly selects which quadrature to measure using homodyne detection. Here to

<sup>2</sup>For the BB84 protocol the threshold is 11%, corresponding to the maximum error rate that we can tolerate when Eve is executing an optimal attack [112].



quantify the interaction of the eavesdropper on the quantum states they estimate the channel's transmission  $T$  and the so-called *excess noise*  $\xi$ . Notably, considering additive Gaussian noise, Bob's outcome will still be a Gaussian variable with variance

$$V_B = \eta T V_A + N_0 + \eta_b T \xi + \nu_{\text{ele}} . \quad (3.1)$$

This variance includes shot noise  $N_0$ , electronic noise of Bob  $\nu_{\text{ele}}$ , and Bob's efficiency  $\eta_b$ , all of which are pre-calibrated values, measured before launching the protocol. We now give a detailed description of all the steps of the protocol.

1. **Quantum communication:** Alice generates  $2n$  random variables from a normal distribution with zero mean and variance  $V_A$ :  $q_1, p_1, \dots, q_n, p_n \sim \mathcal{N}(0, V_A)$ . She then prepares and sends  $n$  coherent states  $|q_1 + ip_1\rangle, \dots, |q_n + ip_n\rangle$  to Bob through the quantum channel.
2. **Measurement:** Upon receiving each state, Bob randomly selects a quadrature,  $q$  or  $p$ , for homodyne measurement and obtains  $n$  classical outcomes  $\mathbf{b} = b_1, \dots, b_n \in \mathbb{R}^n$ .
3. **Sifting:** He informs Alice of his quadrature choices. Alice retains the corresponding data,  $q_i$  or  $p_i$ , as  $a_i$  for each state, obtaining the outcomes  $\mathbf{a} = a_1, \dots, a_n \in \mathbb{R}^n$ . Consequently, after sifting, Alice and Bob always share  $n$  pairs of correlated classical variables  $(a_1, b_1), \dots, (a_n, b_n)$ .
4. **Parameter estimation:** They select a random subset  $P$  of  $m$  indices<sup>3</sup>  $\{i_1, \dots, i_m\} \subset \{1, \dots, N\}$  and publicly disclose the associated data  $(a_{i_1}, b_{i_1}), \dots, (a_{i_m}, b_{i_m})$ . Using this data, they estimate the quantum channel's transmission  $T$  and excess noise  $\xi$ .
- 5-6. **Error correction and privacy amplification:** Alice and Bob then apply error correction methods [114], similar to those that are used in the telecom industry, to agree on a shared binary string  $z$ . An important detail is that they use a method called *reverse reconciliation*, meaning Bob is the one who sends the needed classical info  $c$  to Alice over the CAC. Finally, they perform standard privacy amplification to extract the identic cryptographic keys  $k_A$  and  $k_B$ , respectively.

The GG02 protocol was later improved to a *no-switching* version [115], where Bob performs heterodyne detection on both quadratures simultaneously. There are also several ways to potentially improve the performance of this protocol. For instance, opting for discrete modulation [116, 117] could simplify the post-processing steps, as opposed to using Gaussian modulation. Additionally, filtering out excessively noisy data through postselection [118] might also increase the overall performance.

---

<sup>3</sup>Note that, compared to BB84, the size of the subset  $P$  can be fixed a priori, since after the sifting Alice and Bob always end up with  $n$  random variables each.

## 3.4 Secure quantum key distribution

### 3.4.1 Security definitions

A quantum key distribution protocol consists of a sequence of steps executed by two honest participants, Alice and Bob, to satisfy two primary objectives by the end of the protocol.

- i) *Correctness*: the keys generated by Alice and Bob, denoted as  $K_A$  and  $K_B$ , must be identical, ensuring  $K_A = K_B$ .
- ii) *Secrecy*: only Alice and Bob should possess any knowledge of the generated key, ensuring its confidentiality.

Nevertheless, adhering strictly to these objectives can be impractical. Concerning correctness, the protocol must incorporate a mechanism for termination, allowing either party to abort the process. This is particularly crucial in scenarios where an adversary, such as Eve, may completely disrupt the communication channel. To accommodate the possibility of aborting, we introduce therefore a special symbol  $\perp$ : if either  $K_A = \perp$  or  $K_B = \perp$ , then the protocol has been aborted. Yet, this alone isn't sufficient. We must also account for a small probability, where the protocol could fail in a way that Alice and Bob cannot detect, preventing them from aborting as needed. Taking all of this in consideration, the concept of correctness in a key distribution protocol can be formally defined as follows.

**Definition 3.4.1** ( $\epsilon_{\text{cor}}$ -correctness). *A QKD protocol is  $\epsilon_{\text{cor}}$ -correct if the following holds. Let  $K_A$  and  $K_B$  denote the user's outcomes in the protocol. Then*

$$\text{Prob}(K_A \neq \perp \wedge K_B \neq \perp \wedge K_A \neq K_B) \leq \epsilon_{\text{cor}} . \quad (3.2)$$

Concerning the secrecy requirement, one can consider the joint state of Alice's key  $K_A$  in the classical system  $K$  and Eve's quantum system  $E$  as a cq-state  $\rho_{KE}$ . Ideally, in the absence of any information leakage to Eve, this joint state would be uncorrelated, that is

$$\rho_{KE}^{\text{ideal}} := \frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} |k\rangle\langle k| \otimes \rho_E , \quad (3.3)$$

where  $\mathcal{K}$  is the set of possible keys. Nonetheless, practical implementations need to allow for minor deviations, where the actual state  $\rho_{KE}^{\text{real}}$  approximates the ideal state  $\rho_{KE}^{\text{ideal}}$  within a small trace distance margin. Furthermore, as for the correctness of the protocol, we must account for the eventuality of abortion. The formal definition is, therefore, as follows.

**Definition 3.4.2** ( $\epsilon_{\text{sec}}$ -secrecy). *A QKD protocol is  $\epsilon_{\text{sec}}$ -secret if the following holds. Let  $\text{Pr}(\text{abort})$  denote the probability that either Alice or Bob returns  $\perp$ . Then*

$$(1 - \text{Pr}(\text{abort}))D(\rho_{KE}^{\text{real}}, \rho_{KE}^{\text{ideal}}) \leq \epsilon_{\text{sec}} , \quad (3.4)$$

where  $\rho_{KE}^{\text{real}}$  is the joint state of Alice's output  $K_A$  and the eavesdropper in an execution of the protocol and  $\rho_{KE}^{\text{ideal}} = \frac{1}{|\mathcal{K}|} \sum_{k \in \mathcal{K}} |k\rangle\langle k| \otimes \rho_E$ .

Finally, by combining these two definitions one gets the so-called  $\epsilon$ -security definition.

**Definition 3.4.3** ( $\epsilon$ -security). *A QKD protocol is  $\epsilon$ -secure, where  $\epsilon = \epsilon_{cor} + \epsilon_{sec}$ , if it is both  $\epsilon_{cor}$ -correct and  $\epsilon_{sec}$ -secret.*

Since this definition can be rewritten in terms of trace distance, this is also called the *trace distance criterion*. Notably, such criterion carries one crucial property: *composability* [119]. Informally, this means that if a key from an  $\epsilon$ -secure QKD protocol is used in an  $\epsilon'$ -secure task, composability ensures that the whole procedure is at least  $\epsilon + \epsilon'$ -secure.

One might naturally wonder, what then is the ideal value for the security parameter  $\epsilon$ ? Ideally, it should be as low as possible, since it indicates the likelihood of a protocol error going unnoticed. However, reducing this parameter generally leads to higher costs in the protocol implementation [107]. Commonly, the security parameter  $\epsilon$  for each generated key in QKD systems is set between  $10^{-6}$  and  $10^{-12}$ , balancing security with practicality and cost.

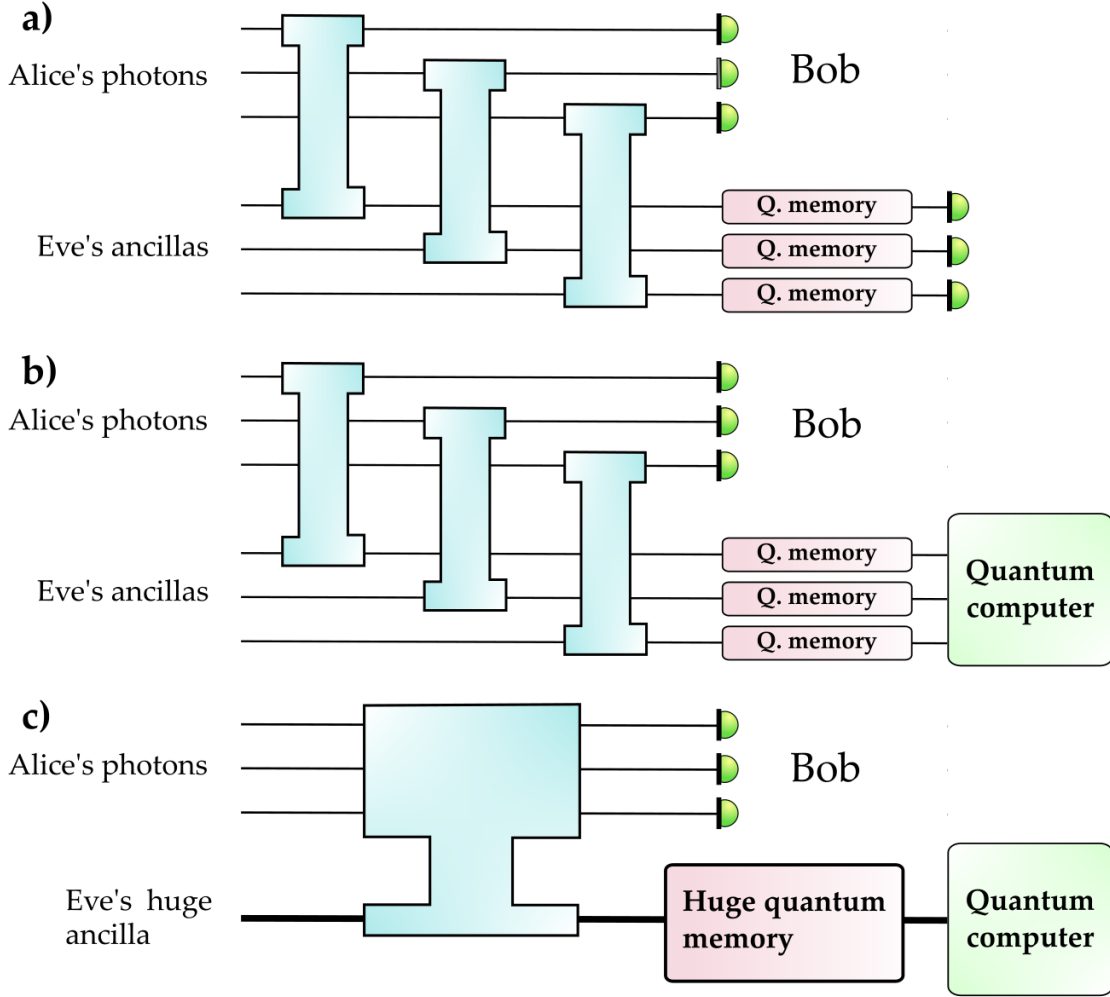
### 3.4.2 Security analysis

When we model possible attacks, we always consider Eve having complete control over the quantum channel, enabling her to manipulate it as she wishes. Moreover, she can introduce any auxiliary states to interact with the signals sent and then carry out measurements on these states. Generally, we also assume that she has access to quantum memory, allowing her to store these states and delay her measurements until after gaining insights from the classical post-processing phase.

#### Types of attack

One can categorize Eve's potential strategies into three attack types. See Figure 3.3 for a pictorial representation.

1. **Individual attacks:** This is the simplest form of quantum eavesdropping. Eve examines each quantum state one at a time and stores them in separate quantum memories. She's restricted to performing individual measurements on each state, although she can delay her measurement until after all public communication is complete.
2. **Collective attacks:** These are similar to individual attacks, with the key difference being Eve's ability to perform a joint measurement on all the quantum states she has accumulated. These are also called independent and identically distributed (i.i.d.) attacks, since the joint quantum state  $\rho_{ABE}^n$  between Alice, Bob, and Eve before any measurement by Eve has the form  $\rho_{ABE}^n = \rho_{ABE}^{\otimes n}$ .
3. **Coherent attacks:** These are the most general attack strategies. Eve can now interact with the entire quantum communication sequence using one single ancilla state in a large Hilbert space before performing any measurement on the full state.



**Figure 3.3:** Attack categories for QKD. **a)** Individual, **b)** collective, and **c)** coherent theoretical attacks considered in security proofs. Figured inspired by [120].

### Secret key rate

Now we present the formalism necessary to derive the secret key rate of a given QKD protocol. The secret key rate  $R$  is defined as the ratio between the size  $l$  of the cryptographic key  $K$  and the number  $N$  of quantum signals exchanged during the protocol

$$R := \frac{l}{N} . \quad (3.5)$$

In the limit  $N \rightarrow \infty$  the *asymptotic secret key rate* is defined as

$$R_\infty := \lim_{N \rightarrow \infty} R . \quad (3.6)$$

In a general QKD protocol, after sifting, Alice holds  $n = N\gamma_{\text{sift}}$  instances of the classical random variable  $A$ , where  $\gamma_{\text{sift}}$  is the *sifting factor*, i.e. the fraction of exchanged symbols

that is kept in the sifting step. For example, in a standard BB84 protocol,  $\gamma_{\text{sift}} = \frac{1}{2}$ , since half the times Bob picks the wrong basis. Moreover, in 2000 Shor and Preskil [112] proved the asymptotic security of BB84<sup>4</sup>, relating its security to entanglement purification protocols [122]. The asymptotic key rate has the simple form of

$$R_{\infty}^{\text{BB84}} = \frac{1}{2} (1 - 2H_2(\text{QBER})) , \quad (3.7)$$

where  $H_2(x) = x \log x - (1 - x) \log(1 - x)$  is the binary Shannon entropy. Notably, the threshold  $\text{QBER} = 11\%$  is the point at which  $R_{\infty}^{\text{BB84}}$  reaches 0.

To study a general QKD protocol however, we will focus on a different line of security analysis based on bounding the conditional min-entropy of a sifted key. We consider for simplicity the specific case of *direct error correction*, where Alice helps Bob correct his raw key  $A^n$ . The size of a  $\epsilon$ -secure secret key is then given by [123, Lemma 1]

$$l = H_{\min}^{\epsilon'}(A^n|E) - \text{leak}_{\text{EC}} - 2 \log \left( \frac{1}{2(\epsilon - \epsilon' - \epsilon_{\text{EC}})} \right) , \quad (3.8)$$

for some  $\epsilon' \geq 0$ . Here,  $\text{leak}_{\text{EC}}$  denotes the amount of information that Alice communicates to Bob during error correction. Moreover,  $\epsilon_{\text{EC}}$  denotes the failure probability of the error correction, which is the probability for Bob to guess the wrong key. Consequently, the main goal in a security proof is to bound the smooth min-entropy in Eq. (3.8) to estimate the secret key rate.

Generally, this quantity is rather difficult to compute under the most general coherent attack. A typical strategy is then to restrict the analysis to collective attacks, for which powerful numerical tools have been developed [124, 125]. Notably, considering i.i.d quantum states, the smooth min-entropy can be written as a conditional Von Neumann entropy for one round of the quantum communication, thanks to the so-called *asymptotic equipartition property* [126]

$$H(A|E)_{\rho} = \lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} H_{\min}^{\epsilon}(A^n|E^n)_{\rho^{\otimes n}} . \quad (3.9)$$

Moreover, the quantity  $\text{leak}_{\text{ER}}/n$  in the asymptotic limit can be made arbitrarily close to the Shannon limit  $H(A|B)$  thanks to the channel coding theorem [98]. As a consequence, one can recover the standard Devetak-Winter bound [65] for the asymptotic secret key rate

$$R_{\infty} = \gamma_{\text{sift}} (H(A|E) - H(A|B)) . \quad (3.10)$$

In DV-QKD security against coherent attacks in a scenario with a finite-size key can then be deduced using methods derived from the de Finetti theorem [17, 127], the entropic uncertainty principle [128], or the entropy accumulation theorem [129–131]. Yet, in CV-QKD, security proofs for the general setting are less mature. In fact, we can only prove the finite-size security for the GG02 no-switching protocol, thanks to a Gaussian de Finetti reduction [132].

---

<sup>4</sup>Initially their approach was non-composable, but later work [121] showed that it could be readily adapted to establish composable security.

## 3.5 Practical quantum key distribution

### 3.5.1 Experimental implementations

Before introducing the landscape of experimental implementations of QKD it is important to mention the fundamental limit for point-to-point quantum communication rates, a constraint imposed by the losses in the quantum channel connecting the two parties. In particular in [81], this fundamental threshold is defined for a channel with transmissivity  $\eta$  by the equation

$$R_{\text{SKC}} = -\log(1 - \eta) . \quad (3.11)$$

This is commonly referred to as Pirandola-Laurenza-Ottaviani-Bianchi (PLOB) bound, named after the authors. To overcome this fundamental rate-loss scaling and achieve long-distance communication different approaches have been considered.

**Quantum repeaters:** The first approach is to deploy the so-called *quantum repeaters*. The main idea behind quantum repeaters is to divide the quantum channel into smaller segments, where losses are not too high, and generate entangled pairs between intermediate nodes. By means of quantum teleportation [133] one can establish a final pair of entangled states over a long distance, which can then be used to perform key distribution. Yet, despite significant advancements toward their development [134], the realization of a fully operational quantum repeater is currently outside the reach of existing technology. The primary issue for quantum communication applications remains that current quantum memory technology is unable to store quantum states for the duration required to create an entangled state between two remote parties.

**Twin-fields approach:** Recently, a novel phase-encoding MDI-QKD protocol called Twin-Field Quantum Key Distribution (TF-QKD) was proposed, which does not rely on a quantum memory. Alice and Bob encode their secret bits and bases within the phases of optical pulses. These pulses are subsequently transmitted to interfere on the beam splitter of an intermediary node. By delegating the measurement to an untrusted party, the secret key rate in TF-QKD scales proportionally to  $\sqrt{\eta}$ , mirroring the performance of a quantum repeater network with a singular intermediary node. This advancement has spurred a series of experiments demonstrating impressive capabilities over long distances [135–137].

**Satellite-based QKD:** Incorporating low-Earth orbit satellites as intermediary nodes offers another viable alternative for extending communication distances in quantum key distribution. These satellites serve as relay points between the two parties who aim to establish a secret key on the ground. The main advantage of using free-space communication is its lower susceptibility to signal loss compared to traditional optical fiber channels, especially at higher altitudes. With this approach quantum communication at the intercontinental level results feasible. For instance, in [138], they established a free-space link of over 7,600 km, successfully connecting China and Europe. Unfortunately, the communication speeds achieved are currently too low for real-world commercial use, calling for technological advancements, especially in detection systems [139], as well as innovations in security proofs [140].

However, the effort of the QKD community is not solely on establishing connections between

extremely distant users; there is also a significant emphasis on improving the overall speed of key generation, particularly for users within metropolitan distances. The current record for the fastest key rates with finite-size security and security parameter  $\epsilon = 10^{-10}$  was set in [141], implementing a DV-QKD protocol with cutting-edge multi-pixel Superconducting Nanowire Single-Photon Detectors (SNSPDs) that boast exceptionally high counting rates, achieving 115.8 Mb/s over a 10km optical fiber span.

Meanwhile, CV-QKD systems offer a viable and cost-effective alternative, with the added advantage of being somewhat compatible with current telecommunications infrastructure. These systems can currently deliver key generation rates in the range of a few megabits per second in metropolitan networks, both for Gaussian [142] and discrete [143, 144] modulation.

### 3.5.2 Quantum hacking

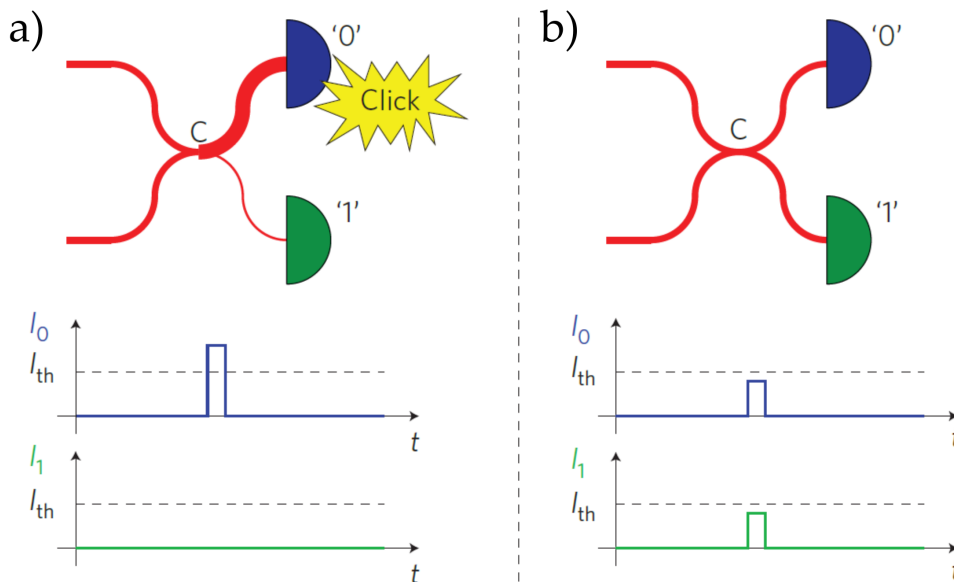
Theoretical security proofs constitute a strong conceptual framework to capture the security properties of QKD protocols. QKD implementations may, however, not fully comply with the model used in the security proof, leading to security vulnerabilities and the possibility of launching *side-channel attacks*. In modern cryptography, side-channel attacks represent any attack that exploits information derived from the physical implementation of a cryptosystem, as opposed to attacks leveraging brute force or inherent theoretical weaknesses. Regardless of their foundation in quantum theory or computational complexity, this issue is a universal challenge across all cryptosystems. Timing attacks, for instance, pose a risk to both quantum [145] and classical cryptosystems [146]. We refer to [58, 147, 148] for extended reviews on quantum side-channel attacks.

The first attack specific to quantum cryptography tackled the implementation of the standard BB84, where a vulnerability was found in the light source. In particular, QKD systems would not use true single photon sources, but opt for attenuated coherent pulses instead. This approach can lead to signals containing multiple photons, where Eve can intercept one photon for herself and pass the rest to Bob. During the subsequent classical communication phase, Eve gains knowledge of the encoding basis, allowing her to accurately measure the photons she intercepted. Even though executing the attack would require currently unavailable technologies, such as long-term quantum memories, the discovery of this attack, known as Photon-Number-Splitting (PNS) attack [149], led to skepticism among researchers about the feasibility of QKD using weak coherent sources. Fortunately, a perfect countermeasure to this was found a few years later by modifying the BB84 protocol to include weaker intensity "decoy states" [52].

#### Practical side-channel attacks

One of the first feasible side-channel attack to be identified on quantum devices was notably low-effort for any eavesdropper: in 2001, as reported in [150], specific photon detectors—namely silicon-based avalanche photodiodes—were discovered to emit light at various wavelengths when they detected a photon. This inadvertently emitted light could potentially reveal which detector was triggered, presenting a rather obvious security loophole. This attack is somehow linked to a broader category of *trojan horse attacks* [151], where Eve typically probes the settings of Alice’s and/or Bob’s devices by injecting light and capturing

the reflected signal. However, in this instance, such active probing was unnecessary, as the devices themselves inadvertently disclosed information. Beyond trojan horse strategies, a variety of hacking techniques have been identified to exploit potential weaknesses of specific implementations, such as *fake-state attacks* [152], *efficiency mismatch attacks* [153], or *time-shift attacks* [145], to name a few. Yet, the *blinding attack* [66] stands out as one of the most impressive for its simplicity and effectiveness, marking quantum hacking as both a significant academic research area and a key consideration for the commercial deployment of QKD systems.



**Figure 3.4:** Illustration of the detection of Eve’s resent pulsed in the blinding attack. **a)** When Eve and Bob choose the same measurement bases and Eve detects a bit value of 0, her pulse is directed towards detector 0. The resulting current exceeds the threshold current, triggering a detection event. **b)** If Eve and Bob select different bases, Eve’s pulse spreads its power equally between both detectors. Since the current in each detector remains below the threshold, no detection event occurs. Figure from [66].

In a blinding attack, Eve can manipulate Bob’s single-photon detectors by shining intense light on them, switching their operational mode from the single-photon sensitive Geiger mode to a less sensitive linear mode, a process known as *detector blinding*. Once blinded, the detectors only respond to very bright pulses. This allows Eve to execute an intercept-and-resend attack without raising the QBER. She intercepts the states from Alice and measures them on a random basis. She then resends her detection results to Bob, but instead of sending pulses at the single-photon level, she sends pulses with tailored brightness just above the triggering threshold for the linear mode. If Eve matches Bob’s measurement basis, the entire pulse is directed to a single detector leading Bob to register a click as if the channel were eavesdropper-free. Moreover, if Eve’s basis differs, she still prevents the introduction of additional noise, since the pulse’s power is split between both detectors, with neither receiving enough to register a detection. This scenario is depicted in Figure 3.4.





## Part II

# QKD vulnerability analysis



# QKD ATTACK RATING

## Contents

|            |   |           |
|------------|---|-----------|
| <b>4.1</b> | <b>Introduction</b>   | <b>50</b> |
| 4.1.1      | Road to certified quantum infrastructures                         | 50        |
| 4.1.2      | Attack rating methodology   | 51        |
| <b>4.2</b> | <b>CV-QKD vulnerability assessment against saturation attacks</b> | <b>53</b> |
| 4.2.1      | The saturation attack principle                                   | 54        |
| 4.2.2      | Attack implementation and rating                                  | 55        |
| <b>4.3</b> | <b>Conclusion</b>   | <b>60</b> |

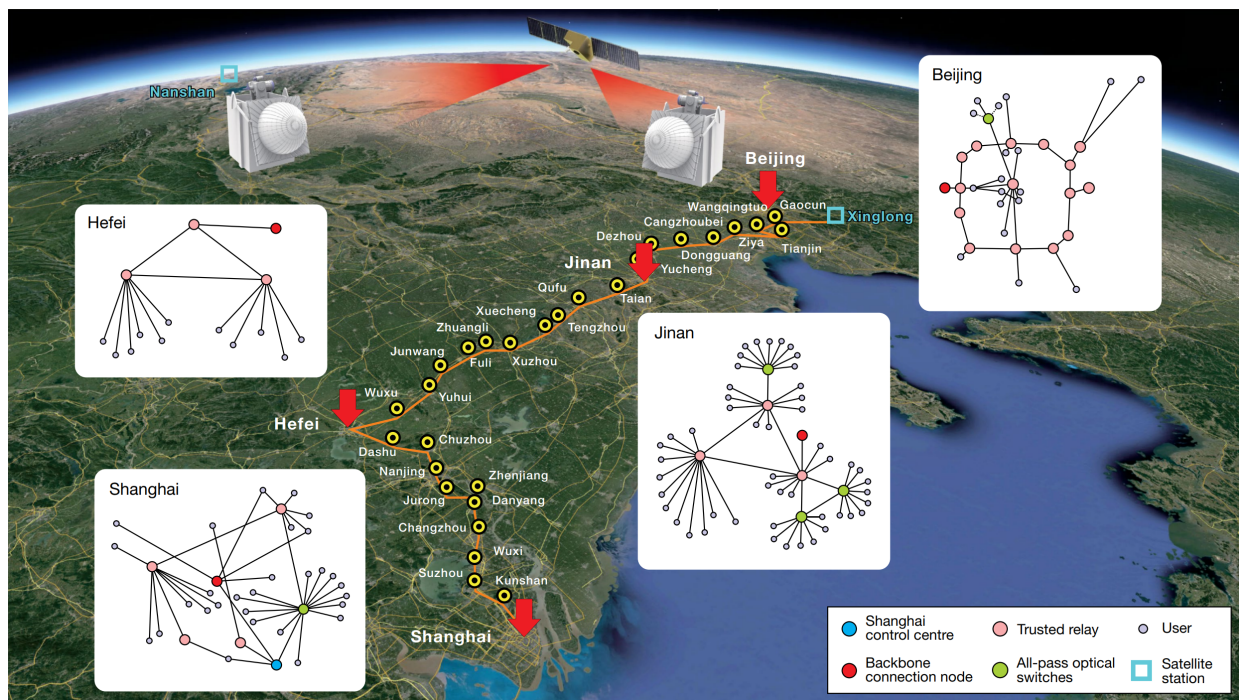
Inspired by the methodology used for classical cryptographic hardware, this chapter introduces the concept of attack ratings within the scope of QKD security assessments. We demonstrate the practicality of this method through a detailed vulnerability analysis of a CV-QKD system, focusing on its resilience against two distinct attack strategies.

## 4.1 Introduction

### 4.1.1 Road to certified quantum infrastructures

The maturity of the field of quantum communication is reflected in the recent development of impressive QKD networks, such as the one developed in China [32], as shown in Figure 4.1. This network spans thousands of kilometers and links four metropolitan areas. Moreover, halfway around the world, Europe launched in 2019 the EuroQCI initiative [154] aimed at deploying a pan-European quantum communication infrastructure in the next 10 years, connecting strategic public sites.

However, in order to take the final step towards a trusted global quantum infrastructure, we necessarily need tools to ensure the process of specification, implementation, and evaluation of quantum devices. To broaden the market of quantum cryptographic technologies, the need of the hour is, therefore, a standardized approach for security certification. This undoubtedly constitutes a complex task, requiring the collaboration of experts from different fields ranging from Information Technology (IT) security, quantum engineering and theory. Nevertheless, over the last few years, several international standardization organizations have been actively working towards this goal, under the unified Common Criteria framework: the ETSI Industry Specification Group (ISG) on QKD has been focusing on many different aspects of QKD implementation security [58] and has recently published the



**Figure 4.1:** Illustration of the space-ground integrated quantum network in China [32]. it consists of four quantum metropolitan networks located in Beijing, Jinan, Shanghai, and Hefei, a backbone network that spans more than 2000 km, and ground-satellite quantum links. This network enables communication between any pair of users, spanning distances of up to 4,600 kilometers.

first QKD Protection Profile [60], i.e. a document that provides a standardized approach for the evaluation and the security certification of QKD systems. In parallel, ISO/IEC JCT 1/SC 27, a joint technical committee of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), has been working on the security requirements [61], security evaluation, testing and specification [62] of point-to-point QKD modules.

In our work we try to give a different perspective, tackling the task of reducing the gap between practical and theoretical security by rating the feasible attacks and prioritizing accordingly the greatest threats. As system design and security evaluation are in practice almost always limited by resources, attacks that are easier to implement should be prioritized, as they represent the greatest threats. For instance, some attacks on QKD can be realized with a relatively simple procedure and inexpensive hardware, such as detector blinding attack [66] that has even been demonstrated on a live QKD connection [155]. Some other attacks, on the other hand, such as the photon number splitting attack [149] and more generally collective and coherent attacks on QKD [17], have played a fundamental role in our understanding of QKD theory. Yet, their implementation requires the ability to store and retrieve single photons from a quantum memory, potentially over milliseconds or larger timescales, which is currently out of reach, given the limitations of existing quantum memory technology [156–158]. Hence, to guarantee a very high security level for QKD, forward-looking methods and standards in quantum cryptography implementation security shall be adopted, following a methodology similar to the one used to certify the security of classical crypto-systems [159], called Common Criteria.

### 4.1.2 Attack rating methodology

Common Criteria is the set of internationally recognized technical standards and configurations for security evaluations of IT products and technology. The terminology and the concepts deployed in the Common Criteria aim to be as general as possible. Indeed, they are not intended to restrict the class of IT security problems to which Common Criteria is applicable, making them well suited to be extended for quantum communication devices, such as a QKD system. In simple terms, this comprehensive methodology aims at supporting the needs of three groups with a general interest in the evaluation of the security properties of a certain Target Of Evaluation (TOE): owners, developers, and evaluators. In particular, what the owner of the TOE of the device wants is to protect his *assets* (any possible entity that he places value upon) from possible *threat agents*, i.e. someone or something that can abuse these assets against the interests of the owner. A comprehensive methodology offers general guidance and metrics to rate the possible attacks against the assets. It also considers both the likelihood that a threat agent may successfully perform the attack and the magnitude of the impact that this attack has on the assets. In our rating procedure we shall focus on the likelihood of an attack, evaluating the total effort required to successfully mount the attack, called the Attack Potential (AP): the higher the attack potential, the lower the chances of the attack being performed are. The rating procedure consists in attributing a numeric value to the attack potential by considering the factors listed in Table 4.1.

| Expertise        |    | Window of Opportunity        |    |
|------------------|----|------------------------------|----|
| Laymen           | 0  | Unnecessary/unlimited access | 0  |
| Proficient       | 3  | Easy                         | 1  |
| Expert           | 6  | Moderate                     | 4  |
| Multiple experts | 8  | Difficult                    | 10 |
| Knowledge of TOE |    | Equipment                    |    |
| Public           | 0  | Standard                     | 0  |
| Restricted       | 3  | Specialized                  | 4  |
| Sensitive        | 7  | Bespoke                      | 7  |
| Critical         | 11 | Multiple bespoke             | 9  |

**Table 4.1:** Table for the evaluation of the Attack Potential used in the thesis. Elapsed time factor has not been considered: see text for explanations. For a complete guide on how evaluate those factors refer to the Common Evaluation Methodology version 3.1 [57].

- The *expertise* refers to the level of technical expertise required to successfully perform the attack. Clearly, an attack that can be mounted by a person with a regular level of education without advanced knowledge in any specific field should be prioritized.
- The *knowledge of the TOE* involves, instead, the amount of knowledge of the TOE design and operation required: retrieving detailed specifications about the device, for example, might be challenging for an attacker, leading to a higher attack potential.
- Regardless of the information acquired about the TOE, it is possible that, to successfully mount the attack, a previous tuning of the hacker’s setup is needed. This aspect is considered in the *window of opportunity*, together with possible difficulties on getting access to the TOE.
- One last remarkable factor is the level of sophistication of the *equipment* used in the attack: an attack using equipment easy to obtain and simple to operate is obviously more dangerous than another attack that would require more advanced equipment.

To coherently consider these different factors and evaluate their contribution to the final attack potential we assign at each factor one numerical value, following Table 4.1. In order to guarantee a consistent evaluation with respect to attacks to other TOEs, the different levels for each factor and their numerical values come from the Common Evaluation Methodology version 3.1 [57] section B.4, where there is a full description of each possible level. Indeed, their description is particularly generic, to guarantee a meaningful characterization of an attack to a wide range of possible TOEs (such as a QKD device).

In the Common Criteria an additional factor is considered to rate the attacks: the elapsed time, i.e. the time taken to identify a certain vulnerability and to successfully mount the

attack. To fix a correct timescale, this quantity needs to be compared with the usual time needed for a countermeasure to be applied. The vulnerability analysis that we report about in this article, has been performed on a laboratory QKD system. In this context, the main drivers of the elapsed time such as the product revision lifecycle, or the time during which an attacker could access the QKD system, cannot be meaningfully defined. For these reasons, we did not consider the elapsed time factor in our evaluation. We should however state that this factor will become well defined when considering the security of QKD products deployed on real-world networks and should hence be taken into account in future security evaluations of QKD, in conformity with Common Criteria.

Moreover, in a complete vulnerability analysis, attack rating is sometimes split in two steps, for example in the case of smartcards [160]. The *identification step* is related to the effort required to create and apply the attack to the TOE for the first time. The *exploitation step* is then related to the effort required to apply the attack to the TOE knowing the techniques developed in the identification step. Both steps lead to a rating, based on the different factors. For the sake of simplicity, we have not distinguished these two steps in the present article, but we have just followed the general ground rules provided by Common Criteria. This can moreover be justified by the fact that the operational context associated to the exploitation step is essentially missing in the context of laboratory QKD prototype.

Finally, in Table 4.2 we define the semi-qualitative correspondence between rating and attack difficulty. Attack paths with an AP between 0 and 10 are for example rated as *Basic*. Such attacks can be implemented with little effort and therefore constitute very serious threats. On the other hand, attacks with an extremely high attack potential, rated here *Beyond High*, are extremely difficult to implement and therefore constitute less pressing threats.

| Rating      | AP Range      |
|-------------|---------------|
| Basic       | 0 – 10        |
| Moderate    | 11 – 15       |
| High        | 16 – 19       |
| Beyond High | 20 – $\infty$ |

**Table 4.2:** Semi-qualitative scale for attack rating. This scaling is adapted with respect to the Common Evaluation Methodology [57], taking into account the fact that we consider 4 out 5 factors in our analysis.

This has led us to adapt the rating methodology and the severity scale presented in Tables 4.2 and 4.1 with respect to the original tables from the Common Evaluation Methodology [57].

## 4.2 CV-QKD vulnerability assessment against saturation attacks

We now approach for the first time the task of prioritizing the feasible attacks against a quantum cryptographic device. To illustrate the relevance of this new approach in the quantum cryptography community, we have implemented and tested two different attack



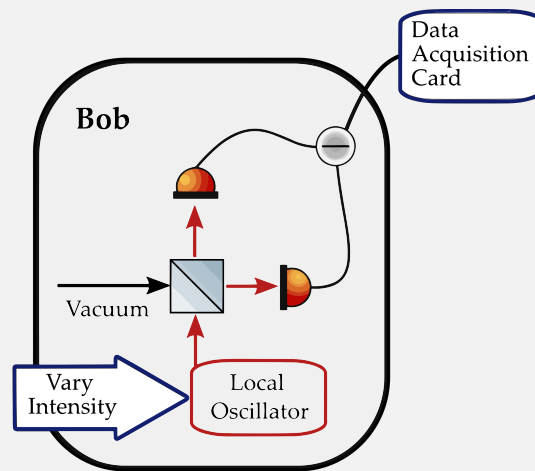
strategies for the *saturation attack* [67, 69] on a working CV-QKD experimental set-up and evaluated their practical feasibility.

### 4.2.1 The saturation attack principle

Saturation attack on CV-QKD consists in biasing the excess noise estimation by actively inducing the saturation of the homodyne detectors. In a CV-QKD system that implements the GG02 protocol, Alice prepares coherent states of quadratures  $\{X_A, P_A\}$ , modulates each quadrature according to a Gaussian distribution of variance  $V_A$  and centered on zero, and sends the modulated coherent state to Bob through the quantum channel. Bob randomly measures one of the quadratures using a balanced homodyne detector. This results in quadrature measurements  $X_B$  and  $P_B$ , with variance  $V_B$ . By correlating sent and measured quadrature values on a fraction of their data, the users estimate channel transmittance  $T$  and then the excess noise  $\xi$ . If these values are within the limit for validating the security of the key, they proceed to key distillation on rest of the data, if not the QKD protocol aborts.

#### Characterization of homodyne detectors

Balancing the homodyne detector prior to protocol run ensures that the mean of the homodyne output values remain close to zero, and therefore that the homodyne receiver is operated in its linear range, except if signals with very large quadrature values are received at Bob side. In case signals with  $X_B \ll \alpha_1$  (respectively  $X_B \gg \alpha_2$ ) are received, then the detector will saturate and output  $X_B = \alpha_1$  (respectively  $X_B = \alpha_2$ ). Assuming it is the same for  $X$  and  $P$  quadrature, we can designate this linearity range as a quadrature interval  $[\alpha_1, \alpha_2]$  ( $\alpha_1 < 0 < \alpha_2$ ).



**Figure 4.2:** Pictorial representation of how to characterize the linearity range of a homodyne detector.

A simple procedure to characterize the linearity range of the homodyne detector response has been proposed in [69]. The key idea is to perform an homodyne measurement while sending only a local oscillator and investigate how the system behaves under

varying intensities. What the authors observed is that when approaching or surpassing the detection limits, response of the detector becomes non-linear to the input signal quadrature. As a result, the measured variance is effectively reduced compared to the true quadrature variance of the received optical signals.

The saturation attack comprises of two main steps: intercepting Alice’s signal and resending a newly prepared signal to Bob with an extra adjustment, which we shall call *saturating tweak*, that will force the saturation of the detectors. As we shall see in details in the next section, we will consider two possible saturating tweaks. The first tweak involves introducing an additional displacement to the resent coherent state, while the second consists in multiplexing the resent coherent state with an external incoherent laser.

Now, from the quadrature measurement data obtained from the saturated induced detector, Alice and Bob estimate channel parameters  $T_{sat}$  and  $\xi_{sat}$ . To characterize the attack, and in particular its impact on key rate, we have defined the following conditions for a successful attack:

- i) The attacker, Eve, performs the saturation attack: an intercept-resend attack with a saturating tweak.
- ii) The channel transmission estimation is unaffected ( $T_{sat} = T^1$ , where  $T$  is the channel transmission in absence of attack).
- iii) Alice and Bob obtain a positive key rate from their estimated parameter  $T_{sat}$  and  $\xi_{sat}$ .

In this scenario, despite Eve launching an intercept-resend attack, which typically would cause the QKD protocol to terminate because of excessive noise preventing key generation, the attack goes undetected due to saturation. Consequently, Alice and Bob end up generating an insecure key, leading to a clear breach in security.

## 4.2.2 Attack implementation and rating

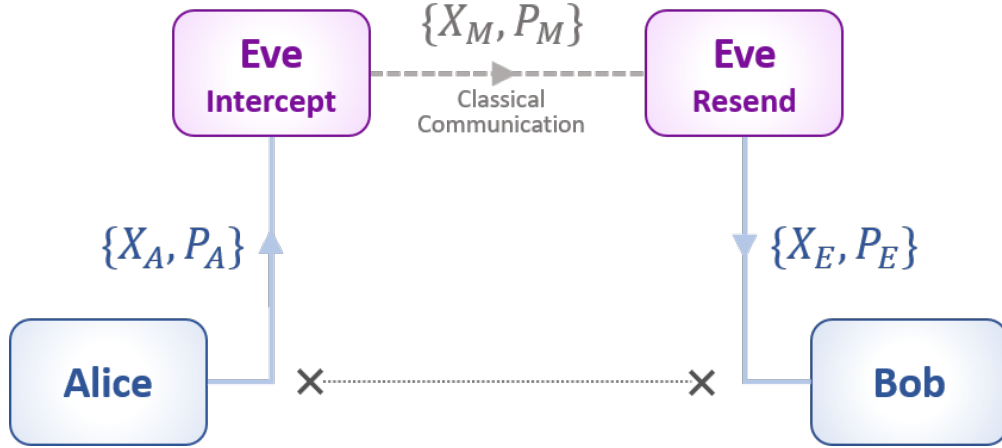
For the sake of clarity, we can consider that two cooperating eavesdroppers are involved in the attack:  $Eve_{intercept}$ , located near Alice intercepts the signals of quadratures  $\{X_A, P_A\}$  and classically communicates the measurement results  $\{X_M, P_M\}$  to  $Eve_{resend}$ —located near Bob as shown in Figure 4.3. Due to the technical restrictions imposed by the laboratory equipment, the experimental demonstration focused only the resend step of the attack and model the impact of the measurement associated with the intercept step.  $\{X_M, P_M\}$  is deduced from  $\{X_A, P_A\}$  by simulating a heterodyne measurement, i.e. 3 dB loss factor and also the addition of a random Gaussian noise of variance 2 shot noise [161].

We will now describe the two main attack strategies for a saturation attack, the reader can refer to Appendix A for a full description of the experimental setup.

### Coherent attack strategy

The signal of quadrature  $\{X_E, P_E\}$  is resent by  $Eve_{resend}$ , which we will from here onwards label as Eve. is experimentally generated, using a setup built around a Sagnac interferometer,

<sup>1</sup>Alice and Bob might view a sudden alteration in the channel’s transmission as something suspicious.

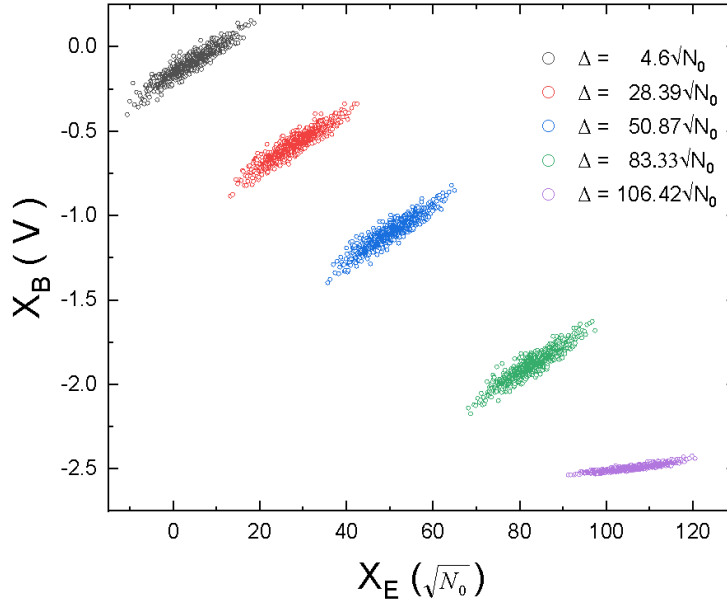


**Figure 4.3:** Scheme for saturation attack.  $Eve_{intercept}$  intercepts Alice’s Gaussian modulated signal of quadratures  $\{X_A, P_A\}$  and shares her measurement results  $\{X_M, P_M\}$  through the classical channel to  $Eve_{resend}$ . The resented and displaced signal of quadrature  $\{X_E, P_E\}$  is measured by Bob’s homodyne detector.

whose functioning is detailed in Appendix A. The role of this set-up is to generate, knowing the in values  $\{X_M, P_M\}$ , a displaced coherent state of quadrature  $\{X_E, P_E\}$  that corresponds to the encoding of  $\{X_M, P_M\}$  on a coherent state, to which is applied a coherent gain  $\sqrt{G/2}$  in amplitude, and a controlled coherent displacement by a value  $\Delta = \Delta_X = \Delta_P$ . The Sagnac loop offers a high phase stability which allows to precisely control  $\Delta$  and therefore minimize the noise. Receiving the displaced coherent state  $\{X_E, P_E\}$ , Bob randomly measures one of the quadratures with a balanced homodyne detector, hence obtaining  $X_B$  or  $P_B$ . Depending on the value of  $\Delta$ , this quadrature measurement will be obtained in the linear or in the saturated regime. See Figure 4.6 for a pictorial representation.

Figure 4.4 shows the effect of the displacement  $\Delta$  on Bob’s experimental quadrature measurements. The mean value of the homodyne output  $X_B$  can be shifted towards one of the detection limit  $\alpha_1 = -2.5V$  of the detector, for a given displacement setting. Selecting displacement angle to 225 degree would direct the shift towards the other limit of the linear range  $\alpha_2 = 3.3V$ . As can be seen on Figure 4.4, when the detector is operated close to its linear range limit, then saturation occurs and quadrature variance reduces drastically.

The coherent displacement set-up demands an active feedback routine to compensate the relative phase drifts between the displaced signal and the local oscillator. Even though Sagnac loop provides a high stability, as illustrated by the level of control obtained on Figure 4.4, we could not lower the residual quadrature noise due to imperfect phase drift compensation below the null key threshold. For example, considering that  $2\pi$  phase drift occurring in 1 second, a  $500 \mu s$  latency in the feedback loop creates about 0.2 degrees of phase error. This in turn results in  $0.23\sqrt{N_0}$  fluctuations in homodyne output and generates excess noise of about  $5N_0$ . This implies that the excess noise  $\xi_{sat}$  is above the null key noise threshold value, and prevents the generation of key. In other words, in the current setup, Alice and Bob would easily detect attack based on coherent displacement. Reducing the feedback latency such that phase drift remains negligible within the feedback intervals, could however bring this attacking strategy to meet the attack success conditions.

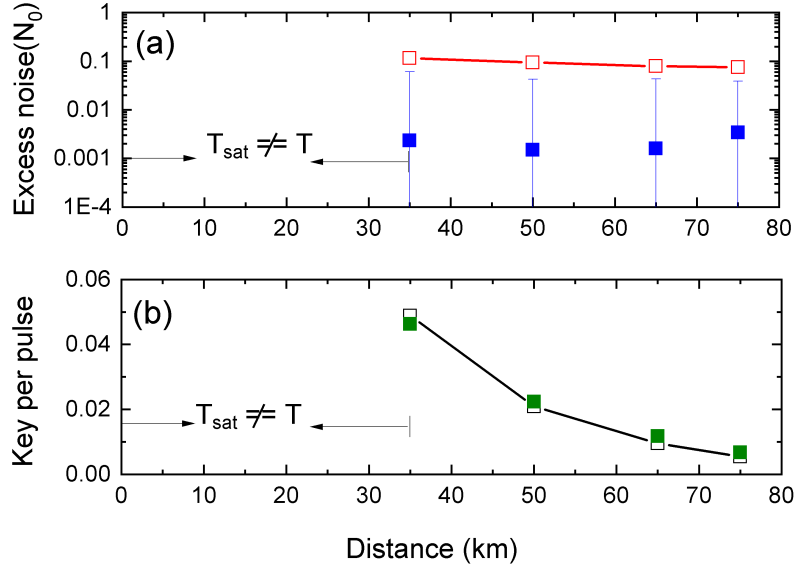


**Figure 4.4:** Scheme for saturation attack. Input signal sent by Eve, with quadrature variance  $Var(X_E) = 22N_0$  with 5 different displacement  $\Delta$  values equals to  $4.6\sqrt{N_0}$  (black),  $28.39\sqrt{N_0}$  (red),  $50.87\sqrt{N_0}$  (blue),  $83.33\sqrt{N_0}$  (green) and saturation at  $106.42\sqrt{N_0}$  (magenta). Displacement creates Bob's quadrature measurement  $X_B$ , expressed here in volts, shifts towards the detection limit  $-2.5$ Volts.

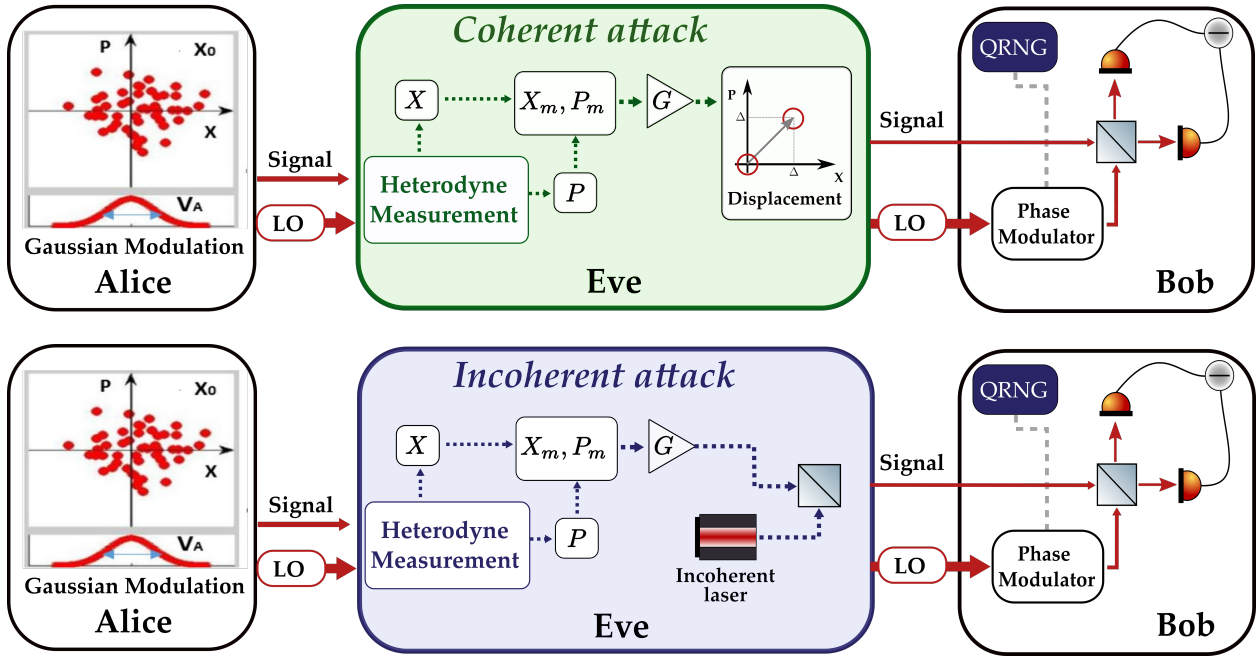
### Incoherent attack strategy

In order to overcome the implementation difficulties of the coherent displacement strategy, we have conceived and tested a much simpler strategy, based on incoherent laser pulse injection [69]. Saturating the homodyne detector with external laser pulse indeed presents several operational advantages over the previous strategy. First, since it is incoherent with the local oscillator, an external laser adds only its own shot noise to the excess noise. More importantly, relative phase drift compensation is not required for keeping the homodyne in the saturated region. In this strategy, saturation is induced by an intense incoherent laser pulse sent along with the resent coherent state, see Figure 4.6 for a pictorial representation.

Since optical phase drift compensation is not needed, saturation attack with an incoherent laser pulse can achieve comparatively much better performance in terms of quadrature stability and noise, and can meet success conditions, provided the channel loss is not too small (low channel loss makes it more difficult for Eve to succeed in the intercept-resend attack). The results in terms of excess noise are given in Figure 4.5(a). The excess noise at Alice has been calculated from the variance of saturated homodyne output experimental data, at various transmission distances between Alice and Bob. It can be seen that the excess noise is below the null key threshold, which indicates Eve's intercept-resend attack remains untraceable. Figure 4.5(b) shows the maximal value of the final key rate per pulse, estimated under collective attacks (see Appendix A.4). Note that the condition  $T_{sat} = T$  cannot be met for a distance below 35 km (see Appendix A.3).



**Figure 4.5:** Results of the incoherent attack. (a) excess noise at Alice. Red squares indicate the null key noise threshold and blue squares indicate the estimated values of  $\xi_{sat}$ . (b) key rate. Black squares are simulated values of the final key per pulse while Green squares are from the experiment. Error bars are one standard deviation of fluctuations among ten smaller data blocks of size  $10^7$ . Success condition of  $T_{sat} = T$  can not be fulfilled below 35km.



**Figure 4.6:** Schematic of both a coherent attack (in green) and an incoherent attack (in blue) against a CV-QKD protocol. The measured signal is resent with an amplification factor  $G$  and displacement  $\Delta$  for the coherent attack. In the incoherent attack, the amplified resent signal is combined with an incoherent laser using a beam splitter instead.

## Rating of the two attacks

Now that we have defined and studied the two possible attack paths to exploit the saturation vulnerability of the homodyne receiver, we are ready to use Table 4.1 to evaluate their attack potential. We assume that the hacker Eve tries to obtain as much information as possible about the TOE design, i.e. we need to assume that Eve has good knowledge about the specifications of the main components of the QKD system. Part of this information can indeed be found easily online. However, some important details might be system-specific or protected by a non-disclosure agreement between the vendor and the owner of the QKD system. For this reason, for both attacks, the Knowledge factor for the TOE factor is evaluated as *restricted*.

Both attacks rely on the intercept-resend strategy and can in principle be launched in real-time. However, such online implementations of the attacks require to evaluate the optimal value of the displacement  $\Delta$  and of the gain  $G$  (see methods): this can be obtained by manually tuning Eve’s setup and measuring the excess noise due to displacement, as in Figure A.3. Assuming a frequent trusted evaluation of the channel loss, this tuning might be quite challenging, especially in the case of a coherent attack, where the tuning precision is inevitably limited by the accuracy of the phase locking. As a result, for the coherent attack, the Windows of Opportunity can be chosen as *difficult*, while *moderate* for the incoherent attack. The main differences between the two attack paths are related to the requirements in terms of equipment and expertise. As previously explained, the coherent attack requires Eve to resend a coherent displaced signal while being successfully phase-locked with Alice and Bob. To achieve this, Eve needs to be an *expert* in coherent optical communications, able to control noise at the quantum level and to have access to *bespoke* equipment. On the other hand, the incoherent attack only requires Eve to send an incoherent signal, without worrying about being phase-locked with Alice and Bob: this is reflected in a simplified setup (Equipment *specialized*) and in a lower level of required technical expertise for Eve (Expertise *proficient*). From Table 4.1 we hence obtain an attack potential of 26 and 14 for coherent and incoherent attack respectively. As expected, the coherent attack is rated as *beyond high*, while the incoherent attack is only rated as *moderate*. A summary of the analysis is given in Table 4.3.

|                   | Attack Potential |          |           |          |                 | Rating             | Experimental Results                               |
|-------------------|------------------|----------|-----------|----------|-----------------|--------------------|--|
| Coherent Attack   | Exp<br>6         | KoT<br>3 | WoO<br>10 | Equ<br>7 | AP<br><b>26</b> | <b>Beyond High</b> | ✓ Noise model characterized<br>× Attack unfeasible |
| Incoherent Attack | Exp<br>3         | KoT<br>3 | WoO<br>4  | Equ<br>4 | AP<br><b>14</b> | <b>Moderate</b>    | ✓ Attack exp. demonstrated                         |

**Table 4.3:** Summary of the analysis on the two attacks to the homodyne detection. We have reported the values for each factor of the attack potential, namely: Exp. stands for Expertise, KoT for Knowledge of the TOE, WoO for Window of Opportunity and Equ for Equipment.

## 4.3 Conclusion

Quantifying the level of security assurance of a QKD device is a complex undertaking that should be based on a sound and largely recognized methodology. The practical ability to evaluate QKD security will also require to set up evaluation lab facilities and to train “QKD security evaluation engineers”, able to conduct penetration testing on QKD systems, both in terms of software and hardware. In that perspective, the experience accumulated in the context of classical secure hardware, and in particular the use of the Common Criteria methodology by the smartcard industry [160] is invaluable.

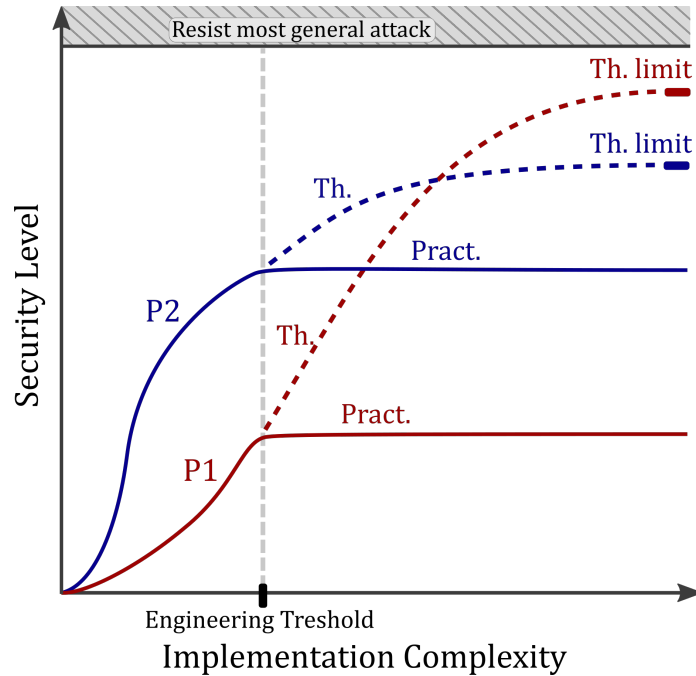
The main message of this chapter is to point at the relevance of calculating attack potential to rate attacks against QKD device, following a methodology already in place to evaluate the security of classical cryptographic hardware. One might however wonder whether this message should be read negatively, from a QKD viewpoint. Does it imply that the security QKD can provide essentially compares to the security that can be reached with classical hardware crypto-systems? We want to argue that this not the case, for fundamental reasons: quantum crypto-systems strongly differ from their classical counterparts and provide a security advantage that is not only related to the information-theoretic security versus computational security paradigm. Quantum cryptography is moreover intrinsically based on models where the inner details of the physical layer are tied to information-theoretic measurable quantities. For instance, a functional QKD system is by definition sensitive to losses or errors occurring at single photon level. This is in strong contrast with classical systems, where information is typically encoded over a very large number of particles, such as classical optical pulses containing many photons. As a consequence, a classical system is oblivious to leakage occurring at the level of single quanta and cannot match the security level that can be provided, at least in principle, by a quantum crypto-system.

Considering the interplay between QKD implementation complexity and security also leads to an important reassessment. Theoretical security and practical security of a given QKD system may indeed significantly differ, notably when practical security is limited by engineering constraints. This calls to reconsider the absolute security claims sometimes associated with QKD and to adopt a more balanced viewpoint taking implementation complexity into consideration. We have depicted on Figure 4.7 an case illustrating this situation: we consider two QKD protocols<sup>2</sup>, P1 and P2, where protocol P1 has a more advanced security proof than protocol P2, therefore allowing to claim a higher security level in theory. However, it is possible that the protocol P2 has a lower implementation complexity than P1 and that, for the practically reachable implementation complexity corresponding to the engineering threshold, the practical security, i.e. the security that can be reached in practice by the QKD system, is larger with P2 than with P1.

Finally, the use of attack potential in QKD has also implications regarding the security that can be targeted. In particular, optimizing the security level of a given QKD device requires to first thwart attacks with the lowest attack potential before focusing on more complex ones. We have moreover explicitly demonstrated, on a live CV-QKD system, how

---

<sup>2</sup>The term *protocol* has to be understood here in a holistic sense, ranging from the specifications of the physical implementation of the QKD devices, to the detail of the logical operations that they perform in order to establish a key.



**Figure 4.7:** Pictorial representation of the possible divergence between theoretical (th.) and practical (pract.) QKD security. A QKD protocol P1 may have a stronger theoretical security (reachable for a perfect implementation) than another QKD protocol P2. Yet, in practice, QKD protocols can only be operated below a certain implementation complexity level materialized by the engineering threshold, and protocol P2 provides a stronger practical security than protocol P1.

different attacks related to the same theoretical vulnerability - i.e. the non-linear response of the homodyne receiver - can lead to different attack potentials. For a first attack path, detector saturation is reached using a coherent displacement. However, the practicality of this attack is limited due to noise generated from the imperfect phase drift compensation. The second attack path is on the other hand much more dangerous in practice: shining a simple external incoherent laser, it allows to drive the homodyne detector in the non-linear region of its characteristics and to precisely control the excess noise generated from Eve's intercept-resend attack, while meeting the conditions defined for the success of the attack. Adapting existing criteria from IT security to the context of quantum cryptography is certainly a long and challenging path, but it is essential if we aim to make quantum devices relevant in the context of cyber security.





## Part III

# Hybrid quantum cryptography from communication complexity



# FROM CLASSICAL TO QUANTUM COMMUNICATION COMPLEXITY

## Contents

|            |   |           |
|------------|---|-----------|
| <b>5.1</b> | <b>Communication Complexity</b>         | <b>66</b> |
| 5.1.1      | Deterministic protocols                 | 66        |
| 5.1.2      | Randomized protocols                    | 67        |
| <b>5.2</b> | <b>Information Complexity</b>           | <b>70</b> |
| 5.2.1      | External and internal information       | 70        |
| 5.2.2      | Compression schemes in one-way setting  | 72        |
| <b>5.3</b> | <b>Quantum Communication Complexity</b> | <b>74</b> |
| 5.3.1      | $\beta$ -Partial Matching Problem       | 74        |
| 5.3.2      | Vector in a Subspace Problem            | 77        |
| 5.3.3      | Comparison between the two problems     | 79        |

In this chapter, we analyze in detail the framework of communication complexity, focusing on distinguishing between the communication and information costs of a protocol. Specifically, we will thoroughly examine two quantum communication complexity problems, the  $\beta$ -Partial Matching and the Vector in a Subspace, which will play a crucial role in the next chapters.

## 5.1 Communication Complexity

Communication complexity is a central model of computation, first defined by Yao [70], where there are two players, Alice and Bob, who each receive an input: Alice gets  $x$  from a set  $\mathcal{X}$  and Bob gets  $y$  from a set  $\mathcal{Y}$ . Their goal is to use the allowed type of communication (either classical or quantum) to compute with high probability the value of  $f(x, y)$ , where  $f$  is a function (or relation) defining the computational problem that the players have to solve. Over the years, communication complexity has been extensively investigated across multiple layout models, which specify the allowed interaction between the players.

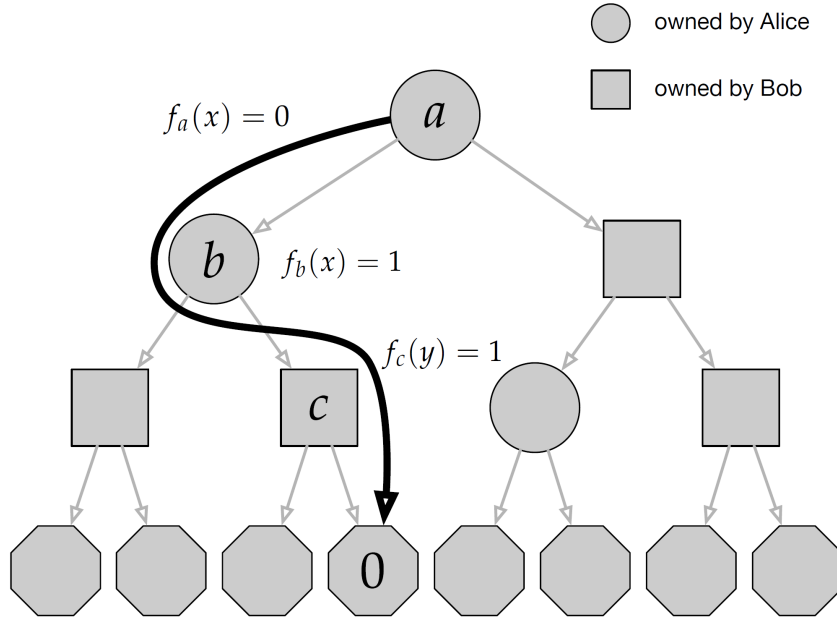
- i) *Two-way (interactive) communication*: Players can exchange messages interactively, until one of them produces the answer.
- ii) *One-way communication*: Only Alice can send a message to Bob. Then Bob needs to produce the answer based on the message he received and his input.
- iii) *Simultaneous message passing*: Both Alice and Bob send one message to a third participant (the referee) who then produces an answer based on these two messages.

To this day, experimental demonstrations of quantum protocols for solving communication complexity problems have focused on one-way communication [162] and simultaneous message passing [163]. Moreover, the main results presented in this thesis, both theoretical (Chapter 7) and experimental (Chapter 8), are formulated using one-way communication complexity. However, the beginning of this chapter serves to introduce the reader to the broader context of interactive communication complexity.

### 5.1.1 Deterministic protocols

As we will see, randomness plays a pivotal role in communication complexity. Nevertheless, it is instructive to begin with a scenario where Alice and Bob lack access to any source of randomness. In such a deterministic setting, before receiving their inputs, Alice and Bob will agree upon a shared protocol  $\pi$  to estimate the output of a given function.

A rooted binary tree (see Figure 5.1) can be used to describe a protocol  $\pi$ , which is an algorithm used to generate a conversation between Alice and Bob. Each internal vertex  $v$  has two children and is owned by either Alice or Bob. Furthermore, each internal vertex  $v$  is associated with a function  $f_v : \mathcal{X} \rightarrow \{0, 1\}$  or  $f_v : \mathcal{Y} \rightarrow \{0, 1\}$ , which maps the input known to the owner to a bit, that is viewed as a child of  $v$ . Given inputs  $(x, y) \in \mathcal{X} \times \mathcal{Y}$ , the protocol's outcome  $\pi_{out}(x, y)$  is computed as a leaf in the protocol tree. They begin by setting the current vertex to be the root of the tree. If the current vertex  $v$  is owned by Alice (Bob), she (he) announces the value  $f_v(x)$  ( $f_v(y)$ ). Both parties then set the new current vertex to be the child of  $v$  indicated by the announced value of  $f_v$ . This process is repeated until the current vertex is a leaf, and the leaf is the outcome of the protocol. Therefore, the inputs  $(x, y)$  induce a path from the root of the protocol tree to the leaf  $\pi_{out}(x, y)$ , which represents the conversation between Alice and Bob, as shown in Figure 5.1. The concatenation of all the bits exchanged during the conversation is often called the *transcript* of the protocol and it is represented as  $\pi(x, y)$ .



**Figure 5.1:** Illustration of an execution of a two-way deterministic protocol. Alice sends the string 01 and Bob answers with the bit 1, allowing to output the final outcome  $\pi_{out}(x, y) = 0$ . Figure from [164].

The efficiency of the protocol is then quantified by its *communication cost*.

**Definition 5.1.1** (Communication Cost). *The communication cost of a protocol  $\pi$ , denoted by  $CC(\pi)$ , is the maximum number of bits that can be transmitted in any run of the protocol.*

One can notice that in a deterministic setting the communication cost is the same as the depth of the protocol tree. This means it is equal to the length of the longest path within the tree.

### 5.1.2 Randomized protocols

Now that we have specified what a deterministic protocol is, we can extend the analysis to a setting where Alice and Bob have access to some source of randomness. We shall therefore consider two main models:

- i) In a *public-coin model* Alice and Bob can share a public random string  $r$ , which can always be assumed to be uniform over some domain. The transcript  $\pi(x, y, r)$  and the final output  $\pi_{out}(x, y, r)$  will be then a function of both inputs  $x, y$  and the shared randomness  $r$ .
- ii) In a *private-coin model*, instead, Alice and Bob have access locally to a private random string  $r_A$  and  $r_B$  respectively, which, as in the case of the shared randomness, can always be assumed to be uniform over some domains. The transcript  $\pi(x, y, r_A, r_B)$  and the final output  $\pi_{out}(x, y, r_A, r_B)$  will be a then function of all the inputs and all the private coins.

Finally, it can be observed that a randomized protocol can be viewed as a distribution on deterministic protocols. Furthermore, the communication cost of a randomized protocol is delineated as the maximum total number of bits transmitted by the players. This maximum value is determined by considering all possible input selections and the corresponding chosen randomness. In order to evaluate the accuracy of a protocol in these randomized settings, one can identify two possible ways of measuring its error probability:

*Worst-case* A protocol has error  $\epsilon$  in the worst-case if the probability of the protocol making an error is at most  $\epsilon$  on every input.

*Average-case* Given a distribution on inputs  $\mu$ , a protocol has error  $\epsilon$  with respect to  $\mu$  in the average-case if the probability of the protocol making an error is at most  $\epsilon$  when the inputs are sampled from  $\mu$ .

### Private vs public-coin: Communication cost

One can notice that whenever we are interested on the communication cost, any private-coin protocol can be simulated by public-coin protocol by revealing the private randomness to both parties (both in the one-way and interactive communication setting). More surprisingly, it turns out that every public coin protocol can also be simulated by a private coin protocol with only an additional logarithmic term in the size of the input.

**Theorem 5.1.1** (Public-to-Private [165]). *For a function  $f : \{0, 1\}^n \times \{0, 1\}^n \rightarrow \{0, 1\}$ , let  $\pi_{pub}$  be a public-coin protocol that computes the function  $f$  with a communication cost  $c$  and error  $\epsilon$  in the worst case, then it can be computed by a private-coin protocol with a communication cost  $c + \log(n/\epsilon^2) + \mathcal{O}(1)$  and error  $2\epsilon$  in the worst case.*

We are also interested in exploring the relationship between public-coin protocols and deterministic protocols. In particular, it is well-known that randomness does not provide any advantage over deterministic approaches when minimizing communication costs in a distributional setting [164].

**Lemma 5.1.1.** *For a function  $f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$ , a distribution  $\mu \in \Delta(\mathcal{X} \times \mathcal{Y})$ <sup>1</sup> and a parameter  $\epsilon > 0$ , let  $\pi$  be a public-coin protocol with communication cost  $CC(\pi)$  which computes  $f$  with an error in the average-case no larger than  $\epsilon$ . Then a deterministic protocol  $\pi_{det}$  with communication cost  $CC(\pi)$  exists which computes  $f$  with an error in the average-case no larger than  $\epsilon$ .*

*Proof.* First, let us notice that by fixing a value for the shared randomness  $r$  in the one-way public-coin protocol  $\pi$  we obtain a deterministic protocol  $\pi_r$ . This means that it suffices to prove that there exists a value  $\bar{r}$  for the shared randomness such that the corresponding deterministic protocol  $\pi_{\bar{r}}$  has a communication cost at most  $CC(\pi)$  and an error probability at most  $\epsilon$ . First, by Definition 5.1.1 the communication cost of  $\pi_r$  is still at most  $CC(\pi)$  for

<sup>1</sup>We remind the reader that we use  $\Delta(\mathcal{S})$  to denote the family of all probability distributions on a set  $\mathcal{S}$ .

any  $r$  in the domain of  $R$ . Now we focus on the error probability. First, we write the average error probability  $P_{err}(\pi)$  of protocol  $\pi$  as

$$P_{err}(\pi) := \Pr_{(x,y) \sim \mu, r \sim \mathcal{P}_R} [\pi_{out}(x, y, r) \neq f(x, y)] \quad (5.1)$$

$$= \sum_{x,y,r} \mathcal{P}_R(r) \mu(x, y) (1 - \delta_{\pi_{out}(x,y,r), f(x,y)}) \quad (5.2)$$

$$= \sum_r \mathcal{P}_R(r) P_{err}(\pi_r), \quad (5.3)$$

where  $\mathcal{P}_R$  is the probability distribution of the shared randomness,  $\delta_{i,j}$  is the Kronecker delta, and  $P_{err}(\pi_r) := \sum_{x,y} \mu(x, y) (1 - \delta_{\pi_{out}(x,y,r), f(x,y)})$  is the average error probability of the deterministic protocol  $\pi_r$ . Now, since  $P_{err}(\pi)$  is at most  $\epsilon$ , from (5.3) we complete the proof by noticing that we can always find a value of  $r$  such that  $P_{err}(\pi_r) \leq \epsilon$ .  $\square$

Now that we have defined the various variants of communication complexity problems, we are finally ready to define the average-case and worst-case complexity of a problem, called respectively *distributional complexity* and *communication complexity*.

**Definition 5.1.2** (Distributional complexity). *For a function  $f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$ , a distribution  $\mu \in \Delta(\mathcal{X} \times \mathcal{Y})$  and a parameter  $\epsilon > 0$ , we define the distributional complexity  $D_\mu(f, \epsilon)$  as the communication cost of the cheapest deterministic<sup>2</sup> protocol for computing  $f$  on inputs sampled according to  $\mu$  with an error in the average-case no larger than  $\epsilon$ , i.e.*

$$D_\mu(f, \epsilon) := \min_{\pi: \Pr_{(x,y) \sim \mu} [\pi_{out}(x,y) \neq f(x,y)] \leq \epsilon} CC(\pi). \quad (5.4)$$

**Definition 5.1.3** (Communication complexity). *For a function  $f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$  and a parameter  $\epsilon > 0$ , we define  $R(f, \epsilon)$  as communication cost of the cheapest public-coin protocol for computing  $f$  with error at most  $\epsilon$  in the worst-case.*

$$R(f, \epsilon) := \min_{\pi: \max_{(x,y) \in \mathcal{X} \times \mathcal{Y}} [\Pr_{r \sim \mathcal{P}_R} [\pi_{out}(x,y,r) \neq f(x,y)]] \leq \epsilon} CC(\pi), \quad (5.5)$$

where  $\mathcal{P}_R$  is the probability distribution of the shared randomness.

Surprisingly, these two definitions are linked by a well-known theorem, namely Yao's min-max theorem [70].

**Theorem 5.1.2** (Yao's min-max). *Let everything be as defined in the previous two definitions, then*

$$R(f, \epsilon) = \max_{\mu} D_\mu(f, \epsilon). \quad (5.6)$$

---

<sup>2</sup>One can prove that even in a public-coin model the cheapest protocol is always deterministic directly from Lemma 5.1.1.



## 5.2 Information Complexity

Information complexity is a measure of the minimum amount of information that two parties need to exchange in order to compute a function in a distributed setting. It generalizes the concept of communication complexity, which measures the total number of bits exchanged, by considering the amount of "useful" information in those bits. In essence, information complexity aims to quantify the inherent difficulty of a computational task by accounting for the amount of information that must be communicated, rather than simply the number of bits exchanged.

The concept of information complexity was first indirectly introduced in [166], in the context of information-theoretic security, focusing on the potential for achieving information-theoretically secure two-party computation when the information complexity is kept low. Subsequently, a separate line of research emerged with [167] and [168], establishing lower bounds on communication complexity by employing information-theoretic reasoning. As we shall see, this framework can also be useful in the context of quantum cryptography, where we are concerned about the amount of information leaking to an adversary.

### 5.2.1 External and internal information

Information complexity is a concept that is analogous to communication complexity, where the measure of cost is replaced with information cost. The information cost can refer to either the amount of information exchanged between the two parties, Alice and Bob, referred to as *internal information cost*, or, alternatively, it can refer to the extent of knowledge an external observer without access to the inputs acquires about them, known as *external information cost*. For a comprehensive analysis refer to [169] and [170].

**Definition 5.2.1** (Information Cost). *Let  $\pi$  be a randomized communication protocol on inputs  $\mathcal{X} \times \mathcal{Y}$  and a distribution  $\mu \in \Delta(\mathcal{X} \times \mathcal{Y})$ . The external and internal information cost of  $\pi$  with respect to  $\mu$  denoted by  $IC_\mu^{ext}(\pi)$  and  $IC_\mu^{int}(\pi)$  respectively, are defined as<sup>3</sup>*

$$IC_\mu^{ext}(\pi) := I(\Pi : XY|R) , \quad (5.7)$$

$$IC_\mu^{int}(\pi) := I(\Pi : X|YR) + I(\Pi : Y|XR) , \quad (5.8)$$

where  $\Pi = \Pi(X, Y, R_A, R_B, R)$  describes the transcript of the protocol.

#### Private vs public-coin: information cost

Definition 5.2.1 considers the general case with a randomized protocol using both public and private coins. However, one can notice that is always possible to simulate a public-coin protocol with a private-coin protocol: Alice can disclose part of her private coin  $R_A$  to simulate the shared randomness  $R$ . Although this exchange increases the total communication cost, it does not increase the information cost, as the shared random bits are independent of the input and might not convey any additional information about

<sup>3</sup>An equivalent formulation can be given by conditioning also on the private randomness  $R_A$  and  $R_B$ .

the input itself. Thus, in terms of information complexity, private-coin protocols can be at least as powerful as public-coin protocols, being somehow in the opposite situation of the communication complexity. Remarkably, a converse theorem to Newman's theorem has been established in the context of bounded-round protocols in terms of information complexity [171]. Specifically, any private-coin protocol that consists of  $q$  rounds can be transformed into a public-coin protocol that requires only  $\mathcal{O}(q)$  rounds and reveals merely an additional  $\mathcal{O}(q)^a$  bits of information.

<sup>a</sup>Neglecting logarithmic terms and factors of the communication and information cost.

Similarly to the communication version, we can now define the information complexity of a problem as the infimum over all possible protocols.

**Definition 5.2.2** (Information complexity). *Let  $\pi$  be a private-coin protocol on inputs  $\mathcal{X} \times \mathcal{Y}$  and  $\mu \in \Delta(\mathcal{X} \times \mathcal{Y})$ . The external (internal) information complexity of  $f$  with error tolerance  $\epsilon$  is defined as the infimum of the external (internal) information cost over all private-coin protocols  $\pi$  for computing  $f$  that achieve an error in the average-case no larger than  $\epsilon$  with respect to  $\mu$ :*

$$IC_{\mu}^{ext}(f, \epsilon) := \inf_{\pi: \Pr_{(x,y) \sim \mu, r_A \sim \mathcal{P}_{R_A}, r_B \sim \mathcal{P}_{R_B}}[\pi_{out}(x,y,r_A,r_B) \neq f(x,y)] \leq \epsilon} IC_{\mu}^{ext}(\pi), \quad (5.9)$$

$$IC_{\mu}^{int}(f, \epsilon) := \inf_{\pi: \Pr_{(x,y) \sim \mu, r_A \sim \mathcal{P}_{R_A}, r_B \sim \mathcal{P}_{R_B}}[\pi_{out}(x,y,r_A,r_B) \neq f(x,y)] \leq \epsilon} IC_{\mu}^{int}(\pi), \quad (5.10)$$

where  $\mathcal{P}_{R_A}$  and  $\mathcal{P}_{R_B}$  are the probability distributions of Alice and Bob's private coins respectively.

A set of equivalent definitions can be given in the one-way setting for both communication and information complexity, where the only difference is that the permitted set of protocols is constrained to those in which Alice transmits a single message to Bob.

One can notice that the distributional complexity acts as an upper limit on the information complexity for any given distribution  $\mu$  since it is impossible for one bit of communication to disclose more than one bit of information. Moreover, the external information complexity is always greater than or equal to the internal information complexity. As the intuition suggests, Alice and Bob know more from the beginning, so they necessarily acquire less information, resulting in the following lemma.

**Lemma 5.2.1** (Hierarchies in a distributional setting [172]). *For any function  $f$ , distribution  $\mu$  and average-case error  $\epsilon$ ,*

$$IC_{\mu}^{int}(f, \epsilon) \leq IC_{\mu}^{ext}(f, \epsilon) \leq D_{\mu}(f, \epsilon). \quad (5.11)$$

Moreover, one of the most notable characteristics of internal information complexity is its complete additivity when it comes to task composition.

**Lemma 5.2.2** (Additivity of internal information complexity). *For any function  $f$ , distribution  $\mu$  and average-case error  $\epsilon$*

$$IC_{\mu^n}^{int}(f^n, \epsilon) = n \cdot IC_{\mu}^{int}(f, \epsilon), \quad (5.12)$$

where we denote by  $IC_{\mu^n}^{int}(f^n, \epsilon)$  the internal information complexity for the task of computing  $f$  for  $n$  independent input pairs drawn from  $\mu$  with an average-case error of  $\epsilon$  for each input pair.

The fundamental idea underlying the lemma can be traced back to the works of [173], and it was further developed explicitly in [72, 169, 174]. However, only recently it has been proven that the same is not true for the external information [172]. As it turns out, the additivity of the internal information allows one to link the latter with the distributional complexity, leading to the following result.

**Lemma 5.2.3** (Information equals amortized communication [72]). *For any function  $f$ , input distribution  $\mu$  and error  $\epsilon > 0$*

$$IC_{\mu}^{int}(f, \epsilon) = \lim_{n \rightarrow \infty} D_{\mu}(f^n, \epsilon), \quad (5.13)$$

where  $\lim_{n \rightarrow \infty} D_{\mu}(f^n, \epsilon)$  is usually called the amortized communication.

## 5.2.2 Compression schemes in one-way setting

Now that we have introduced all the standard definitions in the information complexity setting and some of their properties, we can investigate how to link information and communication complexity using compression schemes. In particular, we will now focus on techniques that distill a message  $M$  transmitted by Alice to Bob to its external information  $I(M : XY)$ <sup>4</sup>. We will then apply these techniques to map the one-way external information complexity to the one-way distributional complexity. First, one can immediately notice from the mutual information chain rule that

$$I(M : XY) = I(M : X) + I(M : Y|X) \quad (5.14)$$

$$= I(M : X). \quad (5.15)$$

Here  $I(M : Y|X) = 0$  holds because the message  $M$  is specifically designed to convey information about Alice's input  $X$  alone, which makes it unrelated to Bob's input  $Y$  once  $X$  is already known. This also implies that one can write the external one-way information cost of a protocol  $\pi$  with input distribution  $\mu$  as  $IC_{\mu}^{1,ext}(\pi) := I(\Pi : X)$ . As we shall see, compression schemes in this context prove to be highly effective. In [175], the authors demonstrated that it is possible to compress each message of a protocol to approximately its contribution to the external information cost plus some additional constant term. While the authors focused only on the asymptotic scaling, we carefully derived all the specific constants for the compression scheme. We refer to the Appendix B for a description of how to derive the theorem from [164].

**Theorem 5.2.1** (Message compression). *Consider a message  $M$  sent by Alice, who holds  $X$ , and where  $M$  is sampled from some conditional probability distribution  $P_{M|X}$ . Alice and*

---

<sup>4</sup>We are not considering the shared randomness, since this can always be simulated by a private-coin protocol.

Bob can use public randomness to simulate<sup>5</sup> sending  $M$  by sending an expected number of bits upper bounded by  $I(M : X) + 1.262 \log(1 + I(M : X)) + 11.6$ . The simulation is one round (i.e. only Alice has to send information) and without error.

Finally, one can then map the one-way distributional communication complexity to the external information complexity in a one-way setting, exploiting the message compression in Theorem 5.2.1, obtaining the result in Lemma V.3 of [175] with explicit constants.

**Lemma 5.2.4** (Mapping to information complexity). *Let  $\epsilon, \delta_2 > 0$ ,  $\mu \in \Delta(\mathcal{X} \times \mathcal{Y})$  and  $f : \mathcal{X} \times \mathcal{Y} \rightarrow \mathcal{Z}$ . Then*

$$IC_{\mu}^{1,ext}(f, \epsilon) \geq \frac{\delta_2}{2} D_{\mu}^1(f, \epsilon + \delta_2) - 6 ,$$

where we call  $D_{\mu}^1(f, \epsilon)$  and  $IC_{\mu}^{1,ext}(f, \epsilon)$  respectively the one-way distributional and external information complexity of  $f$  with error  $\epsilon$  on inputs sampled according to  $\mu$ .

*Proof.* Let  $f$  be a function,  $\mu \in \Delta(\mathcal{X} \times \mathcal{Y})$  be a joint probability distribution over the inputs of  $f$ , and  $\pi$  a one-way private-coin protocol which computes  $f$  with error upper bounded by  $\epsilon$  such that

$$IC_{\mu}^{1,ext}(\pi) \leq IC_{\mu}^{1,ext}(f, \epsilon) + 0.05 . \quad (5.16)$$

We use Theorem 5.2.1 to deduce a new one-way public-coin protocol  $\pi'$  such that the average size of the transcript is upper bounded by

$$\mathbb{E}(|\Pi'|) \leq I(\Pi : X) + 1.262 \log(1 + I(\Pi : X)) + 11.6$$

and the error probability is at most  $\epsilon$ . Then we apply the inequality  $1.262 \log(1+x) \leq x+0.3$  for any  $x \geq 0$  to deduce

$$\begin{aligned} \mathbb{E}(|\Pi'|) &\leq I(\Pi : X) + 1.262 \log(1 + I(\Pi : X)) + 11.6 \\ &\leq 2I(\Pi : X) + 11.9 \\ &\leq 2IC_{\mu}^{1,ext}(f, \epsilon) + 12 , \end{aligned}$$

where in the last inequality we used (5.16). By using Markov's inequality, we can create a new protocol  $\pi''$  which is identical to  $\pi'$  except when the transcript  $\Pi''$  has size greater than  $\frac{1}{\delta_2} \mathbb{E}(|\Pi'|)$ , then the protocol simply aborts. By suitably fixing the public randomness, thanks to Lemma 5.1.1, we obtain a deterministic protocol which has probability to fail upper bounded by  $\epsilon + \delta_2$  and a communication cost at most  $\frac{2IC_{\mu}^{1,ext}(f, \epsilon) + 12}{\delta_2}$ . The lemma then follows from Definition 5.1.2 (see Eq. (5.4)).  $\square$

This result forms a key step in our security proof of the quantum cryptographic protocol presented in Chapter 7. Now the natural question is whether a similar result can be achieved in the case of internal information complexity: as it turns out, this is a harder problem. Although there are known compression schemes that effectively simulate the one-way communication by reducing its communication cost to almost the internal information, they require employing multiple rounds of communication to simulate the message, such as the scheme presented in [72]. Unfortunately, this prevents us from obtaining a map between one-way distribution and internal information complexity equivalent to the one in Lemma 5.2.4.

---

<sup>5</sup>Instead of sending directly  $M$ , Alice and Bob can use their shared randomness to decrease the number of bits Alice has to send, while Bob can still retrieve completely the message  $M$ .

## 5.3 Quantum Communication Complexity

Let us now consider a possible extension of communication complexity which make use of quantum correlations. Yao first introduced this model [70] in the context of a two-way randomized communication complexity model where both parties are allowed to exchange quantum states. Subsequently, Cleve and Buhrman [176] proposed an alternative model where participants could share entangled states and communicate using classical bits. Since a protocol in the former model can always be converted to the latter thanks to quantum teleportation [133], for the rest of this thesis we will only consider the case where Alice and Bob are allowed to exchange quantum states, but they don't have access any pre-shared entanglement. Moreover, we will call  $Q(f, \epsilon)$  the "quantum version" of the communication complexity  $R(f, \epsilon)$ .

Although quantum communication complexity offers advantages over classical communication complexity in several scenarios, this is not immediately evident due to *Holevo's theorem* (see Theorem 2.3.1). This theorem stipulates that the information retrieved from  $n$  qubits does not exceed the information retrieved by  $n$  classical bits. However, in most communication complexity tasks, the objective is not to identify the input itself (where quantum communication does not offer an advantage over classical communication), but to determine a function  $f$  of the input. In these cases, quantum communication complexity can provide significant advantages compared to classical communication complexity [3, 73, 177–179].

### 5.3.1 $\beta$ -Partial Matching Problem

In this section we shall present the quantum communication complexity problem, called  $\beta$ -Partial Matching ( $\beta$ PM) problem, for which  $\Omega(\sqrt{n})$  bits of communication from Alice to Bob are required, against only  $\mathcal{O}(\log(n))$  qubits, with  $n$  the length of input  $x$ . In particular, we will analyze the best-known quantum and classical protocols and a lower bound for its one-way distributional complexity for a particular input distribution  $\mu_{\beta PM}$ .

Let  $n \in \mathbb{N}$  and define the notation  $[n] = \{1, \dots, n\}$ . In the following  $n$  will be assumed to be even. A *matching*  $M$  is a set of pairs  $(a, b) \in [n]^2$ , such that no two pairs contain the same index, where, each index is called a *vertex* and a pair of vertices is called an *edge*. For example if  $n = 4$  then the set of edges  $\{(1, 2), (3, 4)\}$  or  $\{(2, 3)\}$  are valid matchings whereas  $\{(1, 2), (2, 3)\}$  are not. See Fig. 5.2 for a pictorial representation. We say  $M$  is a  $\beta$ -*matching* if in addition  $|M| = \beta n$ . The  $\beta$ PM problem is built around a  $\beta$ -matching  $M$ , that constitutes part of the input given to Bob.  $M$  consists of a sequence of  $\beta n$  disjoint edges  $(i_1, j_1) \dots (i_{\beta n}, j_{\beta n})$  over  $[n]$ . We will call  $\mathcal{M}_{\beta n}$  the set of all  $\beta$ -matchings on  $n$  bits: if  $\beta = \frac{1}{2}$  the matching is called *perfect* and if  $\beta < \frac{1}{2}$  the matching is called *partial*.  $M$  can be represented as a  $\beta n \times n$  matrix with only a single one in each column and two ones per row, namely at position  $i_l$  and  $j_l$  for the  $l$ -th row of matrix  $M$ . Let  $x \in \{0, 1\}^n$ , applying the matching  $M$  to  $x$  leads to the  $\beta n$ -bit string  $v = v_1, \dots, v_l, \dots, v_{\beta n}$  where  $v_l = x_{i_l} \oplus x_{j_l}$ . Finally, we call  $a^{\beta n}$  a vector of dimension  $\beta n$  with value  $a$  in each component. Using the notation above, we can finally define the  $\beta$ PM problem:

### $\beta$ -Partial Matching: problem formalization

**Alice's input:**  $x \in \{0, 1\}^n$ .

**Bob's input:**  $M \in \mathcal{M}_{\beta n}$  and  $\omega \in \{0, 1\}^{\beta n}$ .

**Promise on the input:** given a bit  $a \in \{0, 1\}$ , then  $\omega = Mx \oplus a^{\beta n}$ .

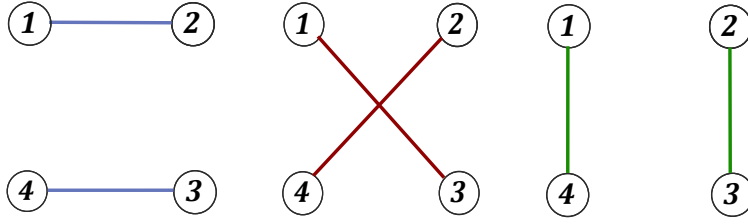
**Communication model:** one-way communication between Alice and Bob.

**Goal:** Bob outputs the bit  $a$  with high probability.

We shall call for clarity  $\mathcal{X} := \{0, 1\}^n$ ,  $y := (M, \omega)$  and  $\mathcal{Y} := \mathcal{M}_{\beta n} \times \{0, 1\}^{\beta n}$ .

Then, one can define the (partial) function  $\beta PM : \mathcal{X} \times \mathcal{Y} \rightarrow \{0, 1\}$  as the function that randomly picks an element from the vector  $Mx \oplus \omega$ .

**Input distribution:** we call  $\mu_{\beta PM} \in \Delta(\mathcal{X} \times \mathcal{Y})$  the input probability distribution uniform over  $x \in \{0, 1\}^n$  and  $M \in \mathcal{M}_{\beta n}$ . The inputs  $x$  and  $M$  together determine the  $\beta n$ -bit string  $v = Mx$ . To complete the input distribution, with probability  $1/2$  we set  $\omega = v$  and with probability  $1/2$  we set  $\omega = \bar{v}$ .



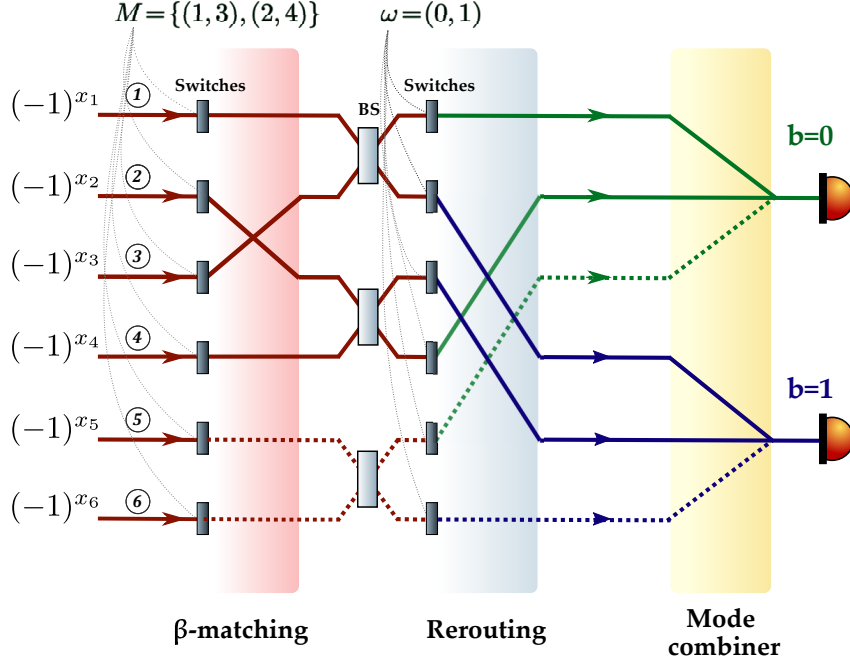
**Figure 5.2:** Illustration of a set of perfect matchings for size  $n = 4$ . For example, considering  $x = 1001$ ,  $\omega = 11$ , for the first perfect matching in blue we have  $Mx = \begin{bmatrix} x_1 \oplus x_2 = 1 \\ x_3 \oplus x_4 = 1 \end{bmatrix}$ , resulting in  $a = 0$ .

### Best-known quantum protocol

Using a simple quantum protocol, the above task can be solved by transmitting only a  $n$ -dimensional quantum state [3]. Alice sends a uniform superposition of her bits to Bob:

$$|\psi_x\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^n (-1)^{x_i} |i\rangle. \quad (5.17)$$

Bob completes his  $\beta n$  edges to a perfect matching in an arbitrary way and measures with the corresponding set of  $n/2$  rank 2 projectors, where for an edge  $(a, b)$  the projector is  $P = |a\rangle\langle a| + |b\rangle\langle b|$ . With probability  $2\beta$  he will receive an output corresponding to one of the edges  $(i_l, j_l)$  from his input  $\beta$ -matching  $M$ . The state then collapses to  $\frac{1}{\sqrt{2}}((-1)^{x_{i_l}} |i_l\rangle + (-1)^{x_{j_l}} |j_l\rangle)$ , from which Bob can obtain the bit  $v_l = x_{i_l} \oplus x_{j_l}$  using a measurement containing projectors  $\{|+\rangle\langle +|, |-\rangle\langle -|\}$ , where  $|+\rangle = (|i_l\rangle + |j_l\rangle)/\sqrt{2}$  and  $|-\rangle = (|i_l\rangle - |j_l\rangle)/\sqrt{2}$ , and immediately retrieve the bit  $a$ . With probability  $1 - 2\beta$ , instead, he will receive an output that doesn't correspond to any edge of the  $\beta$ -matching  $M$ : in this case, he immediately outputs  $b = \perp$ ,



**Figure 5.3:** Illustration of a possible implementation of Bob's decoding with  $n = 6$  spatial modes and  $\beta = 1/3$ . In the  $\beta$ -matching part Bob uses his knowledge of  $M$  to control each switch and direct each mode to the corresponding beam splitter (BS). The modes with dotted lines are blocked instead, since they don't correspond to any vertex of the partial matching. Then, in the rerouting part, he reorders the modes based on  $\omega$ . Finally, thanks to a mode combiner, he directs the first (second) half of the modes to the first (second) detector.

aborting the protocol. By repeating a constant number of times they can achieve correctness  $\epsilon_{cor}$  for any small constant  $\epsilon_{cor}$ .

As depicted in Figure 5.3, the final measurement can always be thought as a linear operator  $\mathcal{L}_{\beta\text{BM}}(y)$ , which represents the  $\beta$ -matching and rerouting part in Figure 5.3, followed by a projection on two orthogonal subspaces corresponding to  $b = 0$  and  $b = 1$  respectively. See Appendix C.1.1 for a complete description of  $\mathcal{L}_{\beta\text{BM}}(y)$ .

### Classical lower-bound and best-known classical protocol

Now that we have introduced the best-known quantum protocol, we present the scaling law for the lower bound of the one-way distributional complexity of the  $\beta\text{PM}$  protocol, showing an exponential gap in the amount of communication required between quantum and classical strategies.

**Theorem 5.3.1.** *Let  $\beta \in (0, 1/4]$  and  $\mu_{\beta\text{PM}}$  be the input distribution introduced in Section 5.3.1. Then,  $\forall \epsilon \in (0, \frac{1}{2}]$*

$$D_{\mu_{\beta\text{PM}}}^1(\beta\text{PM}, \epsilon) \geq k(\epsilon)\sqrt{n} + d(\epsilon), \quad (5.18)$$

where

$$k(\epsilon) = \frac{1}{50e\sqrt{\beta}} \left(\frac{1}{2} - \epsilon\right)^2 \quad \text{and} \quad d(\epsilon) = 2 \log\left(\frac{1}{2} - \epsilon\right) + 2(\log(2) - \log(5)). \quad (5.19)$$

*Proof.* A complete description of how to derive this theorem from [3] is given in Appendix C.1.2.  $\square$

Moreover, directly from Lemma 5.2.4, we obtain a bound on the external information complexity, which will be a crucial ingredient for the security proof of the key distribution protocol presented in Chapter 7. Finally, we analyze the best-known classical protocol  $\pi_{\beta PM}$ , which has already been sketched in [3].

**Classical protocol  $\pi_{\beta PM}$ .** Alice and Bob can exploit their public randomness to agree on a subset  $\mathbf{s} := \{j_1, \dots, j_d\} \in \mathcal{S}$ , where  $\mathcal{S}$  is the set of all the possible subsets of  $d$  indices in  $[n]$ . Subsequently, Alice transmits the corresponding bit values  $x_{\mathbf{s}} := (x_{j_1}, x_{j_2}, \dots, x_{j_d})$  to Bob. As such, the communication cost of this protocol is  $d$ . Consequently, in this protocol, Bob receives the corresponding  $\frac{d(d-1)}{2}$  edges<sup>6</sup>. Finally, Bob, by knowing  $\omega$ , can give the right answer whenever he gets at least an edge in the matching  $M$  and randomly guesses the bit otherwise.

From our analysis, presented in Appendix C.1.3, we find an upper bound of the error probability.

**Theorem 5.3.2.** *Let  $d \in \mathbb{N}$ . An explicit one-way public-coin protocol  $\pi_{\beta PM}$  exists with a communication cost  $CC(\pi_{\beta PM}) = d$  which solves the  $n$ -dimensional  $\beta PM$  protocol with an error probability for any input at most*

$$\epsilon_{\beta PM}(d) = \sum_{k=0}^d \frac{\binom{2\beta n}{k} \binom{n-2\beta n}{d-k}}{2^{\binom{n}{d}}} e^{-\frac{k(k-1)}{4\beta n}}. \quad (5.20)$$

Specifically, we have numerically shown that a communication cost of  $\mathcal{O}(\sqrt{n})$  is sufficient to solve the problem with a constant probability for any input distribution. This results in an upper bound for the one-way distributional complexity of  $\mathcal{O}(\sqrt{n})$  for any input distribution. Furthermore, in the context of calculating a non-asymptotic upper bound, one can simply define

$$CC^\circ(\beta PM, \epsilon) := \min\{d \in \mathbb{N} \mid \epsilon_{\beta PM}(d) \leq \epsilon\}. \quad (5.21)$$

From Theorem 5.3.2 and Definition 5.1.2, we then obtain, for any input distribution  $\mu$ ,

$$D_\mu^1(\beta PM, \epsilon) \leq CC^\circ(\beta PM, \epsilon). \quad (5.22)$$

### 5.3.2 Vector in a Subspace Problem

The Vector in a Subspace (VS) problem is another communication problem where one party Alice receives a unit vector  $x \in \mathbb{R}^n$  and Bob receives a subspace  $H \subseteq \mathbb{R}^n$  of dimension  $\lfloor n/2 \rfloor$  such that either  $x \in H$  or  $x \in H^\perp$ . Their goal is to answer 0 if  $x$  is in  $H$  and 1 if  $x$  is in  $H^\perp$ . In particular, we will focus on the case where both the unit vector  $x$  and the subspace  $H$  are picked from a uniform distribution, with the promise that  $x$  is either in  $H$  or  $H^\perp$ . We call  $\mu_{VS}$  the corresponding joint distribution.

---

<sup>6</sup>Whenever we say that Bob receives an edge, say  $(j_1, j_2)$ , it implies that he acquires the bit values assigned to the corresponding vertices, i.e.  $(x_{j_1}, x_{j_2})$ .



## Best-known quantum protocol

A one-way quantum protocol is known that only requires  $\mathcal{O}(\log n)$  qubits and no shared randomness between Alice and Bob [180]. The protocol involves Alice creating a quantum state

$$|\psi_x\rangle = \sum_{i=1}^n x_i |i\rangle \quad (5.23)$$

and transmitting it to Bob, who then executes a projective measurement onto the subspaces  $H$  and  $H^\perp$ ). In this protocol, Alice's encoding is based on the relative amplitudes, contrasting with the  $\beta$ PM quantum protocol where the information is encoded in the relative phases. On the other hand, Bob's decoding can also be executed using only two detectors, given that the VS problem produces a boolean output. As a matter of fact, the decoding process can be visualized as a random orthogonal matrix coupled with a mode combiner.

## Classical lower bound and best-known classical protocol

In the study by Regev et al. [73], the authors established a lower bound of  $\Omega(n^{1/3})$  for the two-way classical distributional complexity when the inputs are derived from the uniform distribution  $\mu_{VS}$ . However, the lower bound presented in their work is not considered to be definitive. They propose that a lower bound of  $\Omega(\sqrt{n})$  is likely to be more accurate. In support of this conjecture, a restricted version of the problem was examined in the study by Grupel et al. [181], where they established an optimal lower bound of  $\Omega(\sqrt{n})$  bits.

What's even more interesting is that the classical lower bound for the general problem was extended in a subsequent study [182] to encompass two-way internal information complexity. This marked the first instance of demonstrating an exponential separation between one-way quantum communication complexity and two-way internal information complexity. As indicated by Lemma 5.2.1, demonstrating an exponential separation with the two-way internal information complexity is the most challenging task.

Finally, we analyze the best-known classical protocol  $\pi_{VS}$ , sketched in [177].

**Classical protocol  $\pi_{VS}$ .** Let  $z_1, \dots, z_n$  be  $n$  mutually independent random elements in  $\mathbb{R}$ , each chosen according to the normal distribution  $\mathcal{N}(0, n^{-1})$ , that is, each  $z_i$  has the normal distribution with expectation 0 and variance  $n^{-1}$ . The distribution of  $z = (z_1, \dots, z_n)$  in  $\mathbb{R}^n$  is hence multi-normal (we call this distribution  $\psi$ ). Let  $k = \lfloor 2^{C\sqrt{n}} \rfloor$ , where  $C$  is a large enough constant. Let  $z^1, \dots, z^k$  be  $k$  mutually independent random elements of  $\mathbb{R}^n$ , each chosen according to the distribution  $\psi$ . We assume that both players can see  $z^1, \dots, z^k$  (using their pre-shared secret). Let  $z^{\hat{j}}$  be the element in  $\{z^1, \dots, z^k\}$  with the largest scalar product with the input vector  $x \in S^{n-1} \cap H$  (same analysis for  $H^\perp$ ). Alice knows the value of the index  $\hat{j}$  and sends that index to Bob. Now Bob knows vector  $z^{\hat{j}}$ . He will answer 0 if  $z^{\hat{j}}$  is closer to  $H$  and 1 if  $z^{\hat{j}}$  is closer to  $H^\perp$ . The total communication cost of the protocol is  $C\sqrt{n}$ .

Similar to the  $\beta$ PM problem, we only introduce the key theorem here that establishes an upper boundary for the error probability. The comprehensive derivation of this theorem can be found Appendix C.2.

**Theorem 5.3.3.** *Let  $d$  be an integer. An explicit one-way public-coin protocol  $\pi_{VS}$  exists with a communication cost  $CC(\pi_{VS}) = d$  which solves the  $n$ -dimensional VS problem protocol with an error probability at most*

$$\epsilon_{VS}(d) = \min_{t_1, t_2 > 0} 1 - \left(1 - e^{-\frac{(T_1+T_2)^2}{8}}\right) \left(1 - 2e^{-\frac{t_2^2}{2}}\right) \left(1 - \frac{1}{t_1^2}\right) \quad (5.24)$$

with  $T \equiv \sqrt{\frac{d}{\pi}} - \sqrt{4\sqrt{n}(t_1 + t_2) + 2\sqrt{2}t_1t_2}$ .

As in the case of the  $\beta$ PM problem, we notice that a communication cost of  $\mathcal{O}(\sqrt{n})$  is sufficient to solve the problem with a constant probability for any input distribution, resulting in an upper bound for the one-way distributional complexity of  $\mathcal{O}(\sqrt{n})$ . We can now again obtain a non-asymptotic upper bound by defining

$$CC^\circ(VS, \epsilon) := \min\{d \in \mathbb{N} \mid \epsilon_{VS}(d) \leq \epsilon\}. \quad (5.25)$$

### 5.3.3 Comparison between the two problems

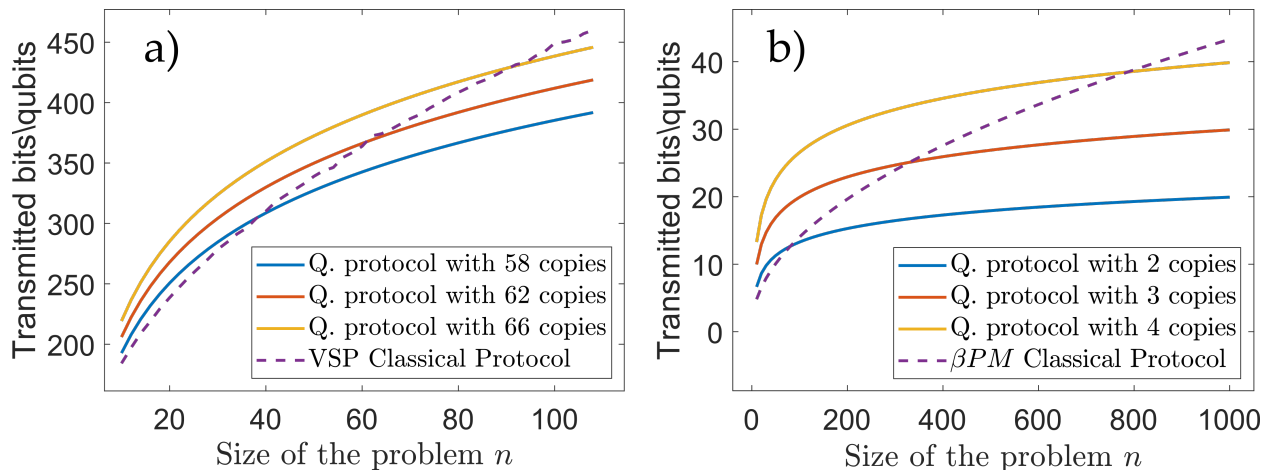
We now summarize all the bounds we have analyzed for the VS problem and the  $\beta$ PM problem in Table 5.1.

|                        | VS  | $\beta$ PM  |
|------------------------|---|---|
| <b>Lower bounds</b>    | $IC_{\mu_{VS}}^{int}(VS, \epsilon) = \Omega(n^{1/3})$                                   | $IC_{\mu_{\beta PM}}^{1,ext}(\beta PM, \epsilon) = \Omega(\sqrt{n})$                          |
| <b>Q. upper bounds</b> | $Q^1(VS, \epsilon) = \mathcal{O}(\log(n))$  | $Q^1(\beta PM, \epsilon) = \mathcal{O}(\log(n))$  |
| <b>C. upper bounds</b> | For any input distribution $\mu$ :<br>- $D_\mu^1(VS, \epsilon) = \mathcal{O}(\sqrt{n})$ | For any input distribution $\mu$ :<br>- $D_\mu^1(\beta PM, \epsilon) = \mathcal{O}(\sqrt{n})$ |

**Table 5.1:** Comparison of the lower and upper bounds of the VS and  $\beta$ PM problems. We only present the most powerful bounds for each category: for example, an upper bound on the one-way distributional complexity implies an upper bound on the one and two-way information complexities. The color coding of the cells indicates the status of prefactor evaluation: Green cells represent bounds where prefactors have been evaluated in a noiseless model, yellow cells indicate evaluations based on a realistic noise model, and red cells are for bounds for which prefactor evaluations are not currently available. The  $\beta$ PM lower bounds are only valid for  $\beta \in (0, \frac{1}{4}]$ .

However, as we conclude this section, one important question remains open: which of the two protocols is harder to implement in the classical model? Let's say we set a target error probability at 0.2. We can then compare the upper limit of transmitted bits from the best

classical protocol with the number of transmitted qubits in a one-way quantum protocol. In particular, we allow Alice to send multiple copies of the same  $n$ -dimensional quantum state. As we'll explore in upcoming chapters, the ability to send multiple copies to solve the problem enhances the practicality of the implementation. It allows for compensation for potential losses and increases resilience to noise. Finally, given  $m$  copies sent, the amount of qubits transmitted is simply upper bounded by  $m\lceil\log(n)\rceil$ .



**Figure 5.4:** Comparison between transmitted bits/qubits for classical and quantum upper bounds for an error probability of  $\epsilon = 0.2$ . In **a)** we compare the upper bound for VS classical protocol, obtained from Eq. (5.25), with quantum protocols sending up to 66 copies. In **b)** we compare the  $\beta PM$  classical protocol for  $\beta = 1/4$ , obtained from Eq. (5.21), with quantum protocols sending up to 4 copies.

As observed in Figure 5.4, at a fixed size of the problem  $n$ , the VS classical protocol requires to send many more bits compared to the  $\beta PM$  problem. For instance, when considering  $n = 100$ , fewer than 15 bits are required for the  $\beta PM$  problem, in contrast to over 400 for the VS. The plot also illustrates how one could implement the quantum protocol for the VS problem with several copies of the same quantum state and still outperform its classical upper bound even for relatively modest values of  $n$  (e.g. less than 100).

# QUANTUM CRYPTOGRAPHY AGAINST A BOUNDED ADVERSARY

## Contents

---

|            |   |           |
|------------|---|-----------|
| <b>6.1</b> | <b>Introduction</b>                                   | <b>82</b> |
| <b>6.2</b> | <b>Quantum data locking</b>                           | <b>82</b> |
| 6.2.1      | General protocol                                      | 82        |
| 6.2.2      | Security with accessible information                  | 84        |
| 6.2.3      | Practical quantum data locking                        | 85        |
| <b>6.3</b> | <b>Noisy-storage model</b>                            | <b>86</b> |
| 6.3.1      | Physical assumption                                   | 86        |
| 6.3.2      | Quantifying adversarial information                   | 86        |
| <b>6.4</b> | <b>Quantum computational time-lock security model</b> | <b>90</b> |
| 6.4.1      | Computational and physical assumptions                | 90        |
| 6.4.2      | Validity of QCT model                                 | 91        |
| 6.4.3      | Rationale of the QCT model                            | 92        |
| 6.4.4      | Quantifying adversarial information                   | 93        |
| <b>6.5</b> | <b>Conclusion</b>                                     | <b>95</b> |

---

In this chapter, we examine various security models proposed in quantum cryptography literature that impose additional constraints on the capabilities of an eavesdropper. In particular, we present a hybrid security model, introduced for the first time in [78], which will be utilized in Chapter 7 to construct an everlasting key distribution scheme.

## 6.1 Introduction

QKD is renowned for its ability to offer security against adversaries with unrestricted technological capabilities. These adversaries are assumed to possess boundless resources, including a universal quantum computer with unlimited computational power and a perfect quantum memory with infinite capacity. However, it is important to acknowledge that these assumptions may be unrealistic given the current state of quantum technology development. This creates a disparity between the anticipated technological advancements and the capabilities attributed to Eve.

Alternative security scenarios can be explored to address this disparity, considering the technological limitations that potential eavesdroppers may face. These are also called *physical assumptions*. We examine multiple examples of such security models, exploring the benefits of considering an eavesdropper with imperfect quantum memories. Firstly, we explore the assumption that Eve can perfectly store an unlimited number of qubits in a quantum memory, but only for a finite period of time, analyzing a cryptographic construction called Quantum Data Locking (QDL). Secondly, we consider the Noisy-Storage Model (NSM), which accounts for limited and noisy quantum storage resources available to adversaries. However, both QDL and the NSM do not rely on any computational assumptions, but they force the adversary to store the quantum states by intentionally delaying the classical post-processing. While such an approach establishes security adequately, it does pose apparent challenges, particularly when the focus is on enhancing communication speed, which is an important consideration in practical scenarios.

In the final section of this chapter, we introduce a novel hybrid security model, the Quantum Computational Time-lock (QCT). This model aims to address the aforementioned challenges by leveraging both physical and computational assumptions. In particular, we will analyze its validity and the level of security that it can provide. It's worth noting that this model will find practical application in a forthcoming chapter, namely Chapter 7, where we detail a key distribution protocol operating within the QCT paradigm.

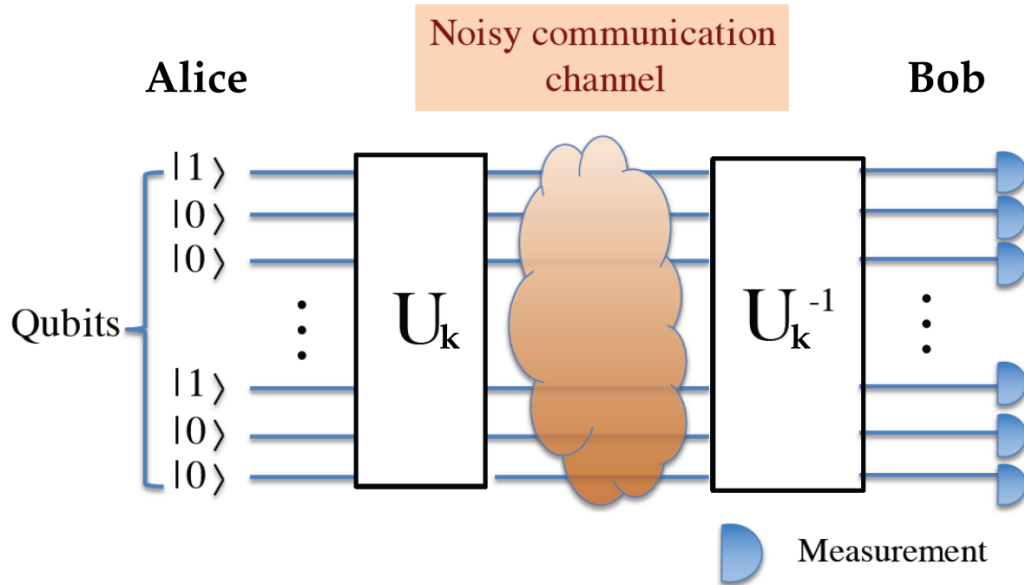
## 6.2 Quantum data locking

Quantum data locking is a quantum phenomenon that enables the encryption of long messages using a short secret key while maintaining information-theoretic security. This stands in stark opposition to classical information theory, where, as per Shannon's principle, the secret key's length must match or exceed the message's length. This phenomenon can be leveraged to achieve efficient QKD protocols, given the additional assumption that any adversary possesses quantum storage of infinite capacity, but can only maintain quantum information for a restricted period of time.

### 6.2.1 General protocol

A typical QDL protocol requires a sender (Alice) and a receiver (Bob) to have access to a short pre-shared secret  $k$ , which is used to agree on a code, for example a set of basis vectors. Alice can then send encrypted information to Bob by applying the corresponding

unitary transformation  $U_k$ . Since it knows the secret  $k$ , Bob can then apply the inverse transformation  $U_k^{-1}$ , followed by a measurement in the computational basis. This process is illustrated in Fig. 6.1.



**Figure 6.1:** QDL protocol's circuit layout. Alice and Bob already possess a shared secret key  $k$ . Alice utilizes this key to encrypt her message using a unitary operation  $U_k$ . Bob, on the other hand, decrypts by performing the reverse operation  $U_k^{-1}$ . Figure from [183].

More formally, one can divide a general QDL protocol into 5 main steps.

### QDL protocol steps

1. **Unitary set agreement:** Prior to any quantum communication, both Alice and Bob agree on a set of  $K$  unitary matrices, represented as  $\{U_k\}_{k=1\dots K}$ . Each matrix in this set represents a distinct basis within the Hilbert space of dimension  $d$ . The elements of the computational basis are symbolized by  $\{|j\rangle\}_{j=1\dots d}$ , and applying the unitary  $U_k$  to this basis results in  $\{U_k|j\rangle\}_{j=1\dots d}$ .
2. **Unitary selection:** Using a secret key that is  $\log K$  bits long, Alice selects a specific unitary transformation from the shared set. This transformation corresponds to a particular basis among the  $K$  agreed-upon bases.
3. **Quantum encoding:** From her chosen basis, Alice selects  $M$  vectors, labeled as  $\{U_k|j_a\rangle\}_{a=1\dots M}$ . These vectors act as her quantum encoding method to transmit  $\log M$  bits of classical information through the channel. This transposition of classical data into quantum system  $Q$  can be characterized by the classical-quantum state

$$\rho_{AQ}^k = \frac{1}{M} \sum_{a=1}^M |a\rangle\langle a| \otimes U_k |j_a\rangle\langle j_a| U_k^\dagger. \quad (6.1)$$

4. **Quantum decoding:** Bob applies the inverse unitary  $U_k^\dagger$  and then measures in the computational basis.
5. **Error correction:** Alice and Bob can communicate reliably over a noisy channel by performing standard error correction, transmitting at rates under the channel's capacity  $r = I(A; B|K)$ , where  $I(A; B|K)$  measures the mutual information between Alice's input  $A$  and Bob's measurement  $B$ , given their shared secret key  $K$ .

## Possible security frameworks

Within the realm of QDL, two distinct security frameworks can be identified [74]. In the context of *Weak QDL*, Alice and Bob communicate over a noisy quantum channel, with Eve intercepting by measuring the channel's environment. This situation is technically characterized by asserting that Eve can tap into the output of the complimentary channel bridging Alice to Bob. Notice that this is analogous to Wyner's wiretap channel model [184]. Conversely, in *Strong QDL*, Eve is assumed to be able to measure the very input of Alice and Bob's channel. This means that the classical-quantum state describing the correlation between the classical message and Eve's quantum state is of the form of Eq. (6.1). The focus of our following discussions will be oriented towards the Strong QDL framework.

### 6.2.2 Security with accessible information

As presented in Chapter 3, the accepted security criterion in the quantum cryptography community is the *trace-distance criterion*. However, this has not always been the case: in the early stage of quantum cryptography, researchers relied on a different criterion, based on the *accessible information*. This criterion requires to bound the classical mutual information between the classical message and the result of any measurement  $\mathcal{Z}$  Eve can make on her quantum system  $Q$

$$I_{acc}(A : Q) := \max_{\mathcal{Z}} I(A : \mathcal{Z}(Q)). \quad (6.2)$$

While this approach might appear practical at first glance, it turns out that it is, in general, not composable [121]. The non-composability of accessible information is rooted in its underlying assumptions about Eve's strategy. Specifically, it presumes that Eve performs a measurement right after the quantum communication is over. However, this might not be the most strategic choice for her. Instead, Eve could opt to withhold her measurements until some additional information has leaked. This delay allows her the opportunity to adapt and refine her measurement tactics based on this additional knowledge, exploiting what is called the *locking of accessible information* [185].

## Locking of accessible information

Let's consider an extension of the setting described in Eq. (6.1), where now the eavesdropper has also access to an additional random variable  $Y$ , resulting in a ccq state  $\rho_{AYQ}$ . Let

$$\Delta := I_{acc}(A : YQ) - I_{acc}(A : Q) \quad (6.3)$$

be the increase in accessible information about  $A$  when the classical information  $Y$  is added to the quantum system  $Q$ . Then we say that the accessible information is *lockable* [185] if  $\Delta$  can be larger than the size of the additional information  $Y^a$ .

<sup>a</sup>The locking property is inherently quantum in nature. When the quantum system  $Q$  is substituted with a classical random variable  $Z$ , we get  $\Delta = I(A : Y|Z) \leq H(Y)$ . This implies that  $\Delta$  can't surpass the size of  $Y$ .

Nevertheless, a core assumption in QDL postulates that Eve can only reliably store quantum information for a finite duration, with Alice and Bob being aware of this maximum storage time. Leveraging this information, they can delay the error correction until after the quantum memory's decoherence time, circumventing the unintended unlocking of Eve's accessible information. This precaution guarantees that any potential eavesdropper would have already measured their portion of the quantum system. Moreover, as shown in [186], one can make a QDL protocol robust against leakage to Eve of part of the message before the expiration time of her quantum memory. This is achieved by increasing the length of the key by a proportionate amount, solidifying the accessible information as a reliable figure of merit for security evaluations.

### 6.2.3 Practical quantum data locking

Initially, QDL protocols involved coherent control over very large Hilbert spaces, including challenging tasks like sampling random unitaries based on the Haar measure [187], or performing universal quantum computations [188]. Hence, given their complexity, these protocols were far from being feasible in practical experiments, not even for basic demonstrations.

Several years later, in 2014, Lupo et al. introduced a more feasible QDL protocol in [74], which necessitated only local random unitaries within a small  $d$ -dimensional Hilbert space. This particular protocol could be implemented using a sequence of  $n$  photons, with each photon existing in a  $d$ -dimensional Hilbert space. While the protocol demands a large number of photons, it ensures security while keeping the dimensionality  $d$  conveniently small.

This pragmatic shift led to the first hands-on experiments two years later [189], where spatial light modulators created pseudo-random unitary transformations on the photon's wavefront. This method, which we'll explore in detail in Chapter 8, successfully demonstrated how to encrypt 6 bits per photon using less than 6 bits per photon of secret key. However, while the single-photon encoding over  $d$  spatial modes shown in [189] is practical from an implementation standpoint, its transmission rate is limited to  $\log d/d$  bits per mode.

More recently, drawing inspiration from Boson Sampling [190], a more efficient use of resources was proposed in [191], where the message is encoded using multiple photons across



many modes. This approach significantly enhances the transmission rate per photon, asymptotically achieving the limit of 1 bit per mode.

## 6.3 Noisy-storage model

We now review some notions regarding the NSM, which is mainly studied in cryptographic tasks between two parties that do not necessarily trust each other, such as quantum bit commitment [192] and quantum oblivious transfer [193]. Our primary emphasis will be on exploring the methodologies used to ensure security within this framework. It's noteworthy to mention that, from an experimental standpoint, there have already been significant demonstrations in this domain. The experimental execution of these protocols has been showcased using contemporary hardware typically employed for quantum key distribution [194, 195]. Additionally, an experimental realization of a quantum protocol for oblivious transfer has been presented for optical continuous-variable systems [196].

### 6.3.1 Physical assumption

The main physical assumption in this setting is that no large-scale reliable quantum storage is available to the adversary at the time of the execution of the protocol. Otherwise, the adversary remains arbitrarily powerful: they have the capability to carry out any form of quantum operations/computations, utilize any encoding and decoding processes, and hold an infinite quantity of classical information. A quantum memory within the broader NSM can be conceptualized as a device accepting inputs from a specific Hilbert space, denoted as  $\mathcal{H}_{Q_{in}}$ . Since it undergoes decoherence, if such a memory retains an initial state  $\rho_{in} \in \mathcal{D}(\mathcal{H}_{Q_{in}})$  for a duration  $t$ , the resultant state is  $\Phi_t(\rho) \in \mathcal{D}(\mathcal{H}_{Q_{out}})$ . Here,  $\Phi_t : \mathcal{L}(\mathcal{H}_{Q_{in}}) \rightarrow \mathcal{L}(\mathcal{H}_{Q_{out}})$  represents a CPTP map. We operate under the basic assumption that the noise exhibits Markovian characteristics. Hence, the set  $\{\Phi_t\}_{t>0}$  forms a continuous one-parameter semigroup, expressed as

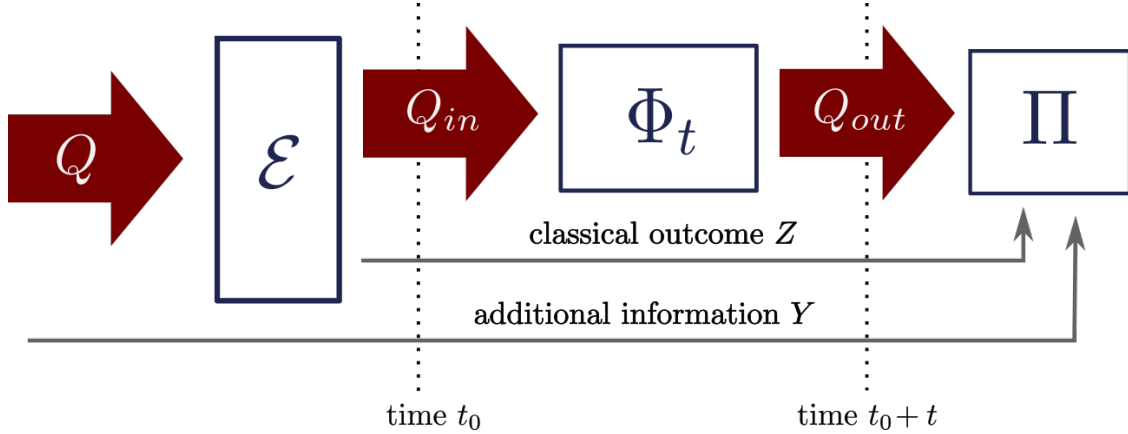
$$\Phi_0 = \mathbb{1} \quad \Phi_{t_1+t_2} = \Phi_{t_1} \circ \Phi_{t_2} . \quad (6.4)$$

This indicates that storage noise increases over time, preventing an adversary from obtaining useful information by postponing the readout. Moreover, since the quantum storage assumption needs to hold only at the time of the execution of the protocol, its security cannot be compromised retroactively, even if we develop more advanced quantum memories in the future. As previously noted, the principal strategy to obtain security in this security model involves introducing a specific time delay, denoted as  $t$ . Within this framework, the optimal strategy for an adversary is to retrieve the information from the device right after time  $t$ , since any additional delay will only lead to a further increase in the amount of noise.

### 6.3.2 Quantifying adversarial information

Despite the framework of two-party cryptography being fundamentally different from QKD, where Alice and Bob do trust each other, and the third party Eve is eavesdropping, the uncertainty relations used to prove security are general and useful in different scenarios.

In order for us to provide a good overview of how one usually proves security in this model, let us consider a general scenario, where an adversary wants to guess the value of a random variable  $A$ . In particular, they immediately have access to some quantum information  $Q$ , and after a time  $t$  obtain some additional classical information  $Y$ . Without loss of generality, one can consider the following strategy, illustrated in Figure 6.2, to retrieve as much information as possible about  $A$ .



**Figure 6.2:** General encoding attack. It consists of an encoding  $\mathcal{E}$  that maps (conditioned on some classical outcome  $Z$ ) the adversary’s quantum system to the memory input  $Q_{in}$ . after a time  $t$ , when the adversary has access to some additional information  $Y$ , they perform the final measurement  $\Pi$  on  $Q_{out}$  using both  $Y$  and the classical outcome  $Z$ .

They immediately apply an encoding operation  $\mathcal{E} : \mathcal{L}(\mathcal{H}_Q) \rightarrow \mathcal{L}(\mathcal{H}_Z \otimes \mathcal{H}_{Q_{in}})$ . This operation prepares the quantum state for storage while extracting additional classical information  $Z$ . Subsequently, the adversary stores the quantum state using a quantum memory defined by the map  $\Phi_t : \mathcal{L}(\mathcal{H}_{Q_{in}}) \rightarrow \mathcal{L}(\mathcal{H}_{Q_{out}})$ . As a consequence of this setting, the adversary after a time  $t$  holds the classical-quantum system  $E = YZQ_{out}$ . At this point, they can perform a POVM  $\Pi : \mathcal{A} \rightarrow \mathcal{P}(\mathcal{H}_Y \otimes \mathcal{H}_Z \otimes \mathcal{H}_{Q_{out}})$  on the output of the quantum memory to guess the variable  $A$ , making use of the unlocked information  $Y$  and the additional classical variable  $Z$ . We refer to this general strategy as an *encoding attack*. One should note that any strategy that performs a measurement at times different from  $t_0$  and  $t_0 + t$ , even if surely suboptimal, can be described by an encoding attack.

In this scenario, therefore, what one is interested in is to bound the relative min-entropy  $H_{\min}(A|YZ\Phi_t(Q_{in}))$ , which quantifies the uncertainty of an adversary about  $A$ , while holding some quantum information  $\Phi_t(Q_{in})$  and classical registers  $Y$  and  $Z$ . We will then discuss a natural extension, useful in cryptography, where the adversary’s goal is to acquire information on  $n$  repetition of the same variables  $A$  and  $Y$ , evaluating therefore  $H_{\min}(A^n|Y^n Z\Phi_t(Q_{in}))$ .

In the following, we will analyze three possible approaches to tackle this problem, based on three assumptions on the available quantum memories:

- bounding the size of the quantum memory,
- bounding its classical capacity,
- bounding its quantum capacity.

## Bounded size of the quantum memory

Historically, the NSM had first been introduced in a less general variant, called the Bounded-Quantum-Storage Model (BQSM) [75], where the quantum memories available at the time of the protocol execution are assumed to be able to store only a finite number  $q$  of qubits perfectly. In this setting, one can now reduce the analysis to a restricted strategy where the adversary never uses a quantum memory, but they immediately perform a measurement. We call such a strategy an *immediate measurement strategy*. In this restricted scenario, the adversary performs an immediate measurement  $\mathcal{Z} : \mathcal{L}(\mathcal{H}_Q) \rightarrow \mathcal{L}(\mathcal{H}_Z)$  and obtains a classical outcome  $Z$ . After a time  $t$ , they unlock the additional information  $Y$  and extract the final guess by performing a classical decoding  $\Pi_1$ , that can again be expressed as a POVM  $\Pi_1 : \mathcal{A} \rightarrow \mathcal{P}(\mathcal{H}_Y \otimes \mathcal{H}_Z)$ .

The way to reduce to this restricted strategy simply consists of using a known chain rule for the min-entropy [17], obtaining

$$\begin{aligned} H_{\min}(A|YZ\Phi_t(Q_{in})) &\geq H_{\min}(A|YZ) - q \\ &\geq \min_{\mathcal{Z}} H_{\min}(A|Y\mathcal{Z}(Q)) - q. \end{aligned} \quad (6.5)$$

This general result also extends to the case with  $n$  repetitions of the same variable  $A$  and  $Y$ , since it only depends on the size of the quantum memory, obtaining

$$H_{\min}(A^n|Y^n Z\Phi_t(Q_{in})) \geq \min_{\mathcal{Z}} H_{\min}(A^n|Y^n \mathcal{Z}(Q)) - q. \quad (6.6)$$

However, in order to analyze the immediate measurement strategy, we need to specify further what information the adversary has access to and what they want to retrieve. Let's consider a standard *BB84* encoding, where the adversary wants to retrieve a single bit  $a \in \{0, 1\}$  and receives a quantum encoding of this bit either in the computational (as  $|a\rangle$ ) or in the Hadamard basis (as  $H|a\rangle$ ). Moreover, the classical information  $Y$  that she unlocks after a time  $t$  is the basis information. In this setting, it can be shown using some state discrimination strategy with post-measurement information [197] that

$$\min_{\mathcal{Z}} H_{\min}(A|Y\mathcal{Z}(Q)) = -\log\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right) \simeq 0.22. \quad (6.7)$$

Moreover, using the semidefinite programming formalism in [197], it has also been shown the extension for  $n$  repetitions [198]

$$\min_{\mathcal{Z}} H_{\min}(A^n|Y^n \mathcal{Z}(Q)) = -n \log\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right) \simeq 0.22n, \quad (6.8)$$

where now  $\mathcal{H}_Q = (\mathbb{C}^2)^{\otimes n}$ . From Eq. (6.6), this means that a non-trivial bound on the adversary information can only be found when  $q \lesssim 0.22n$ . However, this security analysis has been refined further in [199], where they proved that, at the expense of a small error  $\epsilon$ , a much stronger smooth min-entropy uncertainty relation can indeed be obtained:

$$\begin{aligned} \min_{\mathcal{Z}} H_{\min}^{\epsilon}(A^n|Y^n \mathcal{Z}(Q)) &\geq n \left(\frac{1}{2} - 2\delta\right) \\ \text{where } \delta &\in \left(0, \frac{1}{2}\right) \text{ and } \epsilon = \exp\left(\frac{\delta^2 n}{32(2 + \log \frac{1}{\delta})^2}\right). \end{aligned} \quad (6.9)$$

## Bounded classical capacity of the quantum memory

Although simply bounding the size of the quantum memory is enough to prove security for different cryptographic protocols, it is an assumption that might oversimplify the storage capacities of a quantum memory. Furthermore, when we consider continuous variable systems, it becomes evident that there isn't a distinct dimension limit to which the bounded-storage analysis can be readily applied. Therefore, to align more closely with the capabilities of present-day quantum technology, one can then consider alternative assumptions, such as limiting the success probability of correctly transmitting a randomly chosen  $nR$ -bit string  $x \in \{0, 1\}^{nR}$  through the quantum memory  $\Phi_t$ , defined as

$$P_{\text{succ}}^{\Phi_t}(nR) := \max_{\Pi, \{\rho_x\}_x} \frac{1}{2^{nR}} \sum_{x \in \{0,1\}^{nR}} \text{Tr} [\Pi(x)\Phi_t(\rho_x)] , \quad (6.10)$$

where the maximum is taken over families of code states  $\{\rho_x\}_{x \in \{0,1\}^{nR}}$  on  $\mathcal{H}_{Q_{in}}$  and decoding POVMs  $\Pi : \{0, 1\}^{nR} \rightarrow \mathcal{P}(\mathcal{H}_{Q_{out}})$ .

In particular, in [76], they proved that, by bounding  $P_{\text{succ}}^{\Phi_t}$ , one can reduce the analysis of the general attack in Figure 6.2 to the one of the immediate measurement strategy:

$$\begin{aligned} H_{\min}^{\epsilon+\epsilon'}(A|YZ\Phi_t(Q_{in})) &\geq -\log P_{\text{succ}}^{\Phi_t} \left( \lfloor H_{\min}^{\epsilon}(A|YZ) - \log \frac{1}{\epsilon'} \rfloor \right) \\ &\geq -\log P_{\text{succ}}^{\Phi_t} \left( \lfloor \min_{\mathcal{Z}} H_{\min}^{\epsilon}(A|Y\mathcal{Z}(Q)) - \log \frac{1}{\epsilon'} \rfloor \right) . \end{aligned} \quad (6.11)$$

Notably, the first inequality in (6.11) is valid for an arbitrary  $cccq$ -state  $\rho_{AYZQ_{out}}$ , while the second inequality is based on the fact that  $Z$  comes from the general attack strategy in Figure 6.2 and the fact that  $P_{\text{succ}}^{\Phi_t}$  is a monotonically decreasing function. Moreover, the bound in (6.11) is again a general statement that can be applied also to the  $n$  repetitions case, obtaining

$$H_{\min}^{\epsilon+\epsilon'}(A^n|Y^n Z\Phi_t(Q_{in})) \geq -\log P_{\text{succ}}^{\Phi_t} \left( \lfloor \min_{\mathcal{Z}} H_{\min}^{\epsilon}(A^n|Y^n \mathcal{Z}(Q)) - \log \frac{1}{\epsilon'} \rfloor \right) . \quad (6.12)$$

Finally, considering the standard  $BB84$  encoding, one can combine the security reduction in (6.11) with the post-measurement information bound in (6.9) to bound the adversary information on the string of bits  $A^n$  under a general strategy.

In [76], a specific scenario was examined where an adversary employs the same single-qubit quantum memory, denoted as  $\mathcal{N}_t$ , a total of  $\nu n$  times. The collective quantum memory can therefore be represented as  $\Phi_t = \mathcal{N}_t^{\otimes \nu n}$ . By focusing on certain channels that satisfy a strong-converse property [200], the authors established the security of protocols like oblivious transfer and bit-commitment under the condition  $C_{\mathcal{N}_t} \cdot \nu > \frac{1}{2}$ , where  $C_{\mathcal{N}_t}$  is the classical capacity of the single-qubit memory.

## Bounded quantum capacity of the quantum memory

Knowing how well a quantum memory can preserve classical information is not the only way of describing its performance. Moreover, this characterization gives us no information about

its ability to retain purely quantum information. A natural extension of this model is to therefore consider a bound on the (one-shot) quantum capacity of the available quantum memory.

Here, however, we cannot simply use the chain rule used in (6.5) or the bound in (6.11) to reduce the analysis to an immediate measurement strategy. It turns out that the approach this time is quite different: by considering from the beginning a *BB84* encoding is it possible to bound the  $n$  repetitions case with the following uncertainty relation [77]

$$H_{\min}^{\epsilon}(A^n | Y^n Z \Phi_t(Q_{in})) \geq n \cdot \gamma_{BB84} \left( \frac{H_{\min}(Q | Z \Phi_t(Q_{in}))}{n} \right) - 1 - \log \frac{2}{\epsilon^2}, \quad (6.13)$$

where the function  $\gamma_{BB84}(\cdot)$  is

$$\gamma_{BB84}(x) = \begin{cases} x & \text{if } x \geq \frac{1}{2} \\ g^{-1}(x) & \text{if } 0 < x < \frac{1}{2}, \end{cases} \quad (6.14)$$

with  $g(x) = H_2(x) + x - 1$ . The system  $Q$ , as represented in Figure 6.2, is the adversary's initial quantum information, which in this particular case are the  $n$  *BB84*-encoded qubits. Moreover,  $H_{\min}(Q | Z \Phi_t(Q_{in}))$  is a measure of how well an adversary, equipped with a noisy quantum memory, can preserve the entanglement, over a duration  $t$ , of the  $n$  Einstein-Podolsky-Rosen (EPR) pairs that Alice sends when considering a purified version of the protocol. This operational meaning can then be directly connected to the one-shot quantum capacity of the quantum memory, effectively bounding the right term in (6.13). See [77] for additional details. Finally it is important to notice that this last approach is fundamentally different from the previous ones: there is never a reduction to the immediate measurement strategy, but rather a reduction to a purified version where the adversary does not have access to the basis information  $Y$ .

## 6.4 Quantum computational time-lock security model

A novel security model called Quantum Computational Time-lock was introduced in [78], building a bridge between the often disparate worlds of classical and quantum cryptography. By analyzing this security model, we will explore how to combine realistic physical assumptions introduced earlier in this chapter with the assumption of short-term computational security of a classical symmetric encryption scheme. Although this perspective places the QCT model outside the realm of unconditional security, it's important to note that this stance is more cautious than assuming computational long-term security. The latter assumption is often implicitly made in many practical QKD implementations, where QKD is combined with computationally secure block ciphers such as Advanced Encryption Standard (AES). This approach results in a security level dependent on AES, raising questions about the added value of QKD in such scenarios [201].

### 6.4.1 Computational and physical assumptions

In the QCT construction, authorized parties, Alice and Bob, are assumed to be connected via a noiseless and authenticated classical channel and an insecure quantum channel. An

adversary, Eve, is assumed to have full access to the input of Alice and Bob’s communication channels. Every classical (quantum) message communicated between Alice and Bob over the classical (quantum) channel can be wiretapped by Eve and stored in classical (quantum) memory. With this pessimistic setting for Eve’s channel, we are in a similar set-up as strong QDL wherein an adversary Eve receives direct inputs from Alice.

The model is based on two nested assumptions. The first one is that Alice and Bob can use a  $t_{comp}$ -secure encryption scheme.

**Definition 6.4.1** ( $t_{comp}$ -secure encryption scheme). *An encryption scheme  $(Gen; Enc; Dec)$  is said to be  $t_{comp}$ -secure if it is semantically secure against adaptive chosen-ciphertext attacks with respect to any unauthorized attacker Eve for a time at least  $t_{comp}$ , after a ciphertext is exchanged on the classical channel.*

This implies that an encrypted message  $Enc_k(m)$  is (computationally) indistinguishable from a completely random string until at least a time  $t_{comp}$ . Furthermore, the security against adaptive chosen-ciphertext attacks ensures another required property: *non-malleability* [102]. In simple terms, an encryption scheme is called non-malleable if one cannot feasibly manipulate a given ciphertext in such a way that it produces another ciphertext, which, when decrypted, yields a plaintext related to the original.

The second assumption is that an adversary Eve cannot reliably store a quantum state during a time larger than  $t_{comp}$  i.e. that she has access to what we call a  $(t_{comp}, \delta)$ -noisy quantum memory, defined as follows.

**Definition 6.4.2** ( $(t_{comp}, \delta)$ -noisy quantum memory). *A  $(t_{comp}, \delta)$ -noisy quantum memory is a Markovian time-dependent quantum memory  $\Phi_t$  such that at time  $t_{comp}$*

$$\|\Phi_{t_{comp}} - \mathcal{F}\|_{\diamond} \leq \delta, \tag{6.15}$$

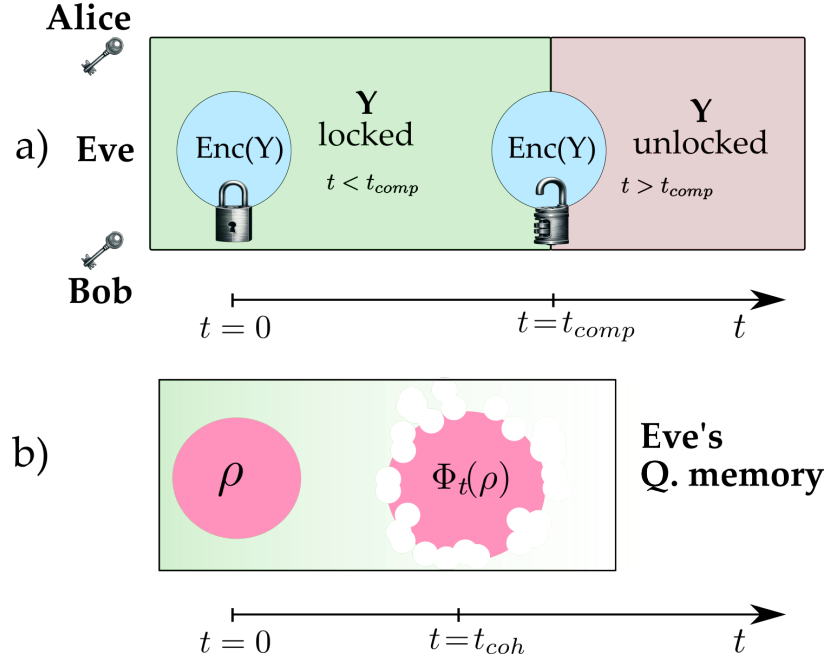
where  $\mathcal{F}(\rho) := \frac{\text{Tr}[\rho]}{d_{out}} \mathbb{1}_{d_{out}}$  is a completely mixing channel,  $\|\cdot\|_{\diamond}$  is the diamond norm [79], and  $d_{out}$  is the dimension of the output of the quantum memory.

In other words, a  $(t_{comp}, \delta)$ -noisy quantum memory is a quantum memory that is hard to distinguish (parametrized by a parameter  $\delta$ ) from a completely mixing channel  $\mathcal{F}$ , when it stores a quantum state for a time  $t_{comp}$  or longer. One can note that assuming that the coherence time of available quantum memories is much shorter than  $t_{comp}$  corresponds to taking  $\delta \ll 1$ .

Notably, while short-term computational security [202] and noisy-storage have been individually explored in the field of quantum cryptography, this model marked the first instance of proposing a combination of these two concepts.

## 6.4.2 Validity of QCT model

The validity of the QCT model is solidly grounded in practice when one considers existing and prospective quantum storage capabilities [158] and puts them in perspective with an extremely conservative lower bound on the time  $t_{comp}$  for which current encryption schemes would be considered secure, such as  $t_{comp} \geq 10^5 s \approx 1$  day. Moreover, it is interesting to



**Figure 6.3:** Overview of the assumptions in the QCT Model. Assumption a) Secure short-term encryption over period  $t_{comp}$ , allowing the exchange of some classical secret  $Y$  between Alice and Bob. Assumption b) A noisy quantum memory  $\Phi_t$  with a coherence time  $t_{coh} \ll t_{comp}$ .

understand that although the QCT assumptions set some limits to the scaling of quantum error-corrected quantum memory, it does not rule out the possibility of having useful quantum computers. Extrapolating for instance on [203] we see that 20 million noisy (with physical gate error  $10^{-3}$ ) qubits would be sufficient to factor a Rivest-Shamir-Adleman (RSA) 2048 key, using  $10^4$  logical qubits. However, considering the same resources and the same number of logical qubits, they could be stored for only a few hours. This would hence not rule out the conservative QCT assumptions mentioned above. We should also stress that the QCT approach enables us to build key establishment schemes that offer everlasting security. This means that the secret keys can be provably secure against an adversary who is computationally unbounded after quantum storage decoherence, where the decoherence time to be considered is the one technologically available at the time of protocol execution. In particular, security holds against any future progress of the attacker's computational and quantum storage capabilities.

### 6.4.3 Rationale of the QCT model

The QCT security model aims to enhance quantum cryptography's performance and functionalities. Its goals are twofold: surpassing classical cryptography's capabilities and offering advantages over standard QKD.

- **Security gain over classical cryptography:** The QCT model aims for everlasting security. While it cannot guarantee unconditional security due to the QCT assump-

tions, it ensures that keys remain secure against an infinitely powerful adversary as long as the initial encrypted communication is not compromised within the quantum storage's decoherence time. This level of security is unattainable with classical methods alone.

- **Enhanced performance compared to QKD:** The QCT model seeks to outperform QKD and the fundamental limits of repeaterless quantum secret capacities. As we will see in the key establishment scheme presented in Chapter 7, it proposes using multiple copies of the same quantum state sent from Alice to Bob, increasing the rate and loss tolerance compared to discrete-variable QKD.

#### 6.4.4 Quantifying adversarial information

Let's consider a case where Alice wants to transmit some classical information  $A$  to Bob. First, she sends to Bob some short-term secret  $Y$ , encrypted using a  $t_{comp}$ -secure encryption scheme, and then some quantum information  $Q$ . Imagine, for example,  $Q$  being many copies of the same quantum state and  $Y$  being some information on how to perform the optimal measurement. Following the Strong QDL framework, the adversary has a full copy of both the classical and quantum information.

One can notice that we are in a scenario similar to the one analyzed for the NSM, where access to the additional information  $Y$  is now delayed thanks to the short-term encryption scheme. Therefore, we consider the encoding attack described in Figure 6.2 for Eve to retrieve as much information as possible about  $A$ . She immediately applies an encoding operation  $\mathcal{E} : \mathcal{L}(\mathcal{H}_Q) \rightarrow \mathcal{L}(\mathcal{H}_Z \otimes \mathcal{H}_{Q_{in}})$ , which is now statistically independent of  $y$  due to the semantic security of the encryption scheme. Moreover, its non-malleability prevents Eve from running any homomorphic strategy, i.e. a quantum operation depending also on  $\text{Enc}_k(y)$ , which could eventually leak sensitive information. Moreover, we consider that after the time  $t_{comp}$ , Eve is given the encrypted secret  $y$ , i.e. that  $\text{Enc}$  can be fully decrypted after  $t_{comp}$ , which is the most favorable case for Eve. As in the NSM, what one is interested in is to bound  $H_{\min}(A|YZ\Phi_t(Q_{in}))$ , which results in analyzing the guessing probability

$$P_{\text{guess}}(A|YZ\Phi_{t_{comp}}(Q_{in})) := \max_{\Pi} \sum_a P_A(a) \text{Tr}[\Pi(a)\Phi_{t_{comp}}(\mathcal{E}(\rho_{YQ}))], \quad (6.16)$$

where we use the notation  $\mathcal{N}(\rho_{XQ}) := (\mathbb{1}_{d_X} \otimes \mathcal{N})(\rho_{XQ})$  for any quantum channel  $\mathcal{N}$  acting only on  $Q$ . We will use this notation throughout the rest of this manuscript.

#### Reduction to immediate measurement

We can now bound  $P_{\text{guess}}(A|YZ\Phi_{t_{comp}}(Q_{in}))$  with respect to an immediate measurement strategy, which, like for the NSM, consists first in an immediate measurement  $\mathcal{Z} : \mathcal{L}(\mathcal{H}_Q) \rightarrow \mathcal{L}(\mathcal{H}_Z)$ . At time  $t_{comp}$ , Eve unlocks  $Y$  and extracts the final guess by performing a classical decoding  $\Pi_1$ , that can be expressed as a POVM  $\Pi_1 : \mathcal{A} \rightarrow \mathcal{P}(\mathcal{H}_Y \otimes \mathcal{H}_Z)$ . The guessing probability can therefore be written as

$$P_{\text{guess}}(A|YZ(Q)) := \max_{\Pi_1} \sum_a P_A(a) \text{Tr}[\Pi_1(a)\mathcal{Z}(\rho_{YQ})]. \quad (6.17)$$



To show the security reduction we first prove the following useful (and more general) theorem.

**Theorem 6.4.1.** *If  $\|\Phi - \mathcal{F}\|_\diamond \leq \delta$ , with  $\mathcal{F}$  being the completely mixing channel, then for any cq-state  $\rho_{AXQ}$  we have*

$$P_{\text{guess}}(A|X\Phi(Q)) \leq P_{\text{guess}}(A|X) + \delta. \quad (6.18)$$

*Proof.* We can bound the guessing probability as follows

$$\begin{aligned} P_{\text{guess}}(A|X\Phi(Q)) &= \max_{\Pi} \sum_a p(a) \text{Tr}[\Pi(a)\Phi(\rho_{XQ})] \\ &= \max_{\Pi} \sum_a p(a) \left( \text{Tr}[\Pi(a)(\Phi - \mathcal{F})(\rho_{XQ})] + \text{Tr}[\Pi(a)\mathcal{F}(\rho_{XQ})] \right) \\ &\leq \max_{\Pi} \sum_a p(a) \left( \|\Pi(a)\|_\infty \|(\Phi - \mathcal{F})(\rho_{XQ})\|_1 + \text{Tr}[\Pi(a)\mathcal{F}(\rho_{XQ})] \right) \\ &\leq \delta + \max_{\Pi} \sum_a p(a) \text{Tr}[\Pi(a)\mathcal{F}(\rho_{XQ})]. \end{aligned}$$

In the third line, we used Hölder's inequality and the fact that  $\sum_a p(a) = 1$ , while the last inequality is obtained by noticing that  $\|M\|_\infty \leq 1$  for any element of a POVM and the fact that  $\|(\Phi - \mathcal{F})(\rho_{AX})\|_1 < \delta$ , since we have  $\|\Phi - \mathcal{F}\|_\diamond \leq \delta$ . Finally, from Lemma 2.3.1 we directly have  $\max_{\Pi} \sum_a p(a) \text{Tr}[\Pi(a)\mathcal{F}(\rho_{XQ})] = P_{\text{guess}}(A|X)$  which concludes the proof.  $\square$

Now, from Theorem 6.4.1, we simply have that for any encoding operation

$$\begin{aligned} P_{\text{guess}}(A|YZ\Phi_{t_{\text{comp}}}(Q_{\text{in}})) &\leq P_{\text{guess}}(A|YZ) + \delta \\ &\leq \max_{\mathcal{Z}} P_{\text{guess}}(A|Y\mathcal{Z}(Q)) + \delta, \end{aligned} \quad (6.19)$$

where we maximized over all possible Eve's immediate measurements  $\mathcal{Z}$ . Hence, considering  $\delta \ll 1$ , we have successfully reduced any general attack strategy to an immediate measurement strategy, without the need to further specify the form of the cccq state  $\rho_{AYZ\Phi_{t_{\text{comp}}}(Q_{\text{in}})}$ . Therefore, as in the NSM, this general result also extends to the case with  $n$  repetitions of the same variables  $A$  and  $Y$ , obtaining

$$P_{\text{guess}}(A^n|Y^n Z\Phi_{t_{\text{comp}}}(Q_{\text{in}})) \leq \max_{\mathcal{Z}} P_{\text{guess}}(A^n|Y^n \mathcal{Z}(Q)) + \delta. \quad (6.20)$$

In the next chapter, we shall see how to bound the guessing probability for the immediate measurement by exploiting known results from the communication complexity framework.

## 6.5 Conclusion

In this chapter, we explored three major quantum cryptographic models: Quantum Data Locking, the Noisy-Storage Model, and Quantum Computational Timelock. We summarize the main features of each security model in Table 6.1.

| Model    | Security Assumptions  | Type of Security Proof  |
|----------|---|---|
| QDL [74] | Time-limited quantum memory ( $\delta = 0$ for a finite time $\tau$ )   | Bound the accessible information $I_{acc}(A : Q)$   |
| NSM      | Quantum memory: <ul style="list-style-type: none"> <li>• bounded size [75]</li> <li>• bounded classical capacity [76]</li> <li>• bounded quantum capacity [77]</li> </ul> | Bound $H_{\min}^{\epsilon}(A YZ\Phi_t(Q_{in}))$ and $H_{\min}^{\epsilon}(A^n Y^nZ\Phi_t(Q_{in}))$ |
| QCT [78] | <ol style="list-style-type: none"> <li>1. <math>t_{comp}</math>-secure encryption scheme</li> <li>2. <math>(t_{comp}, \delta)</math>-noisy quantum memory</li> </ol>      | Bound $H_{\min}(A YZ\Phi_t(Q_{in}))$ and $H_{\min}(A^n Y^nZ\Phi_t(Q_{in}))$                       |

**Table 6.1:** Comparison of cryptographic models: QDL, NSM, and QCT.

In our development of the QCT model, we incorporated techniques from both the QDL and NSM models. Like strong QDL, our model assumes that the adversary has access to a complete copy of the quantum communication. This assumption intriguingly shifts a traditional key distribution problem, typically involving an external hacker, into a scenario where the adversary, Eve, directly receives information from Alice. This shift effectively transforms the model into a two-party cryptographic framework. Therefore, it is not surprising that the general attack in QCT directly mimics the NSM general attack illustrated in Figure 6.2. This mix of features from different frameworks will be even more evident in the next chapter, where we shall explore a detailed key distribution scheme under the QCT model.

More generally, our objective in this discussion was to highlight the critical importance of merging provable security principles with practical assumptions about an adversary’s capabilities, a concept that is fundamentally vital in the realm of modern quantum cryptography. This approach not only aligns theoretical robustness with real-world applicability but also opens up new paths for exploring and understanding security dynamics.



# HM-QCT PROTOCOL

## Contents

|            |   |            |
|------------|---|------------|
| <b>7.1</b> | <b>Introduction</b>                             | <b>98</b>  |
| <b>7.2</b> | <b>HM-QCT key distribution scheme</b>           | <b>99</b>  |
| 7.2.1      | Protocol description                            | 99         |
| 7.2.2      | Achievable key rate in the i.i.d. setting       | 100        |
| 7.2.3      | Exploiting the complexity gap                   | 101        |
| 7.2.4      | Everlasting secure key expansion                | 103        |
| <b>7.3</b> | <b>Performance analysis and functionalities</b> | <b>103</b> |
| 7.3.1      | Key rate analysis                               | 103        |
| 7.3.2      | Multicast key distribution                      | 105        |
| 7.3.3      | Security with untrusted detectors               | 106        |

In this chapter, we explore a new approach to quantum cryptography by considering the QCT security model presented in Chapter 6. In particular, we unlock the possibility of sending multiple copies of the same state to perform key establishment with everlasting security with performances that go beyond standard QKD.

## 7.1 Introduction

In quantum cryptography, encoding classical information redundantly on multiple copies of the same quantum state could be highly beneficial from an engineering viewpoint, allowing for higher rates and better resilience to loss. However, this is a problem for the security of many quantum cryptography protocols as it would allow the adversary to gain more information about the underlying state than if just a single copy is sent. This limitation translates into a mean photon number that is typically upper bounded by 1 in QKD protocols, and more generally, into the existence of a fundamental rate-loss trade-off that severely limits the distances over which we can perform QKD [81].

In this chapter, we introduce an explicit construction for a new key distribution protocol called Hidden Matching Quantum Computational Time-lock (HM-QCT). It is built on top of the one-way communication complexity  $\beta$ PM problem [3], for which  $\Omega(\sqrt{n})$  bits of communication from Alice to Bob are required, against only  $\mathcal{O}(\log(n))$  qubits, with  $n$  the length of input  $x$ . See Chapter 5 for more details.

In each round of the HM-QCT protocol Alice generates both inputs  $x$  and  $y$  and shares the latter with Bob using a short-term computationally secure encryption scheme. Alice and Bob can then solve the  $\beta$ PM protocol with a quantum strategy to extract a bit, sending  $m$  copies of the same  $n$ -dimensional quantum state. See Figure 7.1 for a pictorial representation.

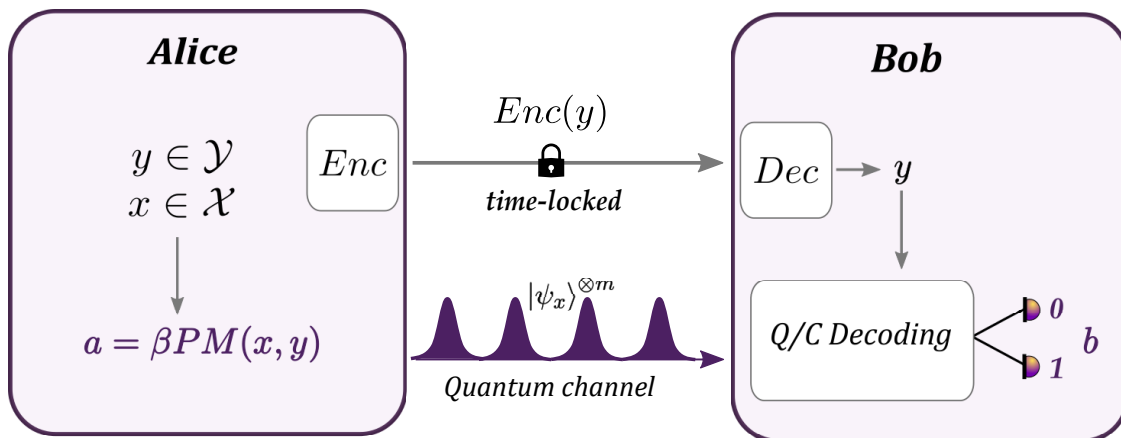


Figure 7.1: One round of the HM-QCT protocol.

Finally, by performing standard classical post-processing to their string of bits, they can distill a secret key, whose security is based on the reduction to classical strategies for this communication complexity problem, effectively connecting the field of communication complexity and quantum cryptography.

## 7.2 HM-QCT key distribution scheme

### 7.2.1 Protocol description

Now that we've outlined the construction approach for our protocol and the rationale behind its security proof, we're set to present a more detailed and formal version of our hybrid key distribution protocol. The notation used is the one introduced in Section 5.3.1.

#### HM-QCT Protocol

##### Parameters:

- dimension  $n$  of the communication complexity problem,
- number of copies  $m$ ,
- number of rounds  $l$ .

##### 1. Data Generation:

- Alice generates and stores  $\mathbf{x} = (x_1, \dots, x_l)$  and  $\mathbf{y} = (y_1, \dots, y_l)$  from the probability distribution  $\mu_{\beta PM}^l \in \Delta^l(\mathcal{X} \times \mathcal{Y})$  presented in Section 5.3.1. She then computes and stores the string  $\mathbf{a} = (a_1, \dots, a_l)$ , where  $a_j = \beta PM(x_j, y_j)$ .

##### 2. QCT exchange

- Alice and Bob run **Gen** and obtain a shared secret  $k$ .
- Alice sends  $\text{Enc}_k(\mathbf{y})$  to Bob.
- Bob decrypts  $\text{Enc}_k(\mathbf{y})$  using  $\text{Dec}_k$ , obtaining  $\mathbf{y}$ .

##### 3. Quantum communication

- for  $i = 1; i \leq l$ 
  - Alice and Bob run the  $\beta PM$  quantum protocol, with input  $x_i$  and  $y_i$  sending  $m$  copies of the quantum state (5.17). Bob stores the output  $b_i$ .

##### 4. Sifting:

- Alice and Bob discard all rounds with  $b_i = \perp$ .

##### 5. Classical post processing:

- Parameter estimation: Alice and Bob estimate the QBER i.e. the error rate of a conclusive round, by revealing a part of their string.
- Alice and Bob perform *error correction*<sup>a</sup> [104] followed by *privacy amplification* [105] to distill a secret key.

---

<sup>a</sup>The correctness of our protocol is ensured by the correctness of the  $\beta PM$  protocol together with an extra step of error correction to deal with noise and loss present in practical scenarios.

## 7.2.2 Achievable key rate in the i.i.d. setting

We now describe how to derive an achievable key rate within our model. We shall analyze the security of our key distribution protocol in the i.i.d. setting, i.e. the restricted case where the adversary Eve performs the same strategy independently on every round<sup>1</sup>. In particular, Eve's general attack to each round of the protocol is the one depicted in Figure 6.2. In this scenario, the initial quantum system  $Q$  is composed of  $m$  instances of the quantum state as defined in Eq. (5.17). Considering the  $j$ -th round, her objective is to deduce the bit  $a_j = \beta PM(x_j, y_j)$ . For clarity, from now on we simplify our discussion by omitting the subscript that denotes the round number. She starts with an encoding operation  $\mathcal{E}$  and subsequently stores the quantum information until the time  $t_{comp}$  required to unlock the encrypted input  $y$ .

As a consequence of this setting, at the end of each round Alice and Bob have access to a realization of correlated classical random variables  $A$  and  $B$ , respectively, whereas the adversary holds the quantum-classical system  $E = YZQ_{out}$ . The final joint state for each round between Alice and Eve will have therefore the form

$$\rho_{AYZ\Phi_{t_{comp}}(Q_{in})} = \sum_{x,y,a} \mu_{\beta PM}(x,y) \delta_{\beta PM(x,y),a} |a\rangle\langle a| \otimes |y\rangle\langle y| \otimes |z\rangle\langle z| \otimes (\mathcal{I}_Z \otimes \Phi_{t_{comp}})(\mathcal{E}(\rho_x)) . \quad (7.1)$$

At this point Eve performs a POVM  $\Pi : \{0, 1\} \rightarrow \mathcal{P}(\mathcal{H}_y \otimes \mathcal{H}_Z \otimes \mathcal{H}_{Q_{out}})$  on the output of the quantum memory to guess the bit  $a$ , making use of  $y$  and the classical string  $z$ . The guessing probability  $P_{\text{guess}}(A|YZ\Phi_{t_{comp}}(Q_{in}))$  can be expressed as follows

$$P_{\text{guess}}(A|YZ\Phi_{t_{comp}}(Q_{in})) = \max_{\Pi} \sum_{x,y,a} \mu_{\beta PM}(x,y) \delta_{\beta PM(x,y),a} \quad (7.2)$$

$$\text{Tr}[\Pi(a)(|y\rangle\langle y| \otimes (\mathcal{I}_Z \otimes \Phi_{t_{comp}})(\mathcal{E}(\rho_x)))] . \quad (7.3)$$

Finally, since the min-entropy lower-bounds the von Neumann entropy, we can lower bound the Devetak-Winter bound [65] in Eq. (3.10) and obtain the following achievable key rate

$$R_{\infty}^{\text{QCT}} \geq \gamma_{\text{sift}} (H_{\min}(A|YZ\Phi_t(Q_{in})) - H_2(\text{QBER})) . \quad (7.4)$$

The sifting factor  $\gamma_{\text{sift}}$  can be expressed as  $1 - p_{\text{abort}}$ , where  $p_{\text{abort}}$  represents the probability that a single round in the quantum communication protocol yields an inconclusive result. In Appendix C.3 we have evaluated  $p_{\text{abort}}$  and QBER as a function of the number of copies sent  $m$  in a practical scenario.

To bound  $H_{\min}(A|YZ\Phi_t(Q_{in}))$ , we can now reduce the analysis to the immediate measurement strategy described in Section 6.4.4, where Eve immediately performs a measurement  $\mathcal{Z}$ . Specifically, drawing from Eq. (6.19), we can determine an upper bound for the key rate

$$R_{\infty}^{\text{QCT}} \geq \gamma_{\text{sift}} \left( -\log \left( \max_{\mathcal{Z}} P_{\text{guess}}(A|Y\mathcal{Z}(Q)) \right) - H_2(\text{QBER}) \right) . \quad (7.5)$$

---

<sup>1</sup>A possible direction to extend the security analysis to a coherent attack is discussed in Chapter 9.

### 7.2.3 Exploiting the complexity gap

To finally estimate an upper bound to Eve's guessing probability we still have to analyze the immediate measurement strategy. Our approach for a full proof follows the idea that extracting a bit of the key with an immediate measurement strategy is as hard as solving the classical  $\beta$ PM problem. In particular, Eve cannot do better than what one would get for the  $\beta$ PM problem by sending  $m \log(n)$  bits of information about the input  $x$ , where  $m \log(n)$  bits is the maximum classical information one can extract from  $m$  copies of a  $n$ -dimensional quantum state thanks to the Holevo bound.

**Lemma 7.2.1.**  $\forall \epsilon \in (0, \frac{1}{2})$  if an immediate measurement strategy with  $P_{\text{guess}}(A|Y\mathcal{Z}(Q)) \geq 1 - \epsilon$  exists, then Alice has sent  $m$  copies of the quantum state (5.17), with

$$m \geq \frac{IC_{\mu_{\beta PM}}^{1,ext}(\beta PM, \epsilon)}{\lceil \log(n) \rceil}.$$

*Proof.* Let's suppose there exists an immediate measurement strategy with  $P_{\text{guess}}(A|Y\mathcal{Z}(Q))$  at most  $1 - \epsilon$ , then we can transform this strategy into a classical protocol to solve the  $\beta$ PM problem. The transformation is straightforward, Alice generates  $m$  copies of the quantum state (5.17), then she immediately performs the measurement  $\mathcal{Z}$  and sends the classical output  $z$  to Bob who, after performing the final POVM  $\Pi_1$  on  $z$  and  $y$ , will output the correct answer with probability at least  $1 - \epsilon$ . Note that the string  $z$  is the transcript of the protocol. Since from Holevo's bound we know that  $I(X : Z) \leq m \lceil \log(n) \rceil$ , by definition 5.2.2 of  $IC_{\mu_{\beta PM}}^{1,ext}(\beta PM, \epsilon)$  we have

$$m \geq \frac{IC_{\mu_{\beta PM}}^{1,ext}(\beta PM, \epsilon)}{\lceil \log(n) \rceil}.$$

□

Finally, thanks to the complexity gap between classical and quantum strategies, Theorem 7.2.1 ensures that Eve's guessing probability is safely bounded far from 1 as long as Alice is sending  $\mathcal{O}\left(\frac{\sqrt{n}}{\log(n)}\right)$  copies of the quantum state.

**Theorem 7.2.1.** Let us suppose  $n \geq 4$ . For any encoding attack Eve's guessing probability is bounded by

$$P_{\text{guess}}(A|YZ\Phi_{t_{\text{comp}}}(Q_{\text{in}})) \leq \frac{1}{2} + 2 \left( \sqrt[3]{-q} + \sqrt{\frac{p}{3}} \right) + \delta, \quad (7.6)$$

with

$$q = \frac{-50}{\sqrt{n}} e^{\sqrt{\beta}((m+1)\lceil \log(n) \rceil + \ln(4) + 6)}$$

$$p = \frac{-50}{\sqrt{n}} e^{\sqrt{\beta} \left( \log\left(\frac{5}{2}\right) - \ln(4) \right)}.$$

*Proof.* We first prove a useful lemma.



**Lemma 7.2.2.**  $\forall \epsilon \in (0, \frac{1}{2}), \forall \delta_2 \in (0, \frac{1}{2} - \epsilon)$  if an encoding attack with  $P_{\text{guess}}(A|YZ\Phi_{t_{\text{comp}}}(Q_{\text{in}})) \geq 1 - \epsilon + \delta$  exists, then Alice must have sent  $m$  copies of the quantum state (5.17), with

$$m \geq \frac{\delta_2 \left( \frac{1}{50e\sqrt{\beta}} \left( \frac{1}{2} - \epsilon - \delta_2 \right)^2 \sqrt{n} + 2 \log \left( \frac{1}{2} - \epsilon - \delta_2 \right) \right) - \log\left(\frac{5}{2}\right)\delta_2 - 6}{\lceil \log(n) \rceil}.$$

*Proof.* Let  $\epsilon \in (0, \frac{1}{2}), \delta_2 \in (0, \frac{1}{2} - \epsilon)$ . Let us suppose there exists an encoding attack with  $P_{\text{guess}}(A|YZ\Phi_{t_{\text{comp}}}(Q_{\text{in}})) \geq 1 - \epsilon + \delta$ . First, by using Theorem 6.4.1, we deduce  $\max_{\mathcal{Z}} P_{\text{guess}}(A|YZ(Q)) \geq 1 - \epsilon$ . Then we use Lemma 7.2.1 to deduce  $m \geq \frac{IC_{\beta PM}^{1, \text{ext}}(\beta PM, \epsilon)}{\lceil \log(n) \rceil}$ . Furthermore, from Lemma 5.2.4 we obtain  $m \geq \frac{\frac{\delta_2}{2} D_{\beta PM}^1(f, \epsilon + \delta_2) - 6}{\lceil \log(n) \rceil}$ . Finally, we conclude the proof by showing that from Theorem 5.3.1 we have

$$m \geq \frac{\frac{\delta_2}{2} (k(\epsilon + \delta_2)\sqrt{n} + d(\epsilon + \delta_2)) - 6}{\lceil \log(n) \rceil},$$

with  $k$  and  $d$  defined in (5.19). □

Now we are ready to prove Theorem 7.2.1. Let  $x$  be equal to  $\frac{1}{2} - \epsilon$  and  $\delta_2 := \frac{x}{2}$ . By contraposition, Lemma 7.2.2 implies that for any encoding attack acting on  $m$  copies, with

$$m = \frac{\frac{1}{50e\sqrt{\beta}} \left( \frac{x}{2} \right)^3 \sqrt{n} - \ln(4) - 6 - \left( \log\left(\frac{5}{2}\right) - \ln(4) \right) \frac{x}{2}}{\lceil \log(n) \rceil} - 1, \quad (7.7)$$

Eve's guessing probability is bounded by  $P_{\text{guess}}(A|YZ\Phi_{t_{\text{comp}}}(Q_{\text{in}})) < \frac{1}{2} + x + \delta$ . We now have to find the real zero of Eq. (7.7) by using Cardan's method. We first rewrite (7.7) in the canonical form

$$z^3 + pz + q = 0, \quad (7.8)$$

where

$$z = \frac{x}{2}, \quad q = \frac{-50}{\sqrt{n}} e\sqrt{\beta} ((m+1)\lceil \log(n) \rceil + \ln(4) + 6),$$

$$p = \frac{-50}{\sqrt{n}} e\sqrt{\beta} \left( \log\left(\frac{5}{2}\right) - \ln(4) \right).$$

We now notice that  $q < 0$  and, since  $(\log(\frac{5}{2}) - \ln(4)) < 0$ , that  $p > 0$ . This means that  $\Delta := -(4p^3 + 27q^2)$  is negative. Therefore, thanks to Cardan's method, the zero of equation (7.8) expressed in the variable  $x$  is

$$x = 2^{1-\frac{1}{3}} \left( \sqrt[3]{-q + \sqrt{\frac{-\Delta}{27}}} + \sqrt[3]{-q - \sqrt{\frac{-\Delta}{27}}} \right). \quad (7.9)$$

From Eq. (7.9), noting the negative second term with  $\sqrt[3]{\cdot}$  and the fact that  $\sqrt[3]{\cdot}$  is subadditive for any integer  $d$ , we deduce that

$$P_{\text{guess}}(A|YZ\Phi_{t_{\text{comp}}}(Q_{\text{in}})) \leq \frac{1}{2} + 2 \left( \sqrt[3]{-q} + \sqrt{\frac{p}{3}} \right) + \delta.$$

□

Finally, from Theorem 7.2.1 we can rewrite the achievable key rate in (7.4) as

$$R_{\infty}^{\text{QCT}} \geq \gamma_{\text{sift}} \left( -\log \left( \frac{1}{2} + 2 \left( \sqrt[3]{-q} + \sqrt{\frac{p}{3}} \right) + \delta \right) - H_2(\text{QBER}) \right). \quad (7.10)$$

## 7.2.4 Everlasting secure key expansion

The security analysis shows that, within the QCT model, we can simplify the scenario to one where Eve’s interaction (measurement) on the quantum state occurs right at the beginning, at  $t = t_0$ . The security analysis after  $t_{\text{comp}}$ , then purely relies on information-theory principles. Hence the resulting key rates are valid against an adversary with unbounded computational power after  $t_{\text{comp}}$ , i.e. our schemes have everlasting security [2]. We note that everlasting secure key establishment cannot be attained with cryptographic protocols relying solely on classical communication, even with computational assumptions. Classical communication can be copied, making harvesting attacks (store now, attack later) a significant vulnerability.

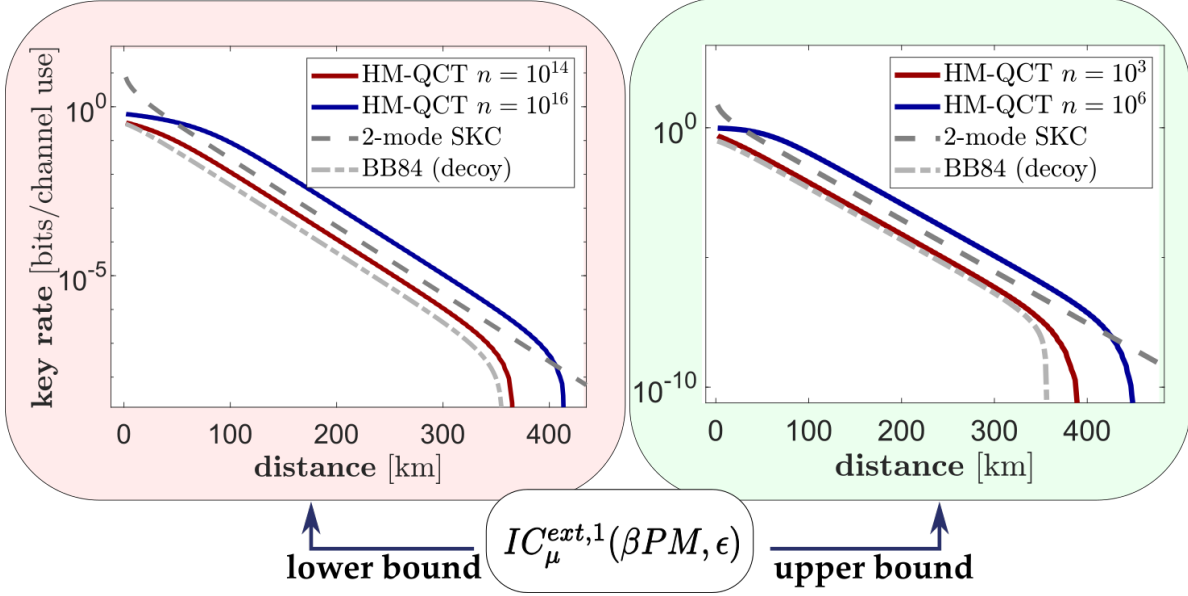
Furthermore, to ensure the effectiveness of our hybrid key distribution scheme, the rate of secure key generation must exceed the rate of key consumption due to the need for a pre-shared key. One way to achieve this is by employing a block cipher in the QCT exchange described in Section 7.2.1, where Alice divides the message  $\mathbf{y}$  into fixed-size blocks. As a block cipher can encrypt an exponential number of blocks in the key size, the rate of pre-shared key consumption grows logarithmically with the number of protocol rounds, while the final key size increases linearly, ensuring secure key expansion.

## 7.3 Performance analysis and functionalities

### 7.3.1 Key rate analysis

While most articles on communication complexity focus on asymptotic scalings of input dimensions, our work necessitates precise knowledge of the lower bounds of communication complexity in the non-asymptotic regime.

With these bounds, we can accurately determine how the guessing probability scales with the dimension and the number of copies sent by Alice. Theorem 7.2.1 is therefore a significant result, derived from a lower bound of the one-way information complexity of the  $\beta$ PM problem, but this bound may not be tight. In fact, the error  $\epsilon_{\text{BKP}}(d)$  from the best-known classical protocol with a communication cost  $d$ , analyzed in Appendix C.1.3, is larger than what one would get from the lower bound.



**Figure 7.2:** Key rate comparison for the HM-QCT protocol between the derivation from the upper bound and the lower bound of the one-way external information complexity of the  $\beta$ PM problem, both evaluated with  $\delta = 10^{-4}$  and  $\beta = \frac{1}{4}$ . We benchmark them with the BB84 protocol with decoy states [52] and the 2-mode Secret Key Capacity (SKC) [81]. The plots for the HM-QCT protocol are derived under a practical implementation, as detailed in Appendix C.3. For both the HM-QCT protocol and the BB84 protocol with decoy states, we used the same detector specifications. These detectors are state-of-the-art SNSPDs, as detailed in [141], characterized by a dark count probability of  $P_{\text{dark}} = 10^{-8}$  and a detection efficiency of  $\eta_{\text{det}} = 65\%$ .

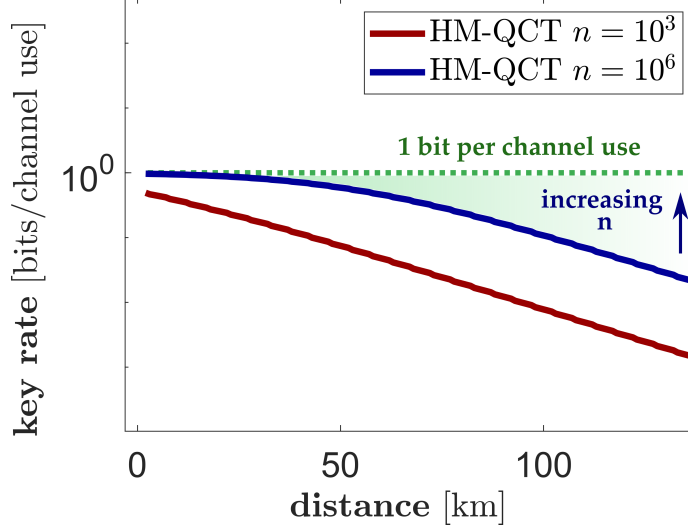
Nevertheless, one can consider an optimistic scenario where the actual one-way information complexity for any error  $\epsilon$  is equal to the information cost of the best-known protocol<sup>2</sup>. In this context, by combining Theorem 6.4.1 and Lemma 7.2.1 we have

$$P_{\text{guess}}(A|YZ\Phi_{t_{\text{comp}}}(Q_{\text{in}})) \leq 1 - \epsilon_{\text{BKP}}(m \lceil \log(n) \rceil) + \delta. \quad (7.11)$$

Consequently, in Figure 7.2 we plot a comparison between the achievable key rate from (7.10) and the key rate obtained from the best-known classical protocol, where in both cases we performed a optimization on the number of copies  $m$ .

Since our protocol is implemented using two detection modes, effectively sending at most one bit per channel use, we benchmark it with two standard key rate limits: the BB84 protocol with decoy states [52] and the more general limit for 2-mode optical key distribution [81], generally called the 2-mode SKC. It's evident from the plot that while the lower bound demands an exceedingly high number of modes, around  $10^{16}$ , to surpass the SKC, the upper bound achieves this with 10 orders of magnitude fewer modes. Moreover, with only a thousand modes, the key rate derived from the upper bound can already surpass the theoretical limit for BB84. Notably, an experimental implementation of a variant of the quantum  $\beta$ PM protocol has already been performed with a similar number of modes [162].

<sup>2</sup>In other words, assuming that future developments on finding tighter lower bounds will show that the



**Figure 7.3:** Key rate over short distances for the HM-QCT protocol derived from the best-known classical protocol.

When focusing on relatively short distances, as illustrated in Figure 7.3, the key rate derived from the upper bound provides a significant insight. By increasing the number of modes  $n$ , it becomes possible to achieve a stabilized key rate nearing one bit per channel use, since there’s a high likelihood of at least one photon reaching the detectors consistently.

In general one can notice that at very long distances the protocol’s efficiency is primarily hindered by detector dark counts, which significantly limit the achievable key rate. At intermediate distance, the key rate’s trend resembles the 2-mode SKC, decaying exponentially with distance due to Bob receiving, on average, less than one photon per channel use.

### 7.3.2 Multicast key distribution

Allowing to send  $m$  multiple copies of the same quantum state not only increases the overall performance of two-party key distribution but also unlocks the possibility of performing multicast key distribution, where one can distill the same key among  $N$  authorized Bobs. The multicast HM-QCT key distribution protocol is simply a generalization of the bipartite version where Alice first shares the secret  $\mathbf{y}$  with all the  $N$  authorized Bobs using a short-term secure encryption scheme. She then can subdivide on each round the total number of copies  $m$  of the quantum states among the  $N$  different Bobs based on their distance, ensuring that more distant Bobs receive a higher number of copies to compensate for potential loss.

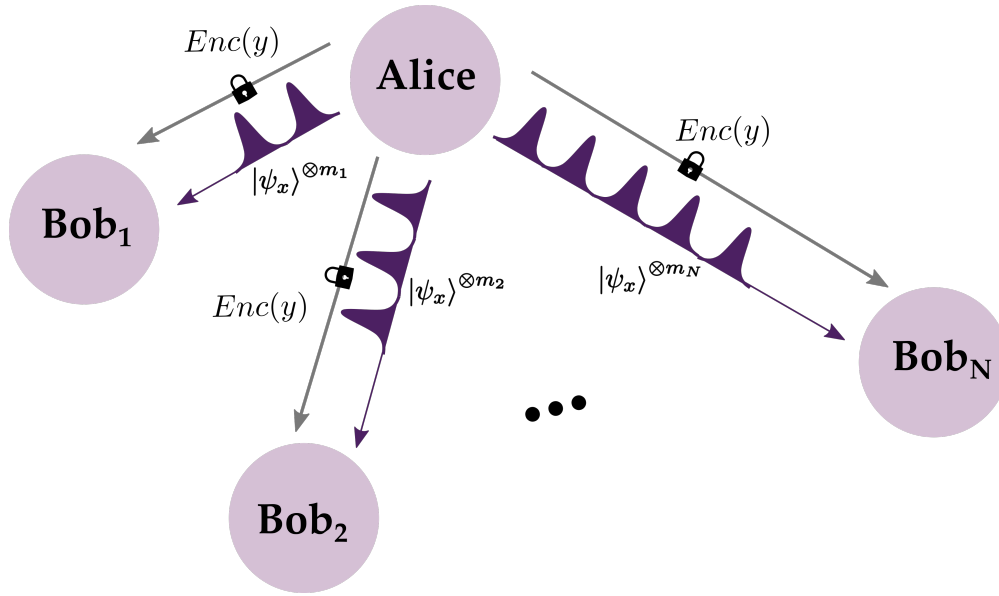
Proving security in this setting turns out to be along analogous lines as in the bipartite case [204, 205], where a generalized version of the Devetak-Winter bound represents the achievable key rate in the asymptotic limit

$$R_{\infty}^N \geq \gamma_{\text{sift}} \left( H_{\min}(A|E) - \max_i H_2(\text{QBER}_i) \right). \quad (7.12)$$

In this context,  $\text{QBER}_i$  denotes the quantum bit error rate corresponding to the  $i$ -th Bob,

---

current best-known classical protocol is the optimal protocol.

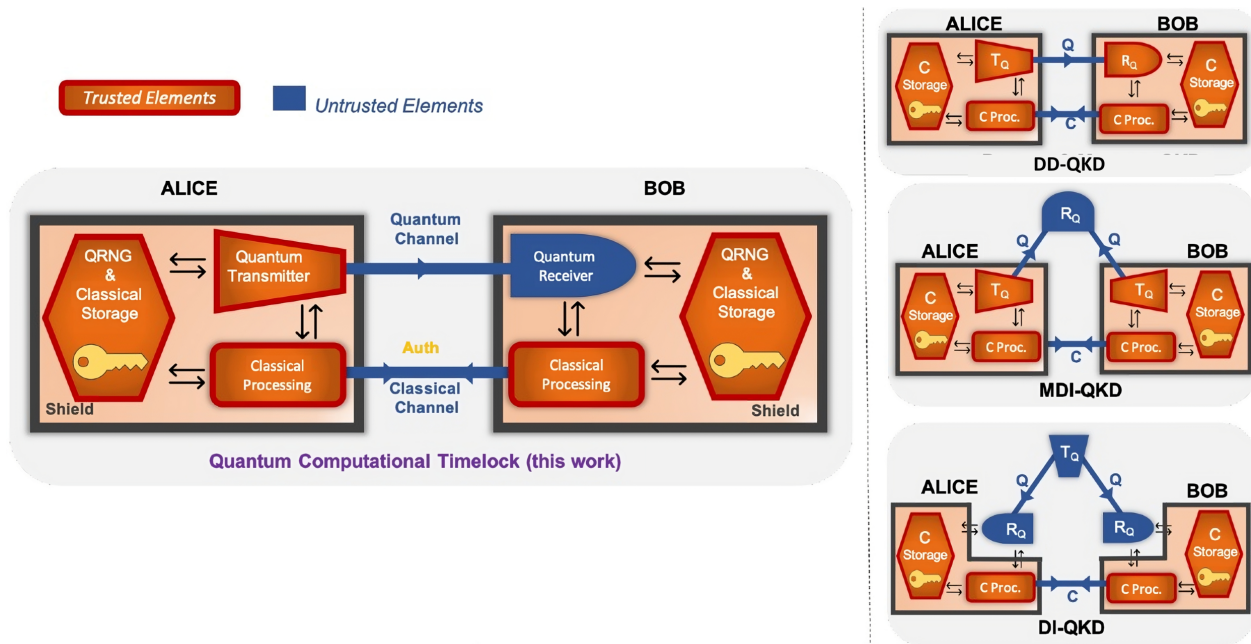


**Figure 7.4:** One round of the multicast HM-QCT protocol, where  $m = \sum_{i=1}^N m_i$  are sent among  $N$  different Bobs.

while the quantum system  $E$  describes the total classical and quantum information available to Eve in each protocol round. Importantly, given our assumption that Eve has access to all  $m$  transmitted quantum states in every round, the process of bounding the relative min-entropy  $H_{\min}(A|E)$  remains the same as described for the two-party model. Moreover, it is interesting to notice how the amount of information that could potentially leak to an eavesdropper during the error correction phase only depends on the Bob with the highest level of noise.

### 7.3.3 Security with untrusted detectors

In our security analysis, one can notice that the way we establish a bound on the min-entropy  $H_{\min}(A|YZ\Phi_{t_{comp}}(Q_{in}))$  only depends on the dimension of the input state prepared by Alice's quantum source. In fact, it is sufficient to know from Holevo bound that Alice is leaking at most  $m\lceil\log(n)\rceil$  bits of information about her input to then reducing Eve's attack strategy to a classical strategy for solving the  $\beta$ PM protocol. This simply means that we are not required to know the specifications of Bob's measurement device or the amount of noise between Alice and Bob. In particular, the QBER at Bob's side only influences the amount of leakage that happens during the error correction step, but it doesn't affect  $H_{\min}(A|YZ\Phi_{t_{comp}}(Q_{in}))$ . In Figure 7.5 we compare the trust assumptions of the QCT model with other standard trust models: DD-QKD, MDI-QKD, and DI-QKD.



**Figure 7.5:** Comparison of hardware trust requirements between the QCT model and the conventional trust models: DD-QKD, MDI-QKD, and DI-QKD (see Section 3.2.2 for more details). As in Figure 3.1, components in orange are those that need to be reliable and work as specified in the security proof. In contrast, the blue elements are those where no specific assumptions about their internal functioning and specifications are made. The shield, depicted with a black border, ensures no information leakage from these devices. The smaller figures use abbreviations such as  $T_Q$  for the quantum transmitter,  $R_Q$  for the quantum receiver, C for classical, and Q for quantum. Figure from [78].



# PLATFORM FOR ONE-WAY QUANTUM COMMUNICATION COMPLEXITY

## Contents

|            |  |            |
|------------|--|------------|
| <b>8.1</b> | <b>Introduction</b>  | <b>110</b> |
| <b>8.2</b> | <b>Light propagation through disordered media</b>                          | <b>110</b> |
| 8.2.1      | Scattering theory  | 110        |
| 8.2.2      | Multimode fibers as complex media  | 111        |
| 8.2.3      | Introduction to wavefront shaping  | 113        |
| 8.2.4      | Applications of wavefront shaping  | 116        |
| <b>8.3</b> | <b>Reconfigurable optical network for quantum communication complexity</b> | <b>119</b> |
| 8.3.1      | Experimental setup   | 120        |
| 8.3.2      | Acquisition of transmission matrix   | 121        |
| 8.3.3      | Construction of reconfigurable detection system                            | 123        |
| 8.3.4      | Scalability and flexibility of the optical network                         | 125        |
| 8.3.5      | Experimental analysis  | 127        |
| <b>8.4</b> | <b>Conclusion</b>  | <b>132</b> |

In the previous chapter, we introduced a scheme for key establishment, whose security and effectiveness hinge on the ability of two parties to address a one-way quantum communication complexity problem more efficiently than is possible classically. Building on this concept, this chapter investigates the feasibility of experimentally demonstrating a quantum advantage in communication complexity.



## 8.1 Introduction

In our highly connected world, where the demand for higher transmission capacity keeps growing, the spatial degree of freedom within a multimode fiber (MMF) has long been recognized as a valuable asset for boosting communication rates. As we have seen, this is particularly important for QKD, for which the secure key rates are still many orders of magnitude lower than the data transfer rate of classical communication. Despite significant efforts to reduce the inevitable crosstalk in MMFs, it continues to be a major barrier for the practical use of spatial modes in QKD, particularly for long-distance applications [88].

Yet, as we shall see in this chapter, the utility of MMFs extends well beyond enhancing communication speed. A notable application consists of embedding optical linear circuits in the higher dimensional space of a MMF. Conventional designs of reconfigurable linear optical circuits are usually based on integrated optics [206, 207], where the elements are miniaturized and embedded on a chip. The construction of such devices is based on a cascade of interferometers that consists of many beamsplitters and tunable phase shifters. However, as the complexity of the circuit increases, so does the need for more beamsplitters and phase shifters. Notably, the number of these necessary components tends to increase quadratically with the circuit’s size. This rapid escalation in component count not only makes the circuit more cumbersome to implement but also significantly reduces its accuracy.

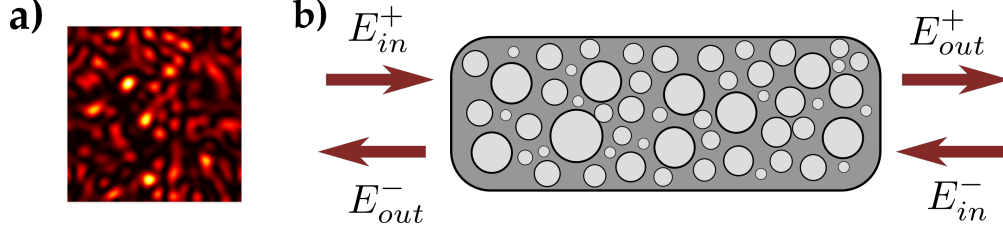
The experimental platform that we deploy, already used to simulate two-photon linear networks [83, 84], offers an innovative approach to circumvent these limitations. Instead of relying on a multitude of beamsplitters and phase shifters, we leverage the intricate mode mixing inherent in a MMF by employing *wavefront shaping techniques* for quantum information processing. Given that our key distribution scheme in Chapter 7 can be constructed from any one-way quantum communication complexity problem, our focus will be on demonstrating the practical use of optical devices that exploit complex mode mixing to tackle such quantum communication problems. Specifically, we will focus on the high-dimensional unitary operators necessary to implement the detection part of the  $\beta$ PM and VS quantum protocols, going beyond the 2-input approach proposed in [83, 84].

## 8.2 Light propagation through disordered media

### 8.2.1 Scattering theory

Light traversing a non-uniform medium undergoes scattering along various optical paths, leading, for coherent light, to the formation of a complex interference pattern at the medium’s output, known as a speckle pattern [208]. This speckle pattern acts as a distinctive mark of the medium’s irregularity under specific lighting conditions. To describe this phenomenon in a simple system, we consider a 2D geometry where monochromatic light travels through a linear waveguide, as depicted in Figure 8.1.

Even though the process is extremely complex, it remains linear and deterministic. The transformation of the incoming optical field  $E_{in}$  to the outgoing one  $E_{out}$  can be thus effectively described by a linear operator, as follows



**Figure 8.1:** a) Speckle pattern. b) Model of light scattering in a complex medium. Considering a planar geometry, the input field  $E_{in}$  consists of components from both directions:  $E_{in}^+$  when the input is from left to right, and  $E_{in}^-$  for right to left input. Correspondingly, the output field,  $E_{out}$ , also has two components: the left-to-right output  $E_{out}^+$ , and the right-to-left one  $E_{out}^-$ .

$$\begin{pmatrix} E_{out}^- \\ E_{out}^+ \end{pmatrix} = \mathbf{S} \begin{pmatrix} E_{in}^+ \\ E_{in}^- \end{pmatrix}, \quad (8.1)$$

where the linear operator  $\mathbf{S}$  is known as the *scattering matrix* of the system [4, 209]. Here, the symbols  $+(-)$  distinguish between fields propagating from left to right (and vice versa). Furthermore, the scattering matrix  $\mathbf{S}$  can be broken down as follows

$$\mathbf{S} = \begin{pmatrix} \mathbf{R} & \mathbf{T}' \\ \mathbf{T} & \mathbf{R}' \end{pmatrix}. \quad (8.2)$$

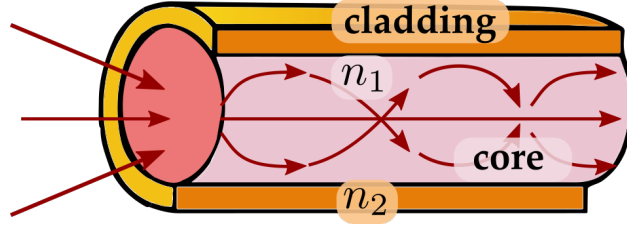
In this decomposition,  $\mathbf{R}$  and  $\mathbf{R}'$  correspond to the reflection matrices for fields entering from the left and right, respectively. The off-diagonal blocks,  $\mathbf{T}$  and  $\mathbf{T}'$ , represent the transmission matrices that describe propagation from left to right and from right to left, respectively. When there is no absorption and energy conservation is enforced, the scattering matrix  $\mathbf{S}$  becomes unitary, satisfying the condition  $\mathbf{S}\mathbf{S}^\dagger = \mathbf{1}$ . Additionally, the time-reversal symmetry indicates that  $\mathbf{S} = \mathbf{S}^T$ . Unfortunately, measuring a complex system's full scattering matrix is usually quite challenging since it requires injection and detection on both sides and the ability to control and measure all the modes.

Nevertheless, when studying a MMF, the focus of this chapter, only a negligible fraction of the energy is reflected during propagation. This is why we primarily explore the characteristics of the Transmission Matrix (TM)  $\mathbf{T}$ , which is not only measurable experimentally [210] but also useful for many different applications, such as quantum information processing and cryptography as discussed in Section 8.2.4.

## 8.2.2 Multimode fibers as complex media

Optical fibers are characterized by a core with a refractive index  $n_1$ , surrounded by a cladding with a lower refractive index  $n_2$  (where  $n_2 < n_1$ ), see Figure 8.2 for a pictorial representation. The fiber's Numerical Aperture (NA), which is the range of angles that it can accept for incoming light, is defined entirely by these two refractive indices as follows

$$\text{NA} = \sqrt{n_1^2 - n_2^2}. \quad (8.3)$$



**Figure 8.2:** Illustration of an optical fiber, composed of a core with refractive index  $n_1$  and a cladding with refractive index  $n_2$ .

Fibers with a uniform refractive index  $n_1$  are called step-index fibers. In contrast, fibers that exhibit a refractive index that varies radially are known as graded-index fibers. This varying refractive index is carefully engineered to minimize modal dispersion, a phenomenon where the propagation velocity of the optical signal is not the same for all possible light paths, or modes, causing signal distortion due to differential arrival times.

To support a high number of modes, MMFs are engineered with cores whose diameters are large compared to the wavelengths propagating through them. In particular, the number of transverse spatial modes  $N_{\text{modes}}$  capable of propagating through the fiber depends on the core radius  $r_c$ , the numerical aperture NA, and the wavelength of the light  $\lambda$  [211] according to the following relation

$$N_{\text{modes}} = 2 \left( \frac{\pi r_c \text{NA}}{\lambda} \right)^2. \quad (8.4)$$

Some appealing features of MMFs are their negligible reflectivity combined with the possibility of space-division multiplexing across thousands of modes, offering significant advantages in high bit-rate optical communications [212, 213]. Nonetheless, challenges like cross-talk among different propagating modes and modal dispersion can limit their effective communication capacities and distances. In this context, the MMF can be conceptualized as a complex scattering system, where light entering the fiber interacts and scatters due to the fiber's inherent inhomogeneities and imperfections, leading to mode mixing. Despite significant efforts to mitigate such mixing, including the study of propagation invariant modes [214], or exploiting neural networks [215–217], in our work we will consider different scenarios that can transform the presence of mode mixing from a challenge into a valuable asset.

## Modeling MMFs

Analyzing the mode mixing in MMFs is a very complex endeavor since it depends on several factors such as inhomogeneities in the refractive index, variations of core radius, impurities in the core, etc. [218]. Historically, investigations into mode mixing in MMFs have primarily employed *power-coupling models* [219–221], which examined the energy distribution among propagating modes [219] and how it varies along the fiber's length [220, 221]. Nonetheless, these models fall short in offering insights into the relative phases between modes and the type of interference occurring at the MMF's output, making them not adapted for applications involving coherent sources.

An alternative approach more suited for coherent light is based on *field-coupling models* [222–225], which investigate the impact of perturbations and impurities on coherent electric fields with a transmission matrix formalism. In particular, they focus on different properties, such as polarization-mode dispersion [223], modal dispersion [224], and mode-dependent loss [225].

Another commonly-used approach for describing MMFs is based on Random Matrix Theory (RMT) [226–228]. While it is well-known that the TM of a complex medium such as a layer of paint is well approximated by a random matrix in the pixel basis [210], MMF characterization depends in practice on the particular type of fibers. Back in 2015, Plöschner et al. [214] used a tailored theoretical model to predict the propagation of light through a step-index fiber for lengths up to hundreds of millimeters solely on their geometry, excluding the possibility of short step-index MMF being well approximated with a random matrix. Later in 2018, it was discovered that graded-index fibers with a perfectly parabolic refractive index could be predicted even more reliably than step-index fibers [229]. However, graded-index fibers turn out to be extremely sensitive to deviations from the ideal refractive index, making them good candidates for obtaining highly isotropic mixing across spatial and polarization modes.

Finally, it is worth mentioning that there is a simple open-source Python module called pyMMF [230], based on the work in [231], which allows finding the propagating modes of MMFs with arbitrary index profiles and simulates their transmission matrix.

### 8.2.3 Introduction to wavefront shaping

The concept of wavefront shaping dates back to the early 1950s, notably within the field of astronomy [232]. Astronomers faced significant challenges in observing starlight due to atmospheric turbulence, which eventually led to distorted wavefronts arriving on the telescope, causing blurred images. The main idea, proposed in [232], involved balancing this distortion by using active optical components of the telescope setup for compensation. This approach is called *adaptive optics*. In the context of perturbation correction, the term wavefront shaping, however, was coined more than 50 years later, in the seminal work of Vellekoop and Mosk [233], where they deployed a Spatial Light Modulator (SLM) to control light propagating through a layer of paint.

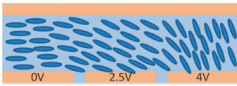

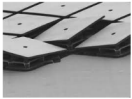
#### Spatial light modulators

Before delving into the different approaches for wavefront shaping, it is useful to analyze the different devices used to control the wavefront of an incoming beam of light. There is a wide range of SLMs, which can be divided into three main categories:

- **Liquid crystal SLMs**, which we generally call SLMs in this thesis, are composed of liquid crystal cells of a size of a few  $\mu\text{m}$  arranged in a grid. The cells' orientations, and hence their optical properties, can be altered by applying varying voltages. In particular, the change in orientation varies the birefringence of the cell, introducing a local phase shift between  $[0, 2\pi]$  on one of the polarization components of the wavefront. They have the highest number of pixels among all the other SLMs, but they have a quite slow refresh rate (a maximal speed of  $\sim 100$  Hz).

- **Micro Electro-Mechanical System (MEMS) SLMs** are arrays of micro-mirrors, each ranging in size from 10 to 100  $\mu\text{m}$ . These mirrors are capable of rapid translation, providing phase modulation in the interval  $[0, 2\pi]$  and achieving refresh rates between 10 kHz and 100 kHz. However, only a few thousand unit cells can be controlled in a single device.
- **Digital Micromirror Device (DMD)** is a particular type of MEMS, where the mirrors are rotated instead of translated. The switching between two possible angular positions guarantees a fast (up to several tens of KHz) binary amplitude modulation, while allowing to control up to  $10^6$  unit cells [234].

In Table 8.1 we summarize the main features of each technology.

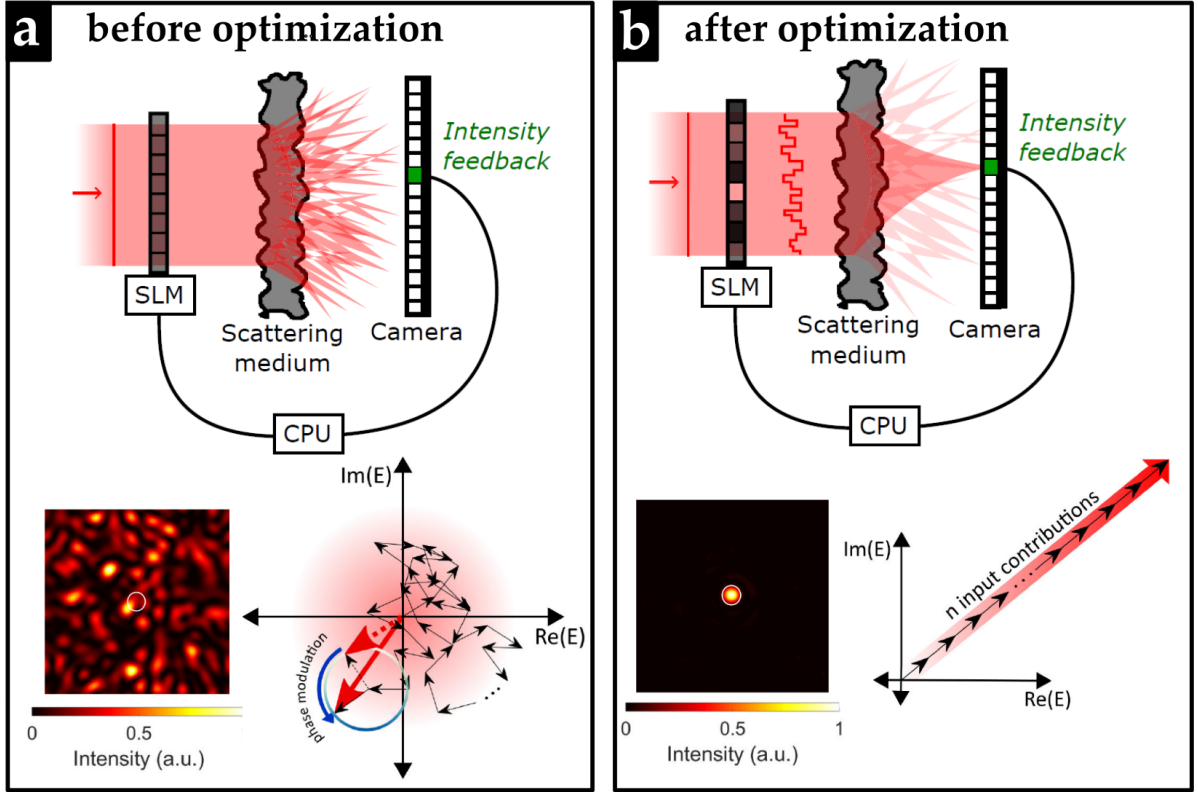
| Technology             | Liquid Crystal SLM  | MEMS   | DMD   |
|------------------------|---|--|---|
| Illustration           |  |  |  |
| Number of Pixels       | $\sim 10^6$   | $\sim 10^3$  | $\sim 10^5 - 10^6$  |
| Diffraction Efficiency | $\sim 90\%$   | 100%   | 50%   |
| Modulation             | Phase $[0, 2\pi]$   | Phase $[0, 2\pi]$  | Binary Amplitude  |
| Maximal Speed          | $\sim 100$ Hz   | $\sim 10$ kHz  | $< 100$ kHz   |
| Cost                   | $\sim 10^4\text{€}$   | $\sim 10^5\text{€}$  | $\sim 10^3\text{€}$   |

**Table 8.1:** Comparison of different types of SLM technologies. Table from [235].

## Optimization method

Going back to the first wavefront shaping experiment in [233], by detecting the light at the output of the complex medium with a camera, one can use a pixel of the camera at a specific position as a feedback signal for optimizing the phase modulation of the SLM. Specifically, this involved testing various phases for each pixel of the SLM, and subsequently keeping the phase that resulted in the maximum intensity at the targeted output. See Figure 8.3 for a pictorial representation.

While this method can achieve intensity enhancement directly proportional to the count of macro pixels on the SLM [233] and can be adapted for multiple output objectives [233] and different optimization methods [238–240], a major drawback—and a key reason for our decision not to adopt this approach—is the necessity for a full optimization procedure each time a new target is established.



**Figure 8.3:** Wavefront shaping with the optimization method. (a) Initially, the SLM’s pattern is uniform, leading to an equal contribution from each pixel. In the complex plane, this results in the fields from the SLM pixels converging at the targeted camera pixel with phases that are randomly distributed due to the scattering process. The feedback for optimization comes from the intensity reading of a specific pixel on a Electron-multiplying Charge-Coupled Device (EMCCD) camera. (b) After the optimization process, there is a significant increase in the intensity at the targeted camera pixel. This enhancement is depicted in the complex plane, where the phase components of the fields contributing to the targeted pixel now align in the same direction. This alignment leads to constructive interference, effectively amplifying the intensity at the specified output location. Figure adapted from [236, 237].

### Digital phase conjugation method

An alternative approach, proposed by S. Popoff et al. in 2010 [210], allows to focus light without the need for an optimization process. This approach is based on the general concept of *digital phase conjugation* [241]. Essentially, it leverages the time-reversal symmetry inherent in optical systems composed by a SLM and a complex medium. The process begins with the characterization of the transmission matrix  $\mathbf{T}$  of the complex medium, using a phase-stepping holographic technique detailed in Section 8.3.2. Once the transmission matrix is known, one can compute the input field  $E_{in}^{\text{target}}$  to send through the complex medium to obtain the targeted output  $E_{out}^{\text{target}}$

$$E_{out} = \mathbf{T}E_{in} \rightarrow E_{in}^{\text{target}} = \mathbf{T}^{-1}E_{out}^{\text{target}} . \quad (8.5)$$

However, in practical scenarios, the inverse  $\mathbf{T}^{-1}$  is extremely sensitive to noise [236]. This means even a slight error or noise in  $\mathbf{T}$  can lead to significant changes in  $\mathbf{T}^{-1}$ . A more robust solution is thus to consider the transpose conjugate  $\mathbf{T}^\dagger$ . In fact, the operator  $\mathbf{T}\mathbf{T}^\dagger$ , also known as the time-reversal operator, has been extensively studied in the RMT framework. In particular, it has been observed that for both layers of paint and sufficiently long MMFs, this operator closely approximates the identity operator [236, 237]. Consequently, the final output can be approximated as follows

$$\begin{aligned} E_{out} &= \mathbf{T}E_{in}^{\text{target}} \\ &= \mathbf{T}\mathbf{T}^\dagger E_{out}^{\text{target}} \\ &\simeq E_{out}^{\text{target}} + \text{noise/background} . \end{aligned}$$

In Section 8.3, we will explore how this technique not only allows the creation of intense focusing spots at the output of a complex medium, but also extends to the construction of reconfigurable linear networks.

### The time-reversal operator in the RMT framework

Understanding the properties of the  $\mathbf{T}\mathbf{T}^\dagger$  is essential in the effective use of wavefront shaping techniques. When considering a basic RMT model where the transmission matrix  $\mathbf{T}$  is a rectangular matrix of dimension  $k \times d$  with elements drawn from i.i.d. complex Gaussian random variables, it has been shown in [242] that

$$\mathbf{T}\mathbf{T}^\dagger = \mathbf{1} + \frac{1}{\sqrt{d}}\mathbf{H} , \quad (8.6)$$

where the noise term  $\mathbf{H}$  is a Hermitian matrix with normalized coefficients. This implies that with a sufficiently large number of controllable modes, the time-reversal operator can approximate the identity operator. Moreover, the probability distribution of transmission eigenvalues in the asymptotic case of this model ( $k, d \rightarrow \infty$ ), which indicates how efficiently each mode (eigenvector) transmits light, follows the so-called Marchenko-Pastur distribution [243].

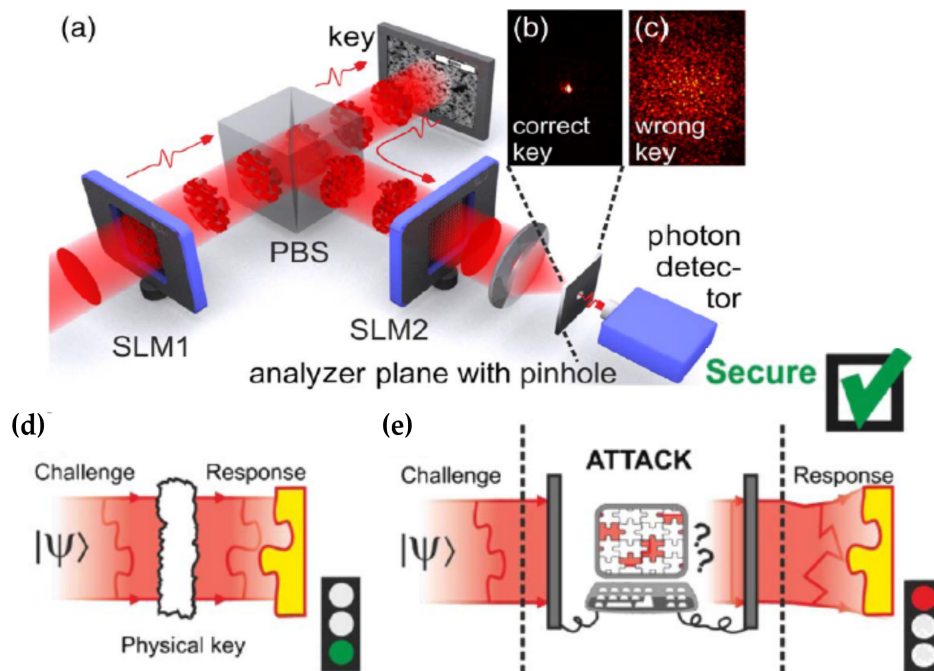
Finally, using a RMT-based concatenated fiber model [226], it has been shown in [244] that, when restricting to the sub-transmission matrix for one particular polarization, the transmission eigenvalues follow a bimodal law of the so-called Dorokhov-Mello-Pereira-Kumar (DMPK) model [245, 246].

## 8.2.4 Applications of wavefront shaping

Wavefront shaping, despite being a relatively new area of research, has had an important impact across several fields, spanning from non-invasive imaging inside biological samples [247] and RADAR imaging [248] to innovations in compressive sensing [249], to name just a few. We refer to [4] for an extensive review. In the next sections, in particular, we will focus on the impact that wavefront shaping has had on cryptography and quantum information processing, which are two central topics of this thesis.

## Applications in cryptography

Considering a highly mixing scattering medium that is too complex to be copied or emulated, has always been a fascinating direction for cryptographic applications. Such an object is usually referred to as an optical Physical Unclonable Function (PUF) or Physical One-Way Function (POWF) [85]. A pioneering cryptographic approach leveraging the inherent complexity of such media, combined with wavefront shaping techniques, is an authentication method known as Quantum-Secure Authentication (QSA) [86]. The scheme involves a



**Figure 8.4:** Illustration of a QSA. (a) setup: SLM1 generates a challenge, which is sent to the optical key. The response is then analyzed back by the SLM2. (b) When the key is correct, the response results in a bright focusing spot. (c) For any other key, instead, one obtains a random speckle. (d) A scenario where the authorized party successfully authenticates itself, but for which (e) an emulation attack fails. Adapted from [86].

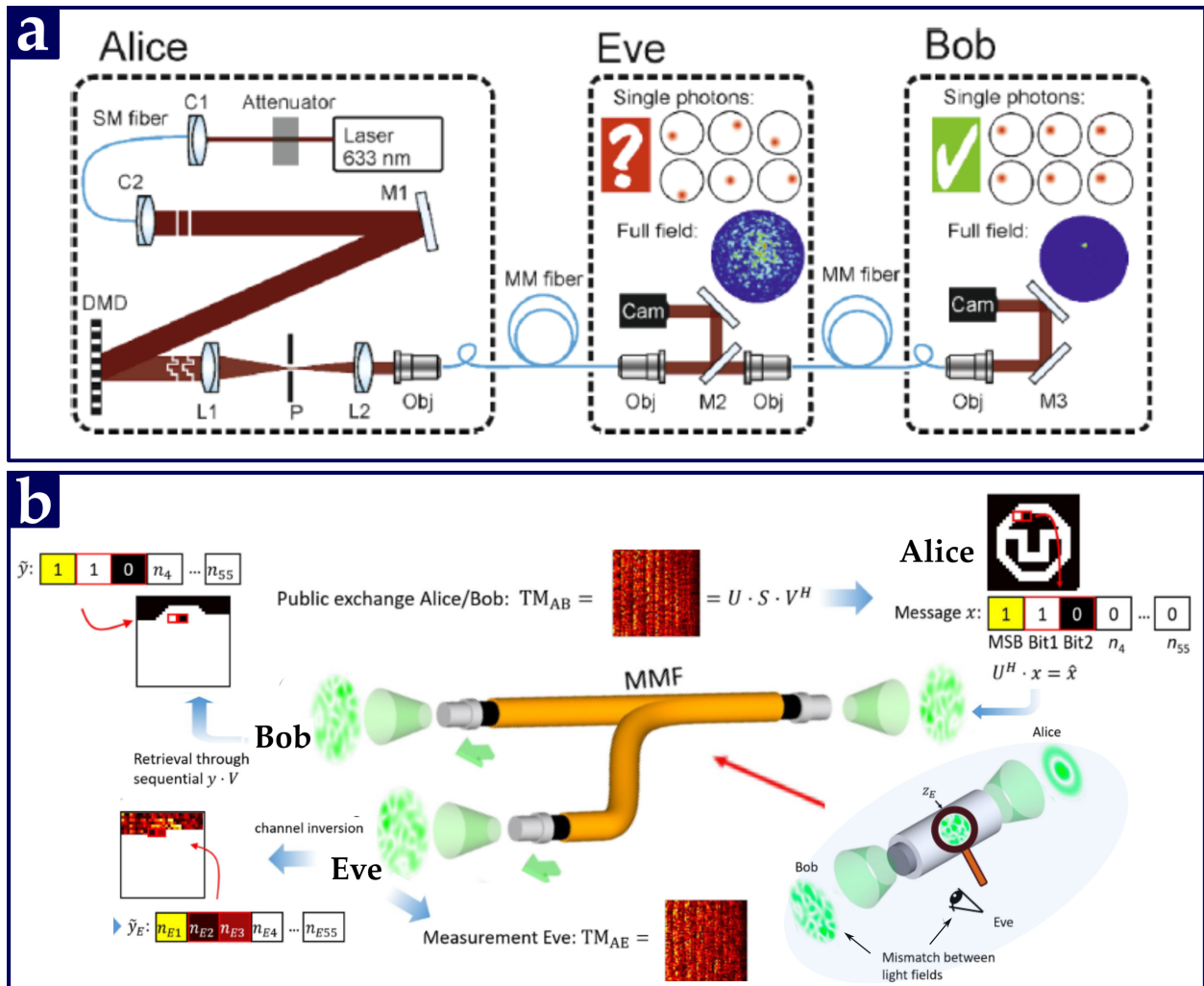
challenge-response protocol for identification where the goal is to prove that one has access to a unique physical object, called an optical key, which is hard to emulate. After manufacturing the optical key, which is a layer of paint in [86], there is a one-time characterization by measuring its transmission matrix<sup>1</sup>. With this approach, a verifier who knows the TM can send a few-photons high-spatial-dimensional quantum state and subsequently verify the response by unscrambling the corresponding speckle-like output of the optical key.

However, authentication is not the only security feature that can be provided using wavefront shaping techniques. Even in the field of QKD, these techniques could be applied to enhance the performance both for free-space [87] and fiber-based communication [88]. For instance, in [87], they showed how, by using a genetic algorithm [250, 251] optimization method, it could be possible to perform a standard free-space BB84 protocol even in scenarios

<sup>1</sup>In Figure 8.4, they considered the reflection matrix instead. However, the formalism remains the same.



with strong scattering effects, such as in the presence of clouds, dust, haze or fog, leading to an over 200-fold enhancement in transmission efficiency. Moreover, as reported in [88], Zhou et al. have already successfully established a high-fidelity communication link over a 1-km-long MMF, where over 200 spatial modes can be controlled by using real-time off-axis holography [252]. This progress represents a crucial milestone in advancing the capabilities of high-dimensional QKD systems with MMFs [253].



**Figure 8.5:** Secure data transmission over a MMF in the presence of an eavesdropper. (a) Eve performs a beam-splitting attack. When imaging into a camera, Eve’s output results in a complex interference pattern, while Bob’s results in a focus on a particular spot of the fiber output facet. Figure from [89]. (b) Eve wiretaps the channel where Bob and Eve each share 50% of the transmitted power. While Alice and Bob diagonalize their channel using the Singular Value Decomposition (SVD) based on their transmission matrix to retrieve the message, Eve measures her own TM and performs channel inversion. Figure adapted from [254]. In both (a) and (b) the security is based on the asymmetry between the transmitted matrix of the legitimate channel and that of Eve’s channel.

Secure communication has also been experimentally analyzed in the presence of an eavesdropper. One such experiment [89] involved a QKD scheme where a portion of the MMF was contained within the labs of the communicating parties, Alice and Bob. By randomly bending the MMF segment inside their labs, they could thwart an eavesdropper’s attempts to fully learn the transmission matrix. In particular, they showed experimentally how they can provide secure communication against a specific beam-splitting attack, as illustrated in Figure 8.5(a). Furthermore, an experimental demonstration of secure data transmission over a wiretapped MMF channel was reported for the first time in [254]. Here, the protocol’s security relied on the physical system’s properties between the legitimate users, employing the so-called Physical Layer Security (PLS) framework [255]. Notably, they utilized a SLM to generate tailored wiretap codes [256] based on the SVD of measured TMs, as shown in Figure 8.5(b).

### Applications in quantum information processing

The first demonstration of controlling single-photon through an opaque scattering medium [257] dates back to 2014, when they used an optimization method to focus a heralded single-photon reflected from a layer of white paint (ZnO). In the same year, Defienne et al. [258] deployed instead the digital phase conjugation method to engineer single photon-states reflecting again from a layer of paint (TiO<sub>2</sub>) and analyze their coherence properties. In 2016, wavefront shaping techniques were extended to make the SLM and the complex medium (both for an opaque scattering medium [259] and for a MMF [260]) act as a fully programmable  $2 \times 2$  beamsplitter and analyze the corresponding two-photon interference.

This first class of reconfigurable operators led to a natural extension to higher dimensions both for single-photon and two-photon linear operators. Two-photon interference with a reprogrammable  $2 \times 4$  linear operator has been first analyzed in [83] and then recently extended to 22 output ports with a SPAD array in [84], showcasing the possibility of scaling the number of controllable outputs. Following a similar approach, but only considering one input port at the time, in [90] they successfully implemented amplitude-only linear operators of dimensions up to  $8 \times 38$ .

A different approach based on single-outcome projective measurements to transport and certify two-photon entanglement has also been experimentally analyzed in [91] where they were able to construct reconfigurable linear operators of dimension up to  $7 \times 7$ . By using one SLMs at each end of the MMF, they were able to measure the TMs without the need for a reference field, being able to retrieve relative phases across the different outputs.

## 8.3 Reconfigurable optical network for quantum communication complexity

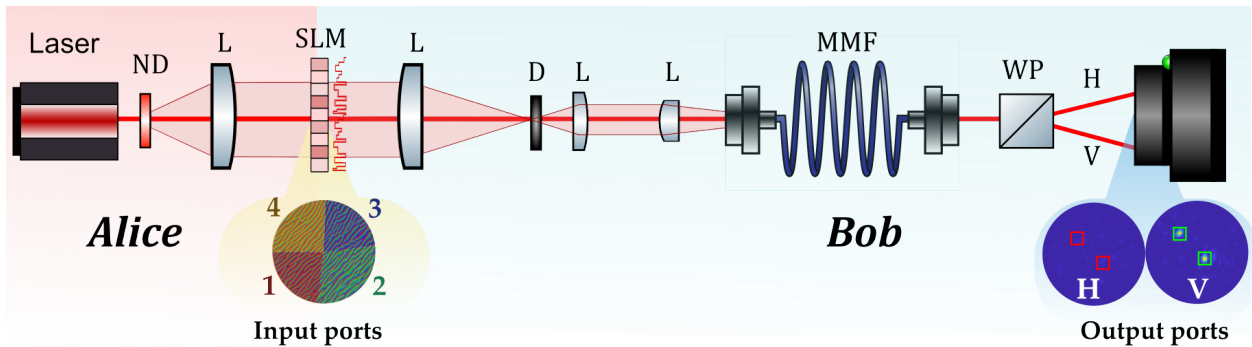
Demonstrating a quantum advantage in solving one-way quantum communication complexity problems presents a fascinating yet challenging task. This process requires the capability for high-dimensional encoding and decoding, coupled with the imperative to minimize overall loss. A key aspect is the careful selection of the right problem to demonstrate a clear advantage over classical strategies. Several factors influence this choice, such as

1. **Quantum encoding:** it's essential to assess how feasible it is for Alice to encode the targeted complex high-dimensional quantum state with the technology deployed.
2. **Quantum decoding:** on the other end, Bob's ability to perform accurate and lossless quantum decoding is equally important.
3. **Classical benchmark:** a quantum protocol that seems easier to implement might not lead to quantum advantage due to a very efficient corresponding classical communication complexity. Thus, accurately estimating both the lower and upper bounds of the classical protocols is crucial in determining the likelihood of achieving a genuine quantum advantage.

Notably, we have already performed a detailed classical benchmark for two particular communication complexity protocols, the  $\beta$ PM and VS protocols (see Section 5.3.3). On the other hand, in this chapter, we will experimentally investigate how to perform a reconfigurable and low-loss quantum decoding from wavefront shaping techniques, while Alice's encoding will be simulated by simply adding an extra phase mask layer to the SLM, as explained in Section 8.3.3. Compared to the previous experiments on the setup [83, 84], we employed a novel method of partitioning the SLM into multiple input ports, as described in Appendix D.1. This approach enables precise control over the amount of light directed to each port.

### 8.3.1 Experimental setup

As illustrated in Figure 8.6, our platform to test one-way communication complexity problems is conceptually divided into two parts.



**Figure 8.6:** Setup configuration to solve a one-way boolean quantum communication complexity problem. Alice's encoding is simulated by adding an additional mask to the SLM, which has been carefully partitioned in  $n$  ports ( $n = 4$  in this illustration). Bob uses the SLM and MMF to build a linear operator. He then divides the output in the camera into two subspaces (light H-polarized and V-polarized), where for each subspace he defines  $k/2$  macro pixels as output ports ( $k = 4$  in this illustration). If Bob detects a greater amount of light in the red detection modes, he responds with  $b = 0$ ; if not, he responds with  $b = 1$ . (L: lens, ND: neutral-density filter, D: Iris diaphragm, WP: Wollaston prism.)

- **Alice’s setup:** Alice employs a superluminescent diode to generate coherent states with a controllable mean photon number. A 1-nm bandpass filter is added on the source path so that spectral dispersion is negligible when light propagates through the MMF<sup>2</sup>. In addition, she has shared access to a SLM, a reflective liquid-crystal phase-only model (Hamamatsu, X10468-02, which is strategically partitioned into  $n$  input ports, as described in Appendix D.1. Consequently, Alice is capable of encoding a sequence of  $n$  spatially multiplexed coherent states, by displaying a phase pattern on the SLM. As a matter of fact, as indicated in [63], a one-way quantum communication complexity protocol using pure single-photon states  $|\psi\rangle$  can be mapped to coherent-state protocols, encoding a coherent state  $|\alpha, \psi\rangle$  as described in Eq. (2.30). The SLM is a reflective liquid-crystal phase-only model (Hamamatsu, X10468-02).
- **Bob’s Setup:** Bob’s apparatus includes the shared SLM and a graded-index MMF capable of supporting approximately 400 propagation modes<sup>3</sup> at 810nm (Thorlabs, GIF50C, length<sup>4</sup>  $55.3 \pm 0.1$  cm, core diameter  $50 \pm 2.5$   $\mu\text{m}$ , NA  $0.200 \pm 0.015$ ). Since our MMF present an isotropic mixing across both spatial and polarization modes, to collect two orthogonal polarizations (H and V) we use a Wollaston prism directing them to separate regions of our EMCCD camera (Andor iXon3 860). This binary division in detection is specifically designed for boolean one-way communication complexity problems.

It’s worth noting that in a practical implementation of a one-way quantum communication protocol, two SLMs would be necessary: one for Alice to encode her quantum states and another for Bob to perform the correct measurements. However, for the sake of simplicity and to minimize costs, our setup employed just a single SLM.

### 8.3.2 Acquisition of transmission matrix

In the following, we present our approach to fully characterize our MMF by independently measuring the transmission matrix  $\mathbf{T}^{(p)}$ , linking the relevant input modes for each  $p$ -th input port to the targeted output modes. In our experiment, we define the input modes as a series of focused spots arranged on an isometric grid at the input facet of the MMF. To ensure a complete characterization of the fiber we always consider  $N_{\text{input}} = 600$  different spots, a number higher than the supported modes by the MMF. Each input mode corresponds to a specific phase ramp displayed on the SLM, while the output modes are simply  $k$  macro pixels of the EMCCD camera, each of which is approximately the size of an average speckle grain. Moreover, to avoid unmodulated light getting into the MMF, we have offset the center of the MMF’s optical axis from the zeroth diffraction order by  $50\mu\text{m}$  in both horizontal and vertical directions.

---

<sup>2</sup>This is because graded-index fibers are less sensitive to modal dispersion. In particular one can define their spectral bandwidth  $\delta\omega$  as the smallest frequency shift that must be applied to the input light to achieve a complete decorrelation in the output speckle pattern. In our experiment, we work with a light source with spectral width (1 nm) much smaller than  $\delta\omega$  to make the effects of dispersion negligible.

<sup>3</sup>However, we control only the H polarization with our SLM, effectively addressing  $\sim 200$  modes.

<sup>4</sup>Length was chosen short enough to neglect spectral dispersion.

Before explaining our particular acquisition process, let us describe a general approach to measure a transmission matrix using a co-propagating reference field. This reference is used to reconstruct the complex values of the TM from intensity measurements exploiting a technique called phase-shifting holography [261].

### General TM acquisition with phase-shifting holography

Let's consider a generic linear optical system  $\mathcal{S}$ , by shifting the phase of a controlled field  $\mathbf{E}^{(S)}$  by a global phase  $\theta$  with respect to a reference field  $\mathbf{R}$  the photocurrent measured at the the  $j$ -th output mode for the  $i$ -th input mode is given by

$$\begin{aligned} I_{ji}^{(S,\theta)} &= |R_j + E_{ji}^{(S)} e^{i\theta}|^2 \\ &= |R_j|^2 + |E_{ji}^{(S)}|^2 + 2|R_j||E_{ji}^{(S)}| \cos(\phi_j^R - \phi_{ji}^{(S)} - \theta). \end{aligned}$$

In this context,  $R_j = |R_j|e^{i\phi_j^R}$  represents the complex reference field directed towards the  $j$ -th output port. Similarly,  $E_{ji}^{(S)} = |E_{ji}^{(S)}|e^{i\phi_{ji}^{(S)}}$  denotes the complex field at the  $j$ -th output mode corresponding to a specific  $i$ -th input mode, essentially forming the element of the TM for the optical system  $S$ . Shifting the phase  $\theta$  over  $N_\theta$  steps allows to compute the *unfiltered transmission matrix*  $\mathbf{M}^{(S)}$

$$\begin{aligned} M_{ji}^{(S)} &= \frac{1}{N_\theta} \sum_{\theta} [I_{ji}^{(S,\theta)} \cos(\theta) - iI_{ji}^{(S,\theta)} \sin(\theta)] \\ &= |E_{ji}^{(S)}||R_j|e^{i(\phi_{ji}^{(S)} - \phi_j^R)}, \end{aligned}$$

from which one can retrieve the transmission matrix  $\mathbf{T}^{(S)}$  by measuring the output reference intensity  $\mathbf{I}_R$

$$T_{ji}^{(S)} = \frac{M_{ji}^{(S)}}{\sqrt{I_{R_j}}} = |E_{ji}^{(S)}|e^{i(\phi_{ji}^{(S)} - \phi_j^R)}. \quad (8.7)$$

This general method allows the retrieval of a transmission matrix from a linear optical system  $\mathcal{S}$ , which still presents some unknown relative phases  $\phi^R$  of the reference field. These phases, however, are not of significance when one directly measures the output of the optical system [236]. Let us now focus on the setup in Figure 8.6. A natural way of creating a co-propagating field is by displaying an additional phase ramp to the SLM to focus part of the light onto one particular input mode of the MMF. This leads to a speckle-like reference field, which may result in low-intensity spots corresponding to targeted output modes. However, it is known that a low-intensity reference field results in an inaccurate estimation of the transmission matrix [262] and hence a limited control when deploying wavefront shaping techniques, making this approach non-optimal.

We have therefore implemented a specific measurement process to estimate the transmission matrix of the optical system in Figure 8.6 for different input ports, while maximizing the intensity of the co-propagating reference field in the targeted outputs. The measuring process is divided into two main steps: in the first step, we acquire the transmission matrix  $\mathbf{T}^{(\text{full})}$  by considering the full SLM as one single-port, with a speckle-like co-propagating field.

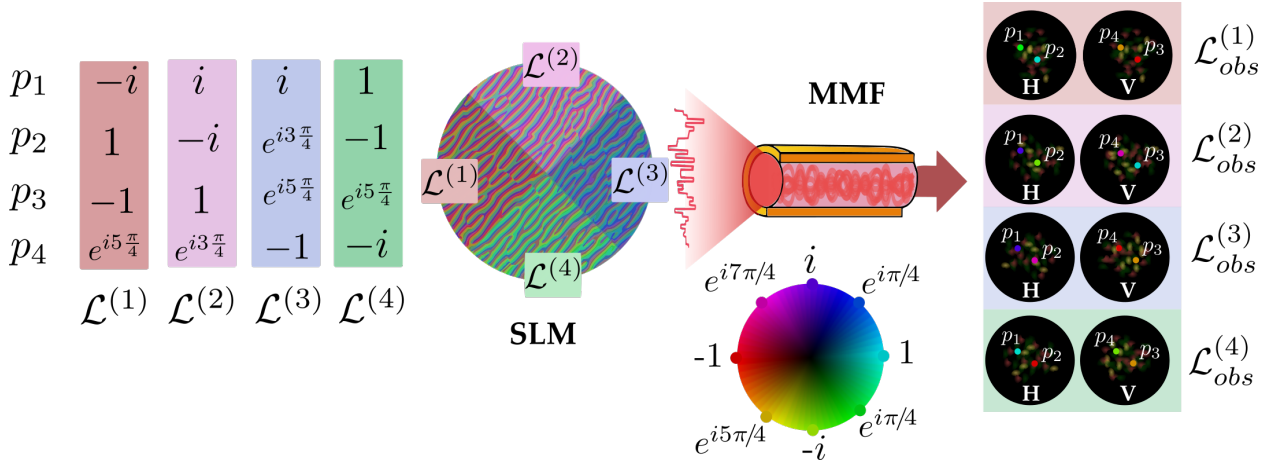
The second step consists of independently measuring the transmission matrices  $\mathbf{T}^{(1)} \dots \mathbf{T}^{(n)}$  of dimension  $k \times N_{\text{input}}$  for  $n$  different input ports<sup>5</sup>. In this phase, the new optimized reference field is obtained by adding an additional phase-layer to the entire SLM. By knowing  $\mathbf{T}^{(\text{full})}$ , one can, in fact, deploy a standard digital phase conjugation method to generate a focusing reference field in the targeted outputs. Notably, by using the same focusing reference field for all  $n$  input ports, it's possible to build a linear optical network using the measured TMs directly. This approach avoids the need for extra calibration of the references, which in [237] required a combination of photon counts and two-photon interferences analysis [263].

### 8.3.3 Construction of reconfigurable detection system

Now that the optical system has been fully characterized, we are finally ready to explain how to harness this information to build a reconfigurable  $k \times m$  linear operator  $\mathcal{L}$ . As explained before, the general concept relies on digital phase conjugation, where each  $p$ -th input port of the SLM is encoded such that optical field at the input of the MMF has the form

$$E_{in}^{(p)} = \mathbf{T}^{(p)\dagger} \mathcal{L}^{(p)}, \quad (8.8)$$

where  $\mathcal{L}^{(p)}$  is the  $p$ -th column of the linear operator, as illustrated in Figure 8.7. In particular, since the SLM is on the Fourier plane of the input face of the MMF, the phase mask displayed on each port of the SLM corresponds to the angular component of the Fourier transform of the input field in Eq. (8.8).



**Figure 8.7:** Pictorial representation of the construction of a  $4 \times 4$  linear operator. Each port of the SLM encodes a different column of the linear operator, controlling both the amplitude and the phase of the corresponding output state. The final output detected is a coherent sum of the contribution of each individual port. Illustration inspired by [237].

Therefore, the combination of the light modulation from the SLM and the mode mixing of the MMF results in an observed linear operator  $\mathcal{L}_{\text{obs}}$ , where the column encoded by the  $p$ -th input port has the form

$$\mathcal{L}_{\text{obs}}^{(p)} = \mathbf{T}^{(p)} \mathbf{T}^{(p)\dagger} \mathcal{L}^{(p)}. \quad (8.9)$$

<sup>5</sup>In this case, the controlled input field  $\mathbf{E}^{(p)}$  is obtained from the light modulated only by the  $p$ -th input port of the SLM.

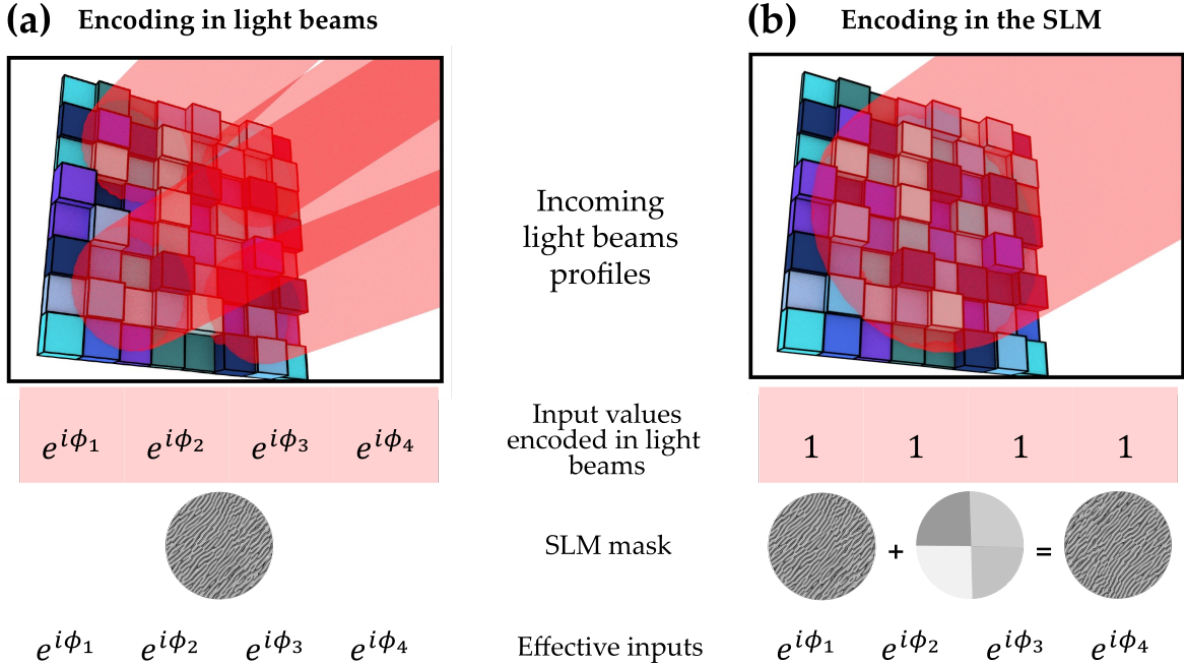
In an ideal implementation, Alice, which in the communication complexity framework has access to a classical input  $x$ , sends a  $n$ -dimensional quantum state  $|\psi_x\rangle$  to Bob, who programs his reconfigurable optical detection system presented in Figure 8.6 according to his classical input  $y$ . The output state impinging the camera has therefore the form

$$|\psi_{out}\rangle = \text{cost} \cdot \mathcal{L}_{obs} |\psi_x\rangle, \quad (8.10)$$

with  $\text{cost}$  being a constant to normalize the state. As shown in Figure 8.7, the first  $n/2$  states of the canonical basis of the output Hilbert space are defined by the output modes in the  $H$  region of the camera, while the remaining  $n/2$  are in the  $V$  region.

### Alice's encoding with one SLM

First, as explained in Section 2.2.2, any standard single-photon one-way quantum communication complexity protocol can be mapped in a coherent state protocol without changing Bob's decoding apparatus. Moreover, to further decrease the complexity of our optical network, drawing inspiration from a strategy implemented in [264], the components of the input quantum states are encoded directly on the SLM as depicted in Figure 8.8(b).



**Figure 8.8:** Alice's methods to encode input vectors for a  $4 \times 4$  linear operator. **(a)** The phases are encoded directly into multiple light beams, and the SLM mask consists only of the mask extracted from Eq. (8.8). **(b)** Only one light beam is sent which doesn't carry information. Alice's input state is encoded by adding additional phase masks to each port of the SLM. Figure adapted from [264].

Unfortunately, since the SLM can only encode phase masks, we are not able to directly simulate the input state such as the one in Eq. (5.23) used to solve the VS quantum one-way communication complexity protocol. Consequently, our experiment will be limited to

the  $\beta$ PM protocol, which requires only phase encoding. However, as discussed in Section 5.3.3, at a fixed size of the problem, the VS has a best-known classical protocol which is much more demanding in terms of communication cost with respect to the  $\beta$ PM, making it a much better candidate to show a quantum advantage. To address the limitations imposed by the SLM's encoding capabilities in the next section we perform a numerical analysis to demonstrate that even when tackling the more general VS problem, our programmable linear network can achieve performance levels comparable to those achievable in the more practically implementable  $\beta$ PM quantum protocol. This approach helps to illustrate the potential of our network in scenarios where direct simulation of certain input states is not feasible.

### 8.3.4 Scalability and flexibility of the optical network

Before we proceed with the numerical analysis of the two distinct one-way quantum communication complexity problems, it is beneficial to first explore how the performance of our network is expected to scale with an increase in the size of linear operators.

#### Scalability in the RMT model

The scalability and programmability of this general approach were studied in [83] under the straightforward RMT model, where the elements of the TMs are drawn from i.i.d. complex Gaussian random variables. Given a fiber with  $N_{\text{modes}}$  physical modes and an optical configuration with  $n$  input and  $k$  outputs ports, one can think of each input port of the SLM being able to effectively address only  $N_{\text{modes}}/n$  of these physical modes. Consequently, the single-port transmission matrix  $\mathbf{T}^{(p)}$  is effectively a  $k \times (N_{\text{modes}}/n)$  random matrix. From Eq. (8.6) an estimation of the single-port time-reversal operator is given by

$$\mathbf{T}^{(p)}\mathbf{T}^{(p)\dagger} = \mathbf{1} + \sqrt{\frac{n}{N_{\text{modes}}}}\mathbf{H}, \quad (8.11)$$

which still converges to the identity operator when the number of physical modes goes to infinity. A metric to quantify the difference of the implemented linear operator from the ideal one is the *fidelity*  $\mathcal{F}$  of the difference between the two operators, defined as

$$\mathcal{F}(\mathcal{L}_{\text{obs}}, \mathcal{L}) := 1 - \frac{\|\mathcal{L}_{\text{obs}} - \mathcal{L}\|_1}{nk}, \quad (8.12)$$

where  $\|A\|_1 := \sum_{i=1}^k \sum_{j=1}^n |A_{ij}|$  is the  $l_1$ -vector norm. From Eqs. (8.9) and (8.11) the asymptotic scaling of the fidelity in this model was found to be

$$\mathcal{F}(\mathcal{L}_{\text{obs}}, \mathcal{L}) = 1 - \mathcal{O}\left(\sqrt{\frac{nk}{N_{\text{modes}}}}\right). \quad (8.13)$$

This equation suggests a critical relationship between the dimensions of linear operators and the number of physical modes  $N_{\text{modes}}$ . Specifically, to increase the dimensionality of square operators ( $k = n$ ) linearly, a quadratic increase is required in the number of physical modes ( $N_{\text{modes}} = \mathcal{O}(n^2)$ ). An increase in the number of physical modes can be achieved, for instance, by engineering MMFs with greater diameters or higher numerical apertures, as shown in Eq. (8.4).



## Numerical analysis for one-way communication complexity

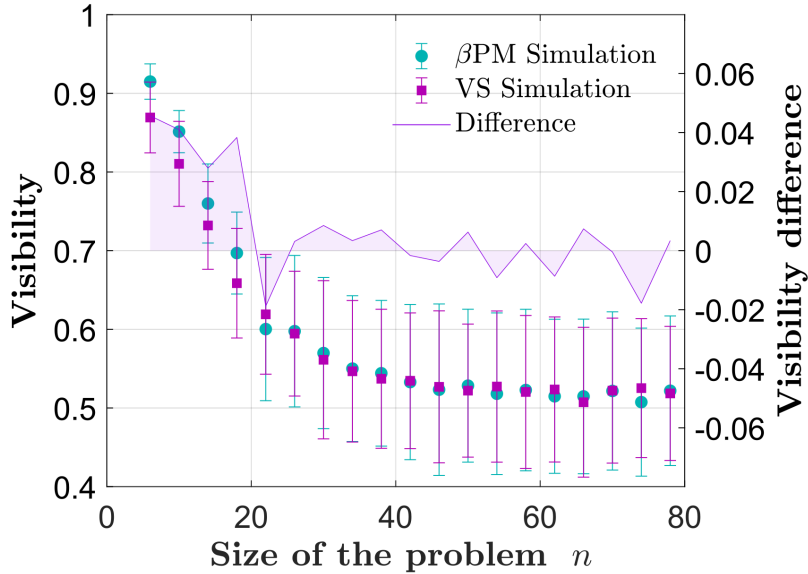
Finally, we are interested to see how this flexibility specifically applies when trying to solve VS and  $\beta$ PM problems, with a model which is closer to our experimental apparatus. In particular, we will consider a measured transmission matrix  $\mathbf{T}^{(\text{full})}$  of size  $k \times N_{\text{input}}$  when using the full SLM as a unique port. We then, following the philosophy of the previous paragraph, extract each single-port transmission matrix  $\mathbf{T}^{(p)}$  not by directly measuring them, but by dividing the full transmission matrix into  $n$  submatrices, i.e.  $\mathbf{T}^{(\text{full})} = \left| \mathbf{T}^{(1)} \right| \dots \left| \mathbf{T}^{(n)} \right|$  of dimension  $k \times N_{\text{input}}/n$ . From now on, since we consider only square linear operators, we will always consider  $k = n$ . Considering for the sake of simplicity lossless single-photon protocols, we choose as a figure of merit to compare the two protocols the *visibility*  $V$  of the boolean detection system, defined as the probability of each photon going in the right region of the camera

$$V = \langle \psi_{\text{out}} | \Pi(a) | \psi_{\text{out}} \rangle, \quad (8.14)$$

with  $a \in \{0, 1\}$  being the correct answer. The operators

$$\Pi(0) = \sum_{i \in H} |i\rangle\langle i|, \quad \Pi(1) = \sum_{i \in V} |i\rangle\langle i| \quad (8.15)$$

represent the POVM associated with the boolean response.



**Figure 8.9:** Numerical simulation for the visibility of  $\beta$ PM and VS protocols. Alice’s input states are in the form of Eqs. (5.17) and (5.23), respectively. The detection linear operator implemented for the  $\beta$ PM corresponds to the unitary matrix in Eq. (C.1). In contrast, the operator for the VS protocol is a random unitary matrix that defines the two distinct subspaces.

Therefore, visibility can be interpreted as the probability of correctly guessing in a one-way quantum communication complexity problem, where a single photon is sent in a scenario

without any loss. As displayed in Figure 8.9, the visibility rapidly decreases with the size of the problem, which is in accordance with the scaling in Eq. (8.13). Moreover, the visibility difference between the  $\beta$ PM<sup>6</sup> and VS protocols is at most 4%, showcasing that the effectiveness of our detection method is influenced not by the specific linear operator used but solely by the size of the linear network.

### 8.3.5 Experimental analysis

In the following section, the experimental results for the  $\beta$ PM quantum protocol are presented using the setup shown in Figure 8.6. First, a calibration of the setup is performed, where the SLM is partitioned in  $n = (4, 6, 8)$  input ports (Appendix D.1), then the transmission matrices linking the  $n$  ports to the  $k = n$  output ports are measured (Section 8.3.2). Finally, Alice's encoding and Bob's decoding are programmed using the SLM (Section 8.3.3). Alice's quantum state is the coherent-state version of the state in Eq. (5.17). Specifically, it is given by

$$|\alpha, x\rangle = \bigotimes_{p=1}^n \left| \frac{\alpha}{\sqrt{n}} (-1)^{x_p} \right\rangle_p, \quad (8.16)$$

where  $x \in \{0, 1\}^n$  is Alice's input and  $\alpha$  is a complex amplitude. By modulating the intensity of the output beam of the superluminescent diode and selecting accordingly the exposure time of the EMCCD camera, we can control the average amount of photons  $|\alpha|^2$  that Alice is sending per round of the protocol, resulting in a quantum communication cost of  $\mathcal{O}(|\alpha|^2 \log(n))$  qubits<sup>7</sup>.

#### Error analysis

The output state impinging the camera after encoding on the SLM Bob's linear operator  $\mathcal{L}_{\beta\text{PM}}(y)$  in Eq. (C.1) has the form

$$\begin{aligned} |\alpha, x, y\rangle &= \bigotimes_{j=1}^n \left| \alpha \sqrt{\frac{\eta}{n}} \sum_{p=1}^n (-1)^{x_p} \left( \mathbf{T}^{(p)} \mathbf{T}^{(p)\dagger} \mathcal{L}_{\beta\text{PM}}^{(p)}(y) \right)_j \right\rangle_j \\ &= \bigotimes_{j=1}^n \left| \alpha_j^{(x,y)} \right\rangle_j, \end{aligned} \quad (8.17)$$

where we defined  $\alpha_j^{(x,y)} := \alpha \sqrt{\frac{\eta}{n}} \sum_{p=1}^n (-1)^{x_p} \left( \mathbf{T}^{(p)} \mathbf{T}^{(p)\dagger} \mathcal{L}_{\beta\text{PM}}^{(p)}(y) \right)_j$  the new complex amplitudes for the  $j$ -th and  $\eta$  the overall efficiency of optical setup.

Let  $D_H$  ( $D_V$ ) be the random variable corresponding to the number of clicks in the  $H$  ( $V$ ) region. Since each the output state in Eq. (8.17) is still a tensor product of  $n$  coherent states, these two variables are

<sup>6</sup>We chose  $\beta = \frac{1}{2}$  to ensure fair comparison with the VS protocol by avoiding additional losses due to partial matchings. This same principle has been followed in the experimental phase as well.

<sup>7</sup>In the following we consider  $|\alpha|^2 \log(n)$  as the effective number of transmitted qubits. However, to upper bound the quantum communication cost, one should derive the precise prefactors from [63, Theorem 1]

distributed according to Poissonian distributions  $D_H \sim \text{Poisson} \left( \mu = \sum_{j \in H} \left| \alpha_j^{(x,y)} \right|^2 \right)$  and  $D_V \sim \text{Poisson} \left( \mu = \sum_{j \in V} \left| \alpha_j^{(x,y)} \right|^2 \right)$ . Considering the bit  $a$  being the right answer, then the error probability  $\epsilon$  of the protocol is

$$\epsilon = \begin{cases} \Pr(D_H > D_V) + \frac{1}{2}\Pr(D_H = D_V) & \text{if } a = 0, \\ \Pr(D_H < D_V) + \frac{1}{2}\Pr(D_H = D_V) & \text{if } a = 1. \end{cases} \quad (8.18)$$

## Setup efficiency

Before presenting the experimental results, it is crucial to further discuss the different sources of loss in our optical system, detailed in Table 8.2. Notably, we have calculated the efficiency of the optical pathway, from the source of the coherent state to the output of the MMF, at approximately 70%. This efficiency reduction is primarily attributed to two factors: the limited reflectivity of the SLM, which has an efficiency of  $\eta_{\text{SLM}} \approx 90\%$ , and the transmission efficiency  $\eta_{\text{MMF}} \approx 80\%$  through the MMF itself. The efficiency loss in the MMF is largely due to losses at the injection of the fiber. This is because the guiding core of the MMF acts as a spatial filter (both spatially and in numerical aperture—i.e. angularly), and some of the high-frequency components of the SLM patterns are filtered. On the detection end, our EMCCD camera exhibits a quantum efficiency of  $\eta_{\text{det}} \approx 75\%$ . However, the main source of loss in the camera arises from utilizing only a limited number of macro pixels as detection ports, which represent a minor portion of the camera’s active area. Notably, the total amount of light directed to the specific  $n$  detection ports of the camera constitutes merely  $\eta_{\text{ports}} \approx 8\%$ <sup>8</sup> of the overall light that impinges the camera. While opting for larger detection ports could significantly boost the efficiency  $\eta_{\text{ports}}$ , such an increase beyond the size of a speckle grain would result in capturing additional light that is not precisely controlled, lacking any information about Alice’s encoding.

| Parameter   | Value |
|---|-------|
| SLM reflectivity: $\eta_{\text{SLM}}$             | 90%   |
| MMF transmission: $\eta_{\text{MMF}}$             | 80%   |
| Detector quantum efficiency: $\eta_{\text{det}}$  | 75%   |
| Detection ports efficiency: $\eta_{\text{ports}}$ | 8%    |

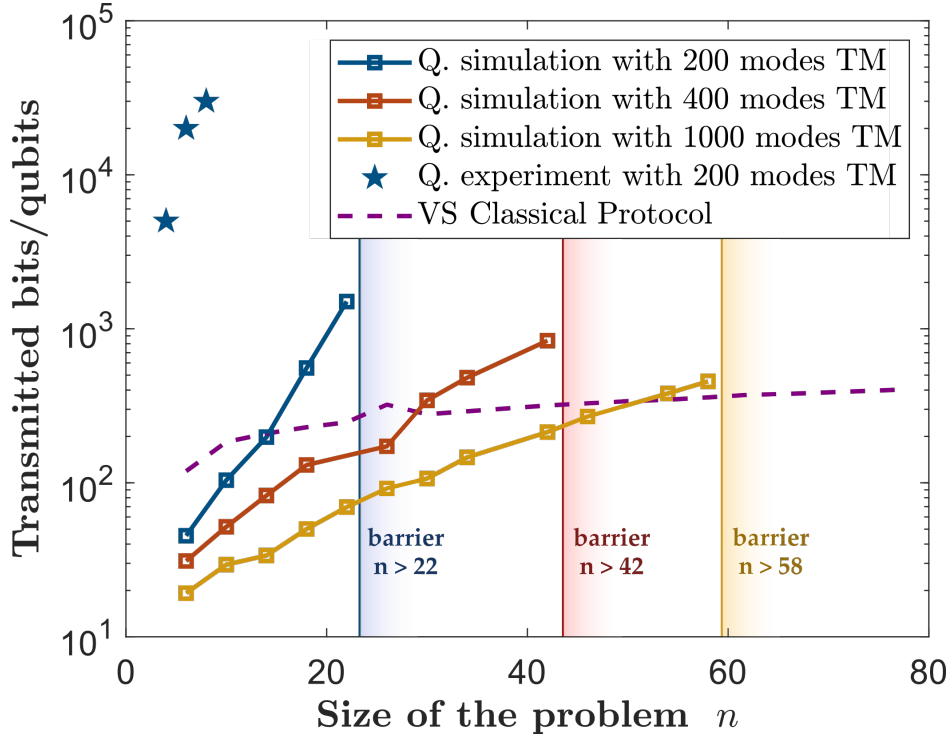
**Table 8.2:** Summary of the efficiency parameters measured in the implementations. All of them have been used in the simulations except  $\eta_{\text{ports}}$ , which has been recalculated when performing the numerical simulations<sup>9</sup>, due to its dependency on the accuracy of the linear operator’s implementation.

<sup>8</sup>Experimentally, the stability of  $\eta_{\text{ports}}$  is maintained even as the number  $n$  of ports increases. This occurs because the reduced accuracy in impinging the detection ports due to a larger linear operator is balanced by a corresponding increase in the detected region of the camera.

<sup>9</sup>To recalculate  $\eta_{\text{ports}}$  in the simulations, we considered a TM carrying the amplitude and phase information of each pixel of the camera.

## Quantum $\beta$ PM and classical benchmark with VS

We are now ready to analyze the performance of our experiment and benchmark it with the best-known classical protocol for the VS problem, analyzed in Appendix C.2. For each partition of the input ports, we performed the  $\beta$ PM protocol over  $l = 500$  instances of the variables  $\mathbf{x} = (x_1, \dots, x_l)$  and  $\mathbf{y} = (y_1, \dots, y_l)$ , where every pair  $(x_i, y_i)$  was drawn from the probability distribution  $\mu_{\beta PM}$  presented in Section 5.3.1. In particular, we fine-tuned the beam intensity and the exposure time of our EMCCD camera to ensure the error probability estimated from the  $l$  instances of the protocol was below a targeted error threshold. We have then measured the number of transmitted photons  $|\alpha|^2$ , and hence the number of transmitted qubits  $|\alpha|^2 \log(n)$ , by injecting the output of the photon source into an avalanche photodiode. As shown in Figure 8.10, experimentally, we required  $(5 \cdot 10^3, 2 \cdot 10^4, 2.5 \cdot 10^4)$  transmitted qubits to solve the  $\beta$ PM problem with an error rate of  $\epsilon = 0.2$  for  $n = (4, 6, 8)$  ports, respectively.



**Figure 8.10:** Plot of the transmitted number of qubits vs. the input size  $n$  for solving the  $\beta$ PM problem within error probability  $\epsilon = 0.2$ . It includes quantum simulations for MMFs with varying mode numbers ( $N_{\text{modes}} = 200, 400, 1000$ ). For each mode count, there are color-coded barriers (blue, red, and yellow, respectively) indicating the maximum  $n$  beyond which the problem cannot be solved within the specified error limit. Furthermore, the graph also includes a comparison with the transmitted bits required by the best-known classical protocol for the VS problem, as deduced from Theorem 5.3.3, serving as a classical benchmark.

We compared the results also to a set of numerical simulations for  $N_{\text{Modes}} = (200, 400, 1000)$ , where for the 200 modes MMF we considered as before a measured transmission matrix  $\mathbf{T}^{(\text{full})}$

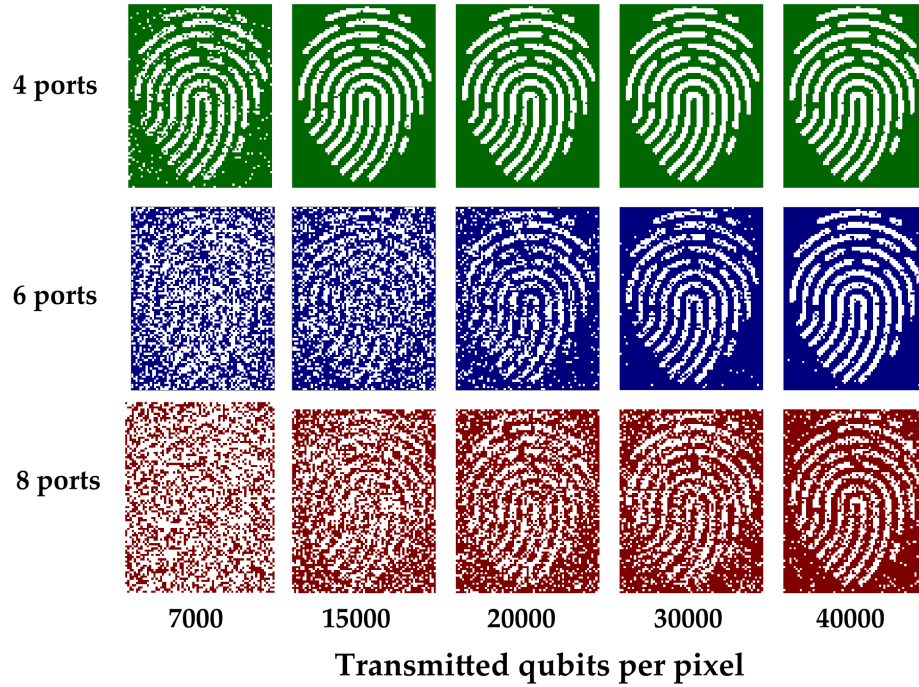
and then divided it into  $n$  submatrices. For the simulation of TMs with a higher number of modes we have simply copied the initial transmission matrix and reshuffled the modes. Although our method is still several magnitudes away from the classical benchmark for the VS problem, the quantum simulations demonstrate its potential to achieve a quantum advantage. Moreover, they highlight again how beneficial it would be to increase the number of effective modes of the MMF.

It is natural to ask why there is such a difference between the simulation and the experiment. First, the simulation assumes perfect wavefront shaping, both in amplitude and phase, which results in a better implementation of the linear operator. However, this is not the only reason. For instance, what we observe from the simulation for 200 modes is that it is impossible for this approach to solve the problem with an error rate of  $\epsilon = 0.2$  for  $n > 22$ , not even sending an infinitely large number of qubits. This is because, for more than 20% of the possible inputs, the protocol will give the wrong answer no matter how much light one decides to send. Nonetheless, it can easily solve the problem for  $n = 22$  by sending only a bit more than a thousand qubits. This gives a pitch for our experimental implementation, as we could still achieve the desired guessing probability by enhancing the signal-to-noise ratio, namely, by increasing the transmitted number of qubits. This suggests that additional noise is present at the detection end, which is not accounted for in Eq. (8.3.5). A further characterization and reduction of dark currents and background events could therefore lead to better performance.

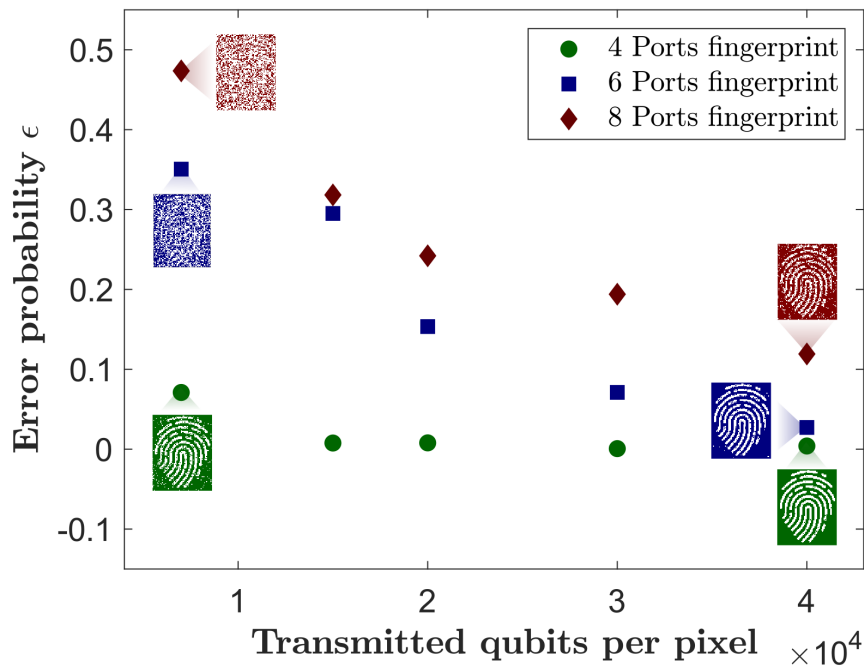
### **$\beta$ PM as a quantum communication channel**

To further explore how well our experimental setup can perform the  $\beta$ PM protocol, we considered a quantum communication scenario where Alice and Bob use  $l = 6 \cdot 10^3$  instances of the  $\beta$ PM protocol to share a binary image of a fingerprint. One can imagine that Alice and Bob have agreed in advance on a set of inputs  $\mathbf{y} = (y_1, \dots, y_l)$ . Alice can then simply choose accordingly each of her inputs  $\mathbf{x} = (x_1, \dots, x_l)$  in order for her to transmit the fingerprint. Specifically the  $j$ -th binary pixel of the targeted image has the value  $a_j = \beta\text{PM}(x_j, y_j)$ .

The experimental results in Figure 8.11 clearly demonstrate that an image with 4 ports becomes distinctly visible with as few as  $7 \cdot 10^3$  transmitted qubits per pixel. When the number of ports increases to 6 and 8, the quantity of qubits required for a clear image does rise significantly, yet the transmission of well-defined images remains achievable. For example, with  $4 \cdot 10^4$  qubits transmitted per pixel, we can successfully transmit an image with 8 ports while maintaining a pixel error rate of  $\epsilon = 0.12$ . See Figure 8.12 for the full plot of the pixel error rates achieved for each image with respect to the number of transmitted qubits per pixel.



**Figure 8.11:** Experimental transmission of a binary classical fingerprint image with  $6 \cdot 10^3$  pixels solving the  $\beta$ PM quantum protocol.



**Figure 8.12:** Plot of error probabilities of the experimental transmission of a binary classical fingerprint solving the  $\beta$ PM problem.

## 8.4 Conclusion

The investigation of novel quantum communication complexity problems with better separations stands as a vibrant and dynamic area of interest. In this context, having a sound and flexible platform for assessing quantum communication protocols and clearly showing the benefits of quantum technology is extremely valuable for advancing the field.

In this chapter, we have introduced one such optical platform leveraging spatial degrees of freedom, specifically designed for addressing quantum communication problems. Our strategy is based on the intricate mode mixing within a MMF, coupled with the precise shaping of the incoming light wavefront. This method's key strength is its flexibility, which enables the implementation of Bob's detection phase for any quantum communication complexity problem.

In particular, we applied this method to the detection part of the  $\beta$ PM quantum protocol, evaluating its effectiveness and discussing how it can be scaled up for larger linear operators by increasing the number of modes supported by the fiber. Additionally, we believe that by leveraging various multiplexing techniques, such as spectral, timing, and polarization, we can enable the solution of quantum communication problems in higher dimensions. Another possibility to dramatically increase the size of the Hilbert space under manipulation is to use and control multiple entangled photons, offering another exciting area for further exploration.

Finally, focusing on one single communication problem, we noticed that our reconfigurable detection platform is particularly effective for problems necessitating the encoding of a wide spectrum of quantum linear operators. An example is the VS problem, for which its classical best-known protocol is quite demanding in terms of communication compared to the  $\beta$ PM problem. Here, we observe that enhancing the number of controllable modes and reducing external noise could potentially lead to outperforming its classical counterpart.

---

## PERSPECTIVES

As we draw this manuscript to an end, this final chapter is dedicated to exploring the various future directions and perspectives that emerge from my PhD research.

### **Prioritizing is the key to practical security**

We have started our journey with my first research project in the world of quantum cryptography, proposing a novel methodology for security certification described in Chapter 4. The introduction of an attack rating methodology in the context of QKD brings new perspectives to the design of quantum cryptographic hardware: the search for strong theoretical security should be balanced with the practical need to keep implementation complexity manageable and reduce the presence of possible loopholes. This dialectic approach is likely to trigger the exploration of novel trade-offs in cryptographic system design.

Furthermore, advancements in the field of vulnerability assessments would play a crucial role in shedding light on the actual security benefits that quantum cryptography can deliver. By doing so, it could help dispel some of the skepticism that national security agencies have recently voiced about QKD [47, 48], establishing a clearer understanding of its practical implications.

### **QCT model exploration and security proof extension**

The second part of my PhD was mostly theoretical and focused on finding novel cryptographic constructions based on the hybrid QCT model. Yet, it's also valuable to more closely examine the mathematical foundation of the QCT model itself. One idea is to formalize the classical short-term encryption assumption in Definition 6.4.1 using a security notion of semantic security against quantum adversaries [265, 266]. With such a formal definition, it would be possible to rigorously show that an eavesdropper cannot exploit in any way the ciphertext  $\text{Enc}_k(y)$ , generated from input  $y$ , before reaching the computational time  $t_{comp}$ .



Additionally, the security of the HM-QCT key distribution scheme is currently only provable within an i.i.d. scenario. However, the general attack in Figure 6.2 could be considered with an extended quantum system  $Q$  including the quantum states sent across all the communication rounds. The most challenging part is to be able, as in the i.i.d. scenario, to effectively show a security reduction to the gap between quantum and classical one-way communication complexity. A promising approach involves leveraging the additivity feature of internal information complexity<sup>1</sup>, as outlined in Lemma 5.2.2. This lemma suggests, in simpler terms, that solving  $n$  independent instances of a communication problem simultaneously doesn't offer a more efficient solution than tackling them one after the other, thereby effectively reducing to an i.i.d. scenario.

## Find novel cryptographic constructions from QCT

The security proof that we have established for a key distribution scheme based on the  $\beta$ PM problem could also be applied to any one-way communication complexity problem with a boolean output. The results illustrated in Chapter 7 hence also pave the way to the study of other communication complexity problems with larger gaps between classical and quantum strategies, which would lead to even greater performances. For instance, it would be interesting to investigate whether one could employ the *k-correlation problem* [267], a query-complexity problem<sup>2</sup> which can be mapped to a communication complexity problem through the *query to communication lifting theorem* [268]. In particular, the corresponding communication complexity problem shows a classical-quantum separation of  $\Omega(n^{1-\epsilon})$  vs  $\mathcal{O}(\log n)$  where  $\epsilon > 0$  can be made arbitrarily small, improving upon the  $\Omega(\sqrt{n})$  vs  $\mathcal{O}(\log n)$  separation of the  $\beta$ PM problem.

Finally, communication complexity is not the only framework that one could explore within the QCT model. Another interesting direction is to consider *pseudorandom quantum states* [269]. A keyed family of  $n$ -qubit quantum states  $\{|\psi_k\rangle\}_{k \in \{0,1\}^\lambda}$  is said to be a pseudorandom state if any polynomially many copies (in  $\lambda$ ) of  $|\psi_k\rangle$  is computationally indistinguishable from the same number of copies of a state drawn from the  $n$ -qubit Haar distribution. In particular, Ji, Liu, and Song [269] conjectured a method, later proved by Brakerski and Shmueli [270], for creating pseudorandom states from uniform binary superpositions with post-quantum one-way functions. Within the QCT model, Alice and Bob could first agree on a key  $k$  by using a short-term encryption scheme. To send a message secret message  $m \in \{0,1\}^n$  to Bob, Alice would then generate a pseudorandom state encoding the message  $m$  into a  $n$ -qubit state with such a family of post-quantum one-way functions. By knowing the key  $k$ , Bob would be able to retrieve the message, while an unauthorized adversary would receive a pseudorandom state as their direct input. Hence, when reducing to an immediate measurement strategy, this state would be indistinguishable from a random quantum state sampled according to the Haar measure, intuitively ensuring the security of the communication protocol.

---

<sup>1</sup>It's important to highlight that our security proof relies on external information complexity at this stage. To pivot towards a dependence only on internal information, we are yet to identify a one-way compression scheme necessary to formulate an analog of Lemma 5.2.4 specific to internal information complexity.

<sup>2</sup>In a query model you are given a black-box access to some input. Your goal is to compute a function of the input while minimizing the number of queries.

## Cryptographic constructions with provable security from complex media

In Chapter 8 we have presented our approach to have a reconfigurable platform for one-way communication complexity using MMFs. However, it would be interesting to focus more on the possible quantum cryptographic constructions based on the isotropic mode mixing of the MMFs and other forms of complex media. The main idea would be to leverage the theoretical work on quantum PUFs that has been conducted in the last years [271–275] and apply it to cryptographic constructions similar to the pioneering experiment [86] depicted in Figure 8.4. The security of this protocol has only been analyzed against some specific strategies such as an intercept-resend attack [276], and attacks focused on retrieving information from an unknown challenge state [277, 278]. This would raise an important question: is it feasible to develop a practical challenge-response authentication system employing wavefront shaping techniques, while also ensuring its security in a rigorous and general mathematical framework? Notably, a recent patent [279] on such quantum authentication methods indicates a growing interest, not only from an academic standpoint but also from an industrial perspective.



---

# METHODS FOR SATURATION ATTACKS

## Contents

---

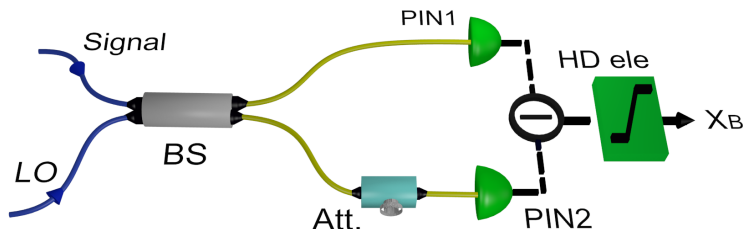
|            |  |            |
|------------|--|------------|
| <b>A.1</b> | <b>Experimental setup</b>                  | <b>138</b> |
| A.1.1      | Bob's homodyne detector                    | 138        |
| A.1.2      | Setup for incoherent attack strategy       | 139        |
| <b>A.2</b> | <b>Estimation of channel parameters</b>    | <b>140</b> |
| <b>A.3</b> | <b>Noise model and attack tuning</b>       | <b>140</b> |
| <b>A.4</b> | <b>Asymptotic secret key rate for GG02</b> | <b>141</b> |

---

## A.1 Experimental setup

### A.1.1 Bob's homodyne detector

As explained in a balanced homodyne detection, the signal is mixed with an intense local oscillator on a 50/50 beam splitter. Quadrature information is retrieved by subtracting the photocurrents generated from two photodiodes of identical detection efficiency connected at the output ports of the beam splitter. Due to the imperfect splitting ratio of the beam splitter, as well as the efficiency mismatch of photodiodes, it is necessary to add appropriate attenuation at the respective output port of the beam splitter, see Figure A.1. This equalizes



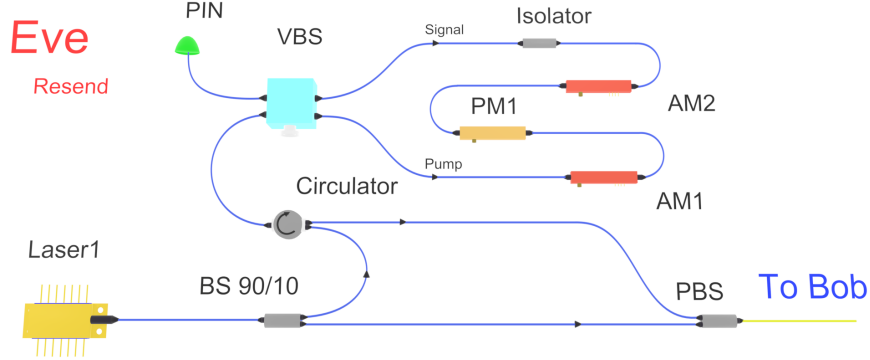
**Figure A.1:** Balanced homodyne detection at Bob's side. An attenuator (Att) in one of the output ports of the 50/50 Beam Splitter (BS) balances the photocurrent generated from photodiodes PIN1 and PIN2. Homodyne electronics circuit amplifies the subtracted photocurrents.

the photocurrents and hence sets the mean of the output voltage of the homodyne detection close to zero. This is referred to as balancing the homodyne or, more precisely "balancing the homodyne with respect to the local oscillator port". It has been shown that such balancing is essential to reduce the excess noise due to local oscillator intensity fluctuation [280]. In case of imperfect balancing, one of the photodiodes generates more current than the other. As a result, the value of the homodyne output shifts towards the detection limit, and this may lead to saturation.

The reason for saturation is due to the limited amplification factor of homodyne electronic circuitry. In our case, the circuit is made around an Amptek A250 charge amplifier, powered by  $\pm 5V$  power supply, that exhibits detection limit  $\alpha_1$  at  $-2.5V$  in the negative DC level and  $\alpha_2$  at  $+3.3V$  in the positive DC level (which is observed while interchanging photodiodes). Saturation behavior is also observed while setting a low dynamic range of the data acquisition card (say,  $\pm 2V$ ) that is used to acquire homodyne output for post-processing. In this work, we have set the data acquisition card range at  $\pm 5V$ . Thus, the linear range is limited solely by the homodyne electronic circuitry.

### Setup for coherent attack strategy

The experimental setup shown in Figure A.2 implements the resend session of the saturation attack. We have implemented CV-QKD  $EvE_{resend}$  system [281] using a Sagnac loop realized with a Variable Beam Splitter (VBS).



**Figure A.2:** Experimental setup for generating displaced coherent state. In the Sagnac loop, Gaussian modulated signals are prepared using the amplitude modulator AM1 and the phase modulator PM1 and are then displaced at the VBS, based on a coherent interference with the pump. Displaced signals are then sent to Bob along with the local oscillator.

We have used a 1530.12nm pulsed laser of width 50ns, at a repetition rate of 1MHz, to generate this displaced signal. Displacing the signal is achieved as follows. The VBS, with splitting ratio  $\approx 99.9\%$ , splits the pulse from the circulator into two. Less intense signal pulse in a clockwise direction goes under Gaussian modulation by the first amplitude modulator AM1 and the phase modulator PM1 and is further heavily attenuated by an isolator (connected in reverse to achieve an attenuation higher than 30dB). The highly intense pulse travels along anti-clockwise directions, referred to as pump pulse, meets the signal pulse at the VBS and displaces it [282]. The amplitude modulator AM2 controls the intensity of the pump and hence the amount of displacement  $\Delta$ . A PIN diode attached to the VBS helps to monitor the stability of displacement operation. The Sagnac configuration helps to lock the relative phase of the pump pulse and signal pulse to zero. Finally, the circulator directs the displaced signal towards the Polarization Beam Splitter (PBS) that polarization multiplexes the local oscillator and displaced signal to the output fiber channel.

### A.1.2 Setup for incoherent attack strategy

In this version of attack, Eve sends external laser pulse of 20ns width, along with signal pulse in the same polarization but at different wavelength (1550.12nm). The signal laser and incoherent laser pulses are synchronized with proper delay. At Bob station, he performs the same homodyne measurement as in the coherent attack strategy, where incoherent laser pulse is polarisation demultiplexed along with signal. It exploits two features of the homodyne setup: imbalance of the homodyne experienced by the light through signal port and also wavelength dependent splitting ratio of the beam splitter [283–285]. By taking into account the wavelength dependent effect and the attenuator value adjusted for the local oscillator, the effective transmittance applied to the incoherent laser is approximately  $T_{bs} \approx 49\%$ , while the transmittance applied to local oscillator is about  $T_{lo} \approx 50\% \pm 0.05\%$ . The equivalence

of the intensity  $I$  of the incoherent laser pulse to the displacement  $\Delta$  can be given by

$$\Delta = \sqrt{\eta_b/I_{lo}}(1 - 2T_{bs})I, \quad (\text{A.1})$$

where  $\eta_b$  is the efficiency of Bob and  $I_{lo}$  is the local oscillator intensity. Therefore, varying intensity of the incoherent light shifts the mean of the homodyne output towards the saturation limit  $\alpha_1$  and as a result affects the output variance.

## A.2 Estimation of channel parameters

In CV-QKD system that uses the quantum channel is characterized by its transmission  $T$  and its excess noise  $\xi$ . These parameters are estimated from Alice and Bob's modulated and measured quadratures. Under saturation attack, these parameters are modified into  $T_{sat}$  and  $\xi_{sat}$ . During the intercept-resend attack, the quadrature measured by Eve is:  $X_M = X_A + X_0 + X'_0$ , where  $X_0$  is the vacuum noise quadrature due to Alice preparation and  $X'_0$  is due to 3dB loss from Eve's heterodyne measurement. The resent signal takes the form:  $X_E = \sqrt{\frac{G}{2}}(X_M + X_{N_{A,E}}) + \Delta_X + X''_0$ . Here,  $G$  is the amplification factor to compensate the loss from the heterodyne detection,  $X_{N_{A,E}}$  accounts the technical noise from Alice and Eve,  $X''_0$  is due to coherent state preparation by Eve. The term  $\Delta_X$  determines the amount of shift in the mean value of quadrature. The same formalism holds true also for  $P$  quadrature. The parameter estimation takes the form [67]

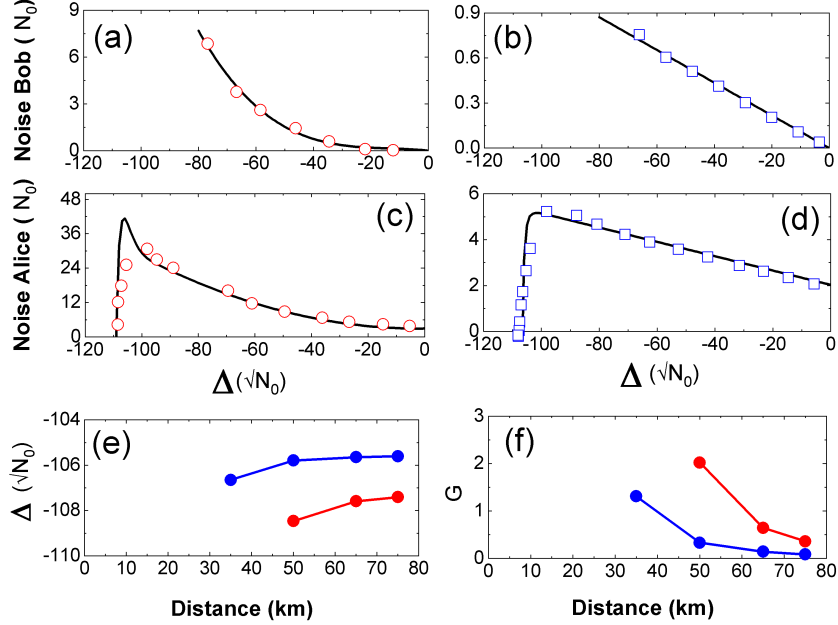
$$\begin{aligned} T_{sat} &= 2\langle X_A X_{B_{sat}} \rangle^2 / (G\eta_B V_A^2) \\ \xi_{sat} &= \frac{2}{G\eta_B T_{sat}} (V_{B_{sat}} - G\eta_B \frac{T_{sat}}{2} V_A - N_0 - \nu_{ele}), \end{aligned} \quad (\text{A.2})$$

where,  $X_{B_{sat}}$  and  $V_{B_{sat}}$  denote quadrature and its variance measured under saturation attack. Moreover,  $\nu_{ele}$  is the electronic variance of the homodyne detector. One aspect of the attack worth mentioning here is that we assume that Eve does not tamper with the shot noise calibration phase.

## A.3 Noise model and attack tuning

To evaluate optimal values of  $\Delta^1$  and  $G$  for successful attack, it is essential to characterize the noises associated with displacement as well as incoherent laser pulse. In the absence of a resent signal, displacement pump/incoherent light is sent to Bob, and the amount of noise is recorded for various values of  $\Delta$ . This helps to model the excess noise at Bob, shown in Figure A.3(a) and (b), and it is taken into account during optimization of  $\Delta$  and  $G$ . Figure A.3(c) and (d) show excess noise at Alice with respect to  $\Delta$ . Value of detection limit  $\alpha_1$  is calibrated as  $-106\sqrt{N_0}$  ( $-2.5V$  expressed in shot noise unit) for the optimization. For each transmission distance and for respective optimal  $V_A$ ,  $\Delta$  and  $G$  are calculated such that excess noise falls below the null key threshold. The optimal values are those that correspond to a maximum key rate, with  $T_{sat} = T$ , shown in Figure A.3(e) and (f). It can be seen

<sup>1</sup>As we have seen in Eq. (A.1), we can consider  $\Delta$  as a parameter to optimize for both the attack strategies.



**Figure A.3:** Excess noise due to displacement (a)-(d). Red circles and blue squares represent noise from coherent displacement and incoherent light, respectively. Black lines are theoretical fits with the respective noise model. (a) and (b) show excess noise at Bob induced by  $\Delta$ . Noise from coherent displacement shows quadratic behavior while incoherent light adds noise from its own shot noise which is linear. Noise at Alice is shown in (c) and (d). (e)-(f) Optimal values of  $\Delta$  and  $G$  at a various distance calculated based on noise model from (a) and (b). Red and blue dots represent coherent and incoherent attacks, respectively.

that at a transmission distance shorter than 50km and 35km, respectively for coherent and incoherent attack strategy, no values of  $G$  and  $\Delta$  are able to meet attack success conditions. The difference in feasible distances may have an impact on the attack potential as it affects the rating factors: (i) knowledge of TOE (which is here the knowledge of optimized QKD signal parameters for those distances) and (ii) window of opportunity (as it is easy to meet attack conditions at a shorter distance than longer distances). However, such deviations will be relevant for larger distance differences and less visible for differences between 50km and 35km. In the incoherent attack strategy, the average power of the incoherent light required to reach the detection limit  $\alpha_2 = -106\sqrt{N_0}$  is observed as 5.55uW.

## A.4 Asymptotic secret key rate for GG02

Here we present the asymptotic key rate for the GG02 protocol, introduced in Section 3.3. In a reverse error correction scenario, the general Devetak-Winter bound in Eq. (3.10) can be rewritten as

$$R_\infty = \gamma_{\text{sift}} (I(A : B) - I(B : E)) . \quad (\text{A.3})$$

One can first notice that for each signal, Alice and Bob always agree on one quadrature, resulting in  $\gamma_{\text{sift}} = 1$ . Moreover, the mutual information between Alice and Bob can be



written as

$$I(A : B) = \frac{1}{2} \log(1 + \text{SNR}) . \quad (\text{A.4})$$

Here the term SNR is the signal-to-noise ratio given by  $\text{SNR} = \frac{TV_A}{1+\chi_{\text{tot}}}$ , where  $\chi_{\text{tot}}$  is the total noise above the shot noise. The analysis of the mutual information between Bob and Eve is, however, more tricky. First, we need to consider the EB version of the protocol. In such a protocol, one can assume without loss of generality that Eve possesses a purifying system for the state  $\rho_{AB}$  shared by Alice and Bob. Then we use a very useful result known as *the optimality of Gaussian attacks* [286], which implies that one can determine the mutual information by restricting  $\rho_{AB}$  to a particular class of states, called *Gaussian states* [96].

Explaining in detail how to calculate the mutual information between Bob and Eve for this particular type of states goes beyond the scope of this thesis. Instead, we'll summarize the key findings and recommend referring to [287] for a comprehensive derivation. The mutual information  $I(B : E)$  can hence be estimated from Alice's variance  $V_A$ , the channel transmission  $T$ , and the excess noise  $\xi$ , as follows

$$I(B : E) = \sum_{i=1}^2 G\left(\frac{\lambda_i - 1}{2}\right) - G\left(\frac{\lambda_3 - 1}{2}\right) , \quad (\text{A.5})$$

where  $G(x) = (x + 1) \log_2(x + 1) - x \log_2 x$ ,  $\lambda_{1,2}$  are the symplectic eigenvalues [96] of the covariance matrix characterizing the purified system for  $A$  and  $B$ , and  $\lambda_3$  the eigenvalue for the state remaining after Bob's measurement. The eigenvalues can be determined as

$$\lambda_{1,2}^2 = \frac{1}{2} \left( \Delta \pm \sqrt{\Delta^2 - 4D} \right) , \quad (\text{A.6})$$

$$\lambda_3^2 = V \left( V - \frac{T(V^2 - 1)}{1 + T(V - 1) + T\xi} \right) , \quad (\text{A.7})$$

where one defines

$$\Delta := V^2 + (1 + T(V - 1) + T\xi)^2 - 2T(V^2 - 1) , \quad (\text{A.8})$$

$$D := (1 + T(V - 1) + T\xi)V - T(V^2 - 1) , \quad (\text{A.9})$$

with  $V := V_A + 1$ .

## ONE-WAY COMPRESSION SCHEME

### B.1 Derivation of Theorem 5.2.1

For the sake of completeness, in this section we show how to derive Theorem 5.2.1, which is an analog result to [164, Corollary 7.7] with a concrete constant. First, we need to define a one-way compression scheme to transmit integers in an optimal way.

**Lemma B.1.1** (Compression scheme). *Let  $z \in \mathbb{N}$ . There exists a one-way protocol that allows Alice to communicate  $z$  to Bob using at most  $\log(z) + 1.262 \log(\log(z)) + 6.3$  bits.*

*Proof.* The protocol consists of two phases. In the first phase Alice sends  $y := \lceil \log(z) \rceil$  in base 3 using the two-bit letters 00, 01, 10. Alice then sends the bits 11 to indicate to Bob that the first phase is complete. In the second phase Alice sends the binary representation of  $z$  to Bob. Note that because Bob knows  $\lceil \log(z) \rceil$ , he knows when the protocol stops.

In the first phase of the protocol Alice sends  $\lceil \log_3(\lceil \log(z) \rceil) \rceil$  two-bit letters plus an additional two bits to complete the phase. Thus the total number of bits can be bounded as

$$\begin{aligned}
 2\lceil \log_3(\lceil \log(z) \rceil) \rceil + 2 &\leq 2 \log_3(2) \log(\lceil \log(z) \rceil) + 4 \\
 &\leq 2 \cdot 0.631 \log(\lceil \log(z) \rceil) + 4 \\
 &= 1.262 \log(\lceil \log(z) \rceil) + 4 \\
 &\leq 1.262 \log(\log(z) + 1) + 4 \\
 &\leq 1.262 \log(\log(z)) + 5.3 ,
 \end{aligned}$$

where in the last inequality we used the fact that  $\log(x + 1) \leq \log(x) + 1$  for  $x \geq 1$ . In the second step Alice only needs to send  $\lceil \log(z) \rceil \leq \log(z) + 1$  bits. By combining the upper bounds we obtain the claimed result.  $\square$

Then, we can use Claim 7.9 of [164], and replace the Claim 7.8 by our Lemma B.1.1 to complete the derivation.



# QUANTUM COMMUNICATION COMPLEXITY

## Contents

|            |  |            |
|------------|--|------------|
| <b>C.1</b> | <b><math>\beta</math>-Partial Matching problem</b> | <b>146</b> |
| C.1.1      | Detection linear operator for quantum protocol     | 146        |
| C.1.2      | Derivation of Theorem 5.3.1                        | 147        |
| C.1.3      | Best known classical protocol                      | 148        |
| <b>C.2</b> | <b>Vector in a Subspace problem</b>                | <b>150</b> |
| C.2.1      | Best known classical protocol                      | 150        |
| <b>C.3</b> | <b>General practical quantum protocol</b>          | <b>154</b> |
| C.3.1      | QBER and $p_{\text{abort}}$ derivation             | 154        |

## C.1 $\beta$ -Partial Matching problem

### C.1.1 Detection linear operator for quantum protocol

In the quantum protocol for the  $\beta$ PM problem, Bob's detection approach, depicted in Figure 5.3, can be described by a linear operator. Specifically, the  $2\beta n \times n$  linear operator  $\mathcal{L}_{\beta\text{PM}}(y)$ , which precedes the final detection phase involving the mode combiner, depends on the matching  $M \in \mathcal{M}_{\beta n}$  and the vector  $\omega \in \{0, 1\}^{\beta n}$ , which together they form the input  $y = (M, \omega)$ . As a matter of fact, the linear operator can be decomposed in a sequence of permutations and pair-wise interference operations

$$\mathcal{L}_{\beta\text{PM}}(y) = \mathbf{P}^{(\omega)} \mathbf{H} \mathbf{P}^{(M)}. \quad (\text{C.1})$$

Given the matching  $M$  of size  $\beta n \times n$  with binary entries, the permutation matrix  $\mathbf{P}^{(M)}$  of size  $2\beta n \times n$  is constructed as follows. For each row  $i$  in  $M$ , ranging from 1 to  $\beta n$ , locate the column indices  $j_1, j_2$  where  $M_{i,j_1} = M_{i,j_2} = 1$ . Then, in the matrix  $\mathbf{P}^{(M)}$ , set

$$P_{2i-1,j_1}^{(M)} = 1 \quad \text{and} \quad P_{2i,j_2}^{(M)} = 1. \quad (\text{C.2})$$

This results in a permutation matrix  $\mathbf{P}^{(M)}$  where each pair of rows  $(2i - 1, 2i)$  corresponds to the non-zero column indices of the  $i$ -th row in  $M$ . Now, we want each pair of modes to interfere through a beam splitter, which is formally described by the action of the operator

$$\mathbf{H} = \mathbf{I}_{\beta n} \otimes \mathbf{H}_2, \quad (\text{C.3})$$

where  $\mathbf{I}_{\beta n}$  is an identity matrix of size  $\beta n$ , ensuring that the Hadamard operation  $\mathbf{H}_2$  is applied independently to each pair of matched modes. Finally,  $\mathbf{P}^{(\omega)}$  is a permutation matrix that reorganizes the elements based on Bob's input  $\omega$ . First, let us consider the matrix  $\mathbf{G}$ , which reorders all the modes. The modes with odd indices are mapped to the first  $\beta n$  modes and the even ones to the last  $\beta n$  modes. One such map is the following permutation matrix

$$G_{ij} = \begin{cases} 1 & \text{if } j = 2i - 1 \text{ for } i = 1, \dots, \beta n, \\ 1 & \text{if } j = 2(i - \beta n) \text{ for } i = \beta n + 1, \dots, 2\beta n, \\ 0 & \text{otherwise.} \end{cases} \quad (\text{C.4})$$

Let now  $\tilde{\mathbf{P}}^{(\omega)}$  be an  $2\beta n \times 2\beta n$  permutation matrix corresponding to the binary vector  $\omega$ , where for each pair  $(2i - 1, 2i)$  with  $i = 1, 2, \dots, \beta n$ , we have

$$\tilde{P}_{jk}^{(\omega)} = \begin{cases} 1 & \text{if } (j, k) = (2i - 1 + \omega_i, 2i - 1) \text{ or } (j, k) = (2i - \omega_i, 2i), \\ 0 & \text{otherwise.} \end{cases} \quad (\text{C.5})$$

This definition ensures that if  $w_i = 1$ , the  $i$ -th pair  $(2i - 1, 2i)$  is flipped, while if  $\omega_i = 0$ , the pair remains unchanged. The final permutation matrix  $\mathbf{P}^{(\omega)}$  is then obtained by combining the two operators

$$\mathbf{P}^{(\omega)} = \mathbf{G} \tilde{\mathbf{P}}^{(\omega)}. \quad (\text{C.6})$$

### C.1.2 Derivation of Theorem 5.3.1

In [3] the authors prove that, given  $\beta \in (0, 1/4]^1$  and  $\epsilon_1 \in (0, 1/2)$ , for any deterministic protocol  $\pi$  for the  $\beta$ PM problem that has a communication cost at most  $\gamma\epsilon_1\sqrt{n/\beta} + \log(\epsilon_1)$ , with  $\gamma$  a positive constant which we will determine afterward, the probability of success with respect to the distribution  $\mu_{\beta PM}$  is upper bounded by  $\frac{1}{2} + \frac{5}{2}\sqrt{\epsilon_1}$ . To make the correspondence with Theorem 5.3.1, we can write  $\epsilon_1$  in terms of the error probability  $\epsilon$  by noticing that  $1 - \epsilon \leq \frac{1}{2} + \frac{5}{2}\sqrt{\epsilon_1}$ . This in fact implies  $\epsilon_1 \geq \frac{4}{25} \left(\frac{1}{2} - \epsilon\right)^2$ . By definition of the distributional complexity we can therefore obtain Theorem 5.3.1, where all we need now is to retrieve the desired upper bound  $\gamma \leq \frac{1}{8e}$ .

#### Bounding $\gamma$

Still from [3], in their analysis they require the value of  $\gamma \geq 0$  to be small enough to satisfy the following inequalities:

$$\frac{\epsilon_1^2}{2} \geq \sum_{\text{even } k=2}^{4c-2} \left( \frac{64e\gamma^2\epsilon_1^2}{k} \right)^{k/2} \quad (\text{C.7})$$

$$\frac{\epsilon_1^2}{2} \geq \left( 8\sqrt{2}e\gamma\epsilon_1\sqrt{\frac{\beta}{n}} \right)^{2c}, \quad (\text{C.8})$$

with  $c \geq 1$ . First, let's prove that the bound  $\gamma \leq \frac{1}{8e}$  implies Eq. (C.7). We notice that  $\gamma \leq \frac{1}{8e} \leq \sqrt{\frac{1}{96e}}$ , resulting in  $96e\gamma^2 \leq 1$ . Then we obtain the following bound for  $\frac{\epsilon_1^2}{2}$ :

$$\begin{aligned} \frac{\epsilon_1^2}{2} &\geq \frac{96e\gamma^2\epsilon_1^2}{2} && (\text{From } 1 \geq 96e\gamma^2) \\ &\geq \frac{32e\gamma^2\epsilon_1^2}{1 - 32e\gamma^2} && (\text{Using } 2 \leq 3 - 96e\gamma^2) \\ &\geq \sum_{k=1}^{\infty} (32e\gamma^2)^k \epsilon_1^2 && (\text{Given } \sum_{k=1}^{\infty} x^k = \frac{x}{1-x}) \\ &\geq \sum_{k=1}^{\infty} (32e\gamma^2\epsilon_1^2)^k && (\text{From } \epsilon_1 < 1) \\ &\geq \sum_{\text{even } k=2}^{\infty} \left( \frac{64e\gamma^2\epsilon_1^2}{k} \right)^{k/2} && (\text{Using } k > 1) \\ &\geq \sum_{\text{even } k=2}^{4c-2} \left( \frac{64e\gamma^2\epsilon_1^2}{k} \right)^{k/2}. && (\text{Truncating the sum}). \end{aligned}$$

---

<sup>1</sup>Note that in this thesis we have used the notation  $\beta$  in place of the  $\alpha$  from [3].

To conclude, we demonstrate that  $\gamma \leq \frac{1}{8e}$  implies (C.8). First, we notice that we can rewrite the bound as  $\frac{1}{2} \geq (4\sqrt{2}e\gamma)^2$ . Then, as before, we derive the desired upper bound for  $\frac{\epsilon_1^2}{2}$ :

$$\begin{aligned} \frac{\epsilon_1^2}{2} &\geq \left(8\sqrt{2}e\gamma\epsilon_1\frac{1}{2}\right)^2 && \text{(From } \frac{1}{2} \geq (4\sqrt{2}e\gamma)^2) \\ &\geq \left(8\sqrt{2}e\gamma\epsilon_1\sqrt{\frac{\beta}{n}}\right)^2 && \text{(Using } \epsilon_1 < \frac{1}{2}) \\ &\geq \left(8\sqrt{2}e\gamma\epsilon_1\sqrt{\frac{\beta}{n}}\right)^{2c}, && \text{(Given } c \geq 1 \text{ and } \beta/n \leq \frac{1}{4}). \end{aligned}$$

### C.1.3 Best known classical protocol

In this section we analyze the best known classical protocol for the  $\beta$ PM problem, introduced in section 5.3.1. First, for the sake of completeness we restate the full protocol.

**Classical protocol  $\pi_{\beta PM}$ :** Alice and Bob can exploit their public randomness to agree on a subset  $\mathbf{s} := \{j_1, \dots, j_d\} \in \mathcal{S}$ , where  $\mathcal{S}$  is the set of all the possible subsets of  $d$  indices in  $[n]$ . Subsequently, Alice transmits the corresponding bit values  $\mathbf{x}_{\mathbf{s}} := (x_{j_1}, x_{j_2}, \dots, x_{j_d})$  to Bob. As such, the communication cost of this protocol is  $d$ . Consequently, in this protocol, Bob receives the corresponding  $\frac{d(d-1)}{2}$  edges<sup>2</sup>. We call  $\sigma(\mathbf{s})$  the set of all those edges. Finally, Bob, by knowing  $\omega$ , can give the right answer whenever he gets at least an edge in the matching  $M$  and randomly guesses the bit otherwise.

Next, we proceed to prove Theorem 5.3.2, which we also restate here for completeness.

**Theorem 5.3.2.** *Let  $d \in \mathbb{N}$ . An explicit one-way public-coin protocol  $\pi_{\beta PM}$  exists with a communication cost  $CC(\pi_{\beta PM}) = d$  which solves the  $n$ -dimensional  $\beta$ PM protocol with an error probability for any input at most*

$$\epsilon_{\beta PM}(d) = \sum_{k=0}^d \frac{\binom{2\beta n}{k} \binom{n-2\beta n}{d-k}}{2^{\binom{n}{d}}} e^{-\frac{k(k-1)}{4\beta n}}. \quad (5.20)$$

*Proof.* First, we define  $\mathbf{s}_M$  as the list of all the vertices in the  $\beta$ -matching  $M$ . For example, let  $n = 4$  and  $M$  be a perfect matching (i.e.  $\beta = 1/2$ ) such that  $M = \{(1, 2), (3, 4)\}$ <sup>3</sup>, then  $\mathbf{s}_M = \{1, 2, 3, 4\}$ . We call  $d_M$  the number of indices in  $\mathbf{s}$  that are part of  $\mathbf{s}_M$ , i.e.  $d_M := |\mathbf{s} \cap \mathbf{s}_M|$ . One can evaluate probability distribution of  $d_M$ :

$$P(d_M = k) = \frac{\binom{2\beta n}{k} \binom{n-2\beta n}{d-k}}{\binom{n}{d}}, \quad (C.9)$$

<sup>2</sup>Whenever we say that Bob receives an edge, say  $(j_1, j_2)$ , it implies that he acquires the bit values assigned to the corresponding vertices, i.e.  $(x_{j_1}, x_{j_2})$ .

<sup>3</sup>Note that here we use the equivalent pairs notation for the matching  $M$ .

where  $\binom{n}{d}$  is the number of ways to pick  $d$  indices in  $[n]$ ,  $\binom{2\beta n}{k}$  is the number of ways to pick  $k$  indices which are part of a  $\beta$ -matching  $\mathbf{s}_M$  and  $\binom{n-2\beta n}{d-k}$  is instead the number of ways to pick  $d-k$  indices which are not part of a  $\beta$ -matching  $M$ <sup>4</sup>.

We now want to evaluate the probability of Bob not receiving any edge which is part of his  $\beta$ -matching for a known value of  $d_M$ . Trivially, whenever Bob doesn't receive any index in  $\mathbf{s}_M$  then the probability of not receiving any edge which is part of  $M$ , i.e.  $d_M = 0$ , is always equal to 1, otherwise we have

$$\begin{aligned}
P(\nexists(i, j) \in \sigma(\mathbf{s}) \text{ s.t. } (i, j) \in M | d_M = k) &= \prod_{l=1}^k \left( \frac{2\beta n - 2(l-1)}{2\beta n - (l-1)} \right) \\
&= \prod_{l'=0}^{k-1} \left( 1 - \frac{l'}{2\beta n - l'} \right) \\
&\leq \prod_{l'=0}^{k-1} \left( 1 - \frac{l'}{2\beta n} \right) \\
&\leq e^{-\sum_{l'=0}^{k-1} \frac{l'}{2\beta n}} \\
&\leq e^{-\frac{k(k-1)}{4\beta n}},
\end{aligned} \tag{C.10}$$

where in the first line we used that, after having checked that the first  $l-1$  indices in  $\mathbf{s}_{d_M}$  do not form any edge in  $M$ ,  $2\beta n - 2(l-1)$  is the remaining number of possible indices in  $\mathbf{s}_M$  that won't form an edge in  $M$  when paired with the indices in the already extracted list  $\{j'_1, \dots, j'_{l-1}\}$ , and  $2\beta n - (l-1)$  is the total number of remaining indices in  $\mathbf{s}_M$ . In the second line we have simply replaced  $l$  with  $l' := l-1$ . The third line is obtained by noticing that  $\frac{a}{x-a} > \frac{a}{x}$  for any  $x, a > 0$  with  $x > a$ . The fourth and fifth lines follow from  $1-x < e^{-x}$  and  $\sum_{i=0}^{k-1} i = k(k-1)/2$  respectively.

Finally, since Bob, by knowing  $\omega$ , can give the right answer whenever he gets at least an edge in the matching  $M$  and randomly guesses the bit otherwise, the error probability for the best-known protocol is at most

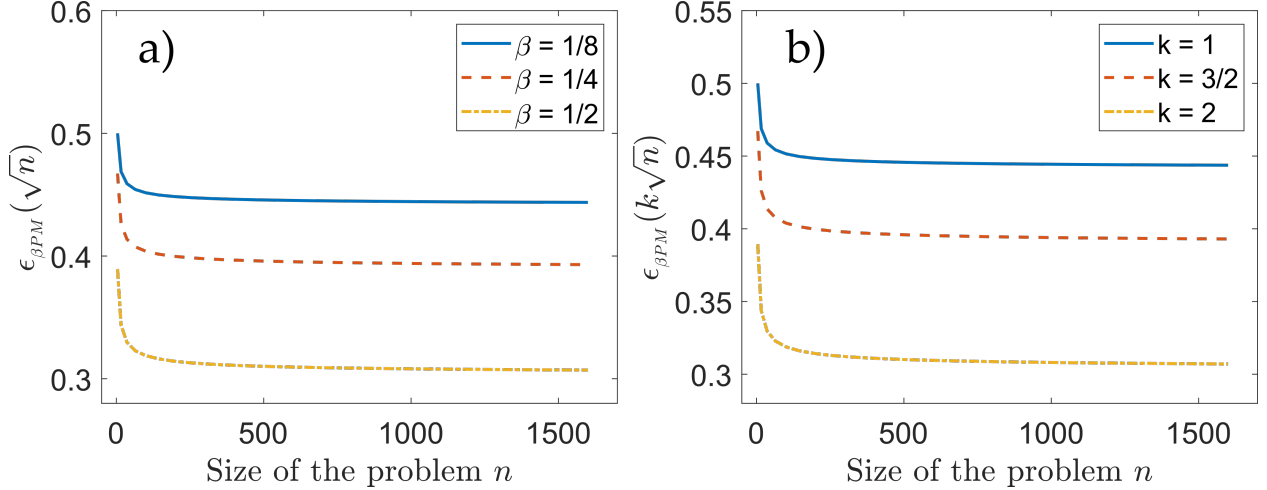
$$\begin{aligned}
&\frac{1}{2} \sum_{k=0}^d P(d_M = k) P(\nexists(i, j) \in \sigma(\mathbf{s}) \text{ s.t. } (i, j) \in M | d_M = k) \\
&\leq \frac{1}{2} \sum_{k=0}^d P(d_M = k) e^{-\frac{k(k-1)}{4\beta n}} \\
&\leq \sum_{k=0}^d \frac{\binom{2\beta n}{k} \binom{n-2\beta n}{d-k}}{2^{\binom{n}{d}}} e^{-\frac{k(k-1)}{4\beta n}}.
\end{aligned}$$

where in the first line we used the fact that  $d_M$  cannot be larger than  $d$ , Eq. (C.10) in the second line and (C.9) in the last line.  $\square$

Now let's say that we want to solve the problem for an error at most  $\epsilon$ , for any  $\epsilon < 1/2$ . Then, by performing the best-known protocol, it is sufficient to send  $d = \mathcal{O}(\sqrt{n})$  bits. To show that we numerically analyze Eq. (5.20) in Figure C.1.

<sup>4</sup>Note that in (C.9) we considered  $\binom{a}{b} = 0$  whenever  $b > a$ .





**Figure C.1:** Error analysis for the best-known protocol for the  $\beta$ PM problem. **a)** Numerical analysis of  $\epsilon_{\beta PM}(\sqrt{n})$  for different values of  $\beta$ . **b)** Impact of different multiplying factors ( $k \in \{1, \frac{3}{2}, 2\}$ ) on error probabilities for  $\beta = \frac{1}{4}$ .

In Figure C.1(a), we observe that  $\epsilon_{\beta PM}(\sqrt{n})$  converges to constant values for various  $\beta$  values, indicating the protocol's stability under varying  $\beta$  settings. Moreover, Figure C.1(b) illustrates the effect of different multiplying factors on error probabilities, taking  $\beta = \frac{1}{4}$  as an example. This demonstrates the ability to achieve the desired error probability  $\epsilon$  by appropriately selecting the factor.

## C.2 Vector in a Subspace problem

### C.2.1 Best known classical protocol

In this section, similar to the previous one where we analyzed the  $\beta$ PM protocol, we provide a comprehensive analysis of the best-known protocol for the VS. Once again, for completeness, we present a restatement of the full VS protocol below.

**Classical protocol  $\pi_{VS}$ .** Let  $z_1, \dots, z_n$  be  $n$  mutually independent random elements in  $\mathbb{R}$ , each chosen according to the normal distribution  $\mathcal{N}(0, n^{-1})$ , that is, each  $z_i$  has the normal distribution with expectation 0 and variance  $n^{-1}$ . The distribution of  $z = (z_1, \dots, z_n)$  in  $\mathbb{R}^n$  is hence multi-normal (we call this distribution  $\psi$ ). Let  $k = 2^d$ , where  $d$  is an integer and let  $z^1, \dots, z^k$  be  $k$  mutually independent random elements of  $\mathbb{R}^n$ , each chosen according to the distribution  $\psi$ . We assume that both players can see  $z^1, \dots, z^k$  (using their pre-shared secret). Let  $z^{\hat{j}}$  be the element in  $\{z^1, \dots, z^k\}$  with the largest scalar product with the input vector  $x \in S^{n-1} \cap H$  (same analysis for  $H^\perp$ ). Alice knows the value of the index  $\hat{j}$  and share that index with Bob, by sending  $d$  bits. Now Bob knows vector  $z^{\hat{j}}$ . He will answer 0 if  $z^{\hat{j}}$  is closer to  $H$  and 1 if  $z^{\hat{j}}$  is closer to  $H^\perp$ .

Next, we proceed to prove Theorem 5.3.3, which we also restate here for convenience.

**Theorem 5.3.3.** *Let  $d$  be an integer. An explicit one-way public-coin protocol  $\pi_{VS}$  exists with a communication cost  $CC(\pi_{VS}) = d$  which solves the  $n$ -dimensional VS problem protocol with an error probability at most*

$$\epsilon_{VS}(d) = \min_{t_1, t_2 > 0} 1 - \left(1 - e^{-\frac{(|T|+T)^2}{8}}\right) \left(1 - 2e^{-\frac{t_2^2}{2}}\right) \left(1 - \frac{1}{t_1^2}\right) \quad (5.24)$$

with  $T \equiv \sqrt{\frac{d}{\pi}} - \sqrt{4\sqrt{n}(t_1 + t_2) + 2\sqrt{2}t_1t_2}$ .

*Proof.* We start with some theorems that we shall use in this proof. First, let's consider the Borel-Tis Inequality [288], a concentration inequality for the maximum of i.i.d. Gaussian random variables.

**Theorem C.2.1** (Borel-Tis Inequality). *Let  $Y = \max_{i=1\dots m} X_i$ , where  $X_i \sim \mathcal{N}(0, \sigma^2)$  are i.i.d. Gaussian random variables. Then*

$$P(y - \mathbb{E}[Y] < -t) \leq e^{-\frac{t^2}{2\sigma^2}}. \quad (C.11)$$

Next, we consider an inequality [289] that provides bounds on its expectation value.

**Theorem C.2.2.** *Let  $Y = \max_{i=1\dots m} X_i$ , where  $X_i \sim \mathcal{N}(0, \sigma^2)$  are i.i.d. Gaussian random variables. Then*

$$\mathbb{E}[Y] \geq \frac{1}{\sqrt{\pi \ln 2}} \sigma \sqrt{\ln m}. \quad (C.12)$$

Finally, we will need a variant of the Levy's Lemma [290], a result which shows that the norm of a projection of a random vector is close to Gaussian.

**Theorem C.2.3** (Levy's Lemma). *Let  $\nu \in S^{n-1}$  be a unit random vector distributed uniformly with  $n > 2$ . Let  $F \subseteq \mathbb{R}^n$  be a subspace of dimension  $l$ . Then for each  $t > 0$*

$$P\left(\left|\|\text{Proj}_F \nu\|_2^2 - \frac{l}{n}\right| \geq \frac{t}{\sqrt{n}}\right) \leq e^{-\frac{t^2}{2}}, \quad (C.13)$$

where  $\|\cdot\|_2$  is the euclidean norm and  $\text{Proj}_F \nu$  is defined as the projection of  $\nu$  onto the subspace  $F$ , formally given by  $\text{Proj}_F \nu := \arg \min_{v \in F} \|\nu - v\|_2$ .

We start our proof by showing how for large  $n$ , with very high probability, any  $z^i$  is very close to a unit vector. The distribution of  $\|z\|_2^2$ , where  $z$  is an  $n$ -dimensional multivariate variable, with each component independently distributed as  $\mathcal{N}(0, n^{-1})$ , is given by  $\|z\|_2^2 \sim \frac{1}{n} \chi^2(n)$ . This indicates that the norm squared of  $z$  follows a chi-squared distribution with  $n$  degrees of freedom, scaled by  $\frac{1}{n}$ . Therefore, Chebyshev's inequality can be used to bound the norm squared of  $z$ : for each  $t_1 > 0$ , the following concentration inequality holds

$$P\left(\left|\|z\|_2^2 - 1\right| < t_1 \sqrt{\frac{2}{n}}\right) \geq 1 - \frac{1}{t_1^2}. \quad (C.14)$$

Moreover, we know that  $\langle z^i | x \rangle \sim \mathcal{N}(0, n^{-1})$ , since it is a projection on a random direction, but all the directions give the same distribution. Let's define  $x^i := \langle z^i | x \rangle$  and

$y := \max\{x^1, \dots, x^m\} = \langle z^{\hat{j}} | x \rangle$ . Now we lower bound the value of the scalar product  $y$  with a combination of Theorem C.2.1 and C.2.2, where in our case  $\sigma = \frac{1}{\sqrt{n}}$ . First one can show that, from Theorem C.2.2.

$$\mathbb{E}[Y] \geq \frac{\sqrt{\ln m}}{\sqrt{n\pi \ln 2}} = \sqrt{\frac{d}{n\pi}}. \quad (\text{C.15})$$

Finally, from Theorem C.2.1 one obtains for each  $t_3 > 0$

$$P\left(y \geq \frac{1}{\sqrt{n}} \left(\sqrt{\frac{d}{\pi}} - t_3\right)\right) \geq 1 - e^{-\frac{t_3^2}{2}}. \quad (\text{C.16})$$

Now we have all the ingredients to evaluate the projection of  $z^{\hat{j}}$  on  $H$  and  $H^\perp$ . We will consider the case  $x \in H$  (the case  $x \in H^\perp$  has the same analysis). One can write  $z^{\hat{j}}$  as  $z^{\hat{j}} = xy + \nu\sqrt{\|z\|_2^2 - y^2}$ , where  $\nu$  is uniformly distributed over the unit sphere in  $x^\perp$  which is a subspace of  $\mathbb{R}^n$  of dimension  $n - 1$ . Since  $\dim[H] = n/2$  and  $H^\perp \in x^\perp$ , we have that for each  $t_2 > 0$

$$P\left(\left|\|\text{Proj}_{H^\perp} \nu\|_2^2 - \frac{1}{2}\right| < \frac{t_2}{\sqrt{n}}\right) \geq 1 - 2e^{-\frac{t_2^2}{2}}, \quad (\text{C.17})$$

where we considered  $n$  to be large enough such as the expected value of the squared norm is  $\frac{n/2}{n-1} \simeq 1/2$ . From eq. (C.14), it can be observed that for each  $t_1 > 0$ , with a probability at least  $1 - \frac{1}{t_1^2}$ , the squared norm of the projection  $\text{Proj}_H z^{\hat{j}}$  is

$$\begin{aligned} \left\|\text{Proj}_H z^{\hat{j}}\right\|_2^2 &= y^2 + (\|z\|_2^2 - y^2) \|\text{Proj}_H \nu\|_2^2 \\ &> y^2 + (1 - \sqrt{\frac{2}{n}}t_1 - y^2)(1 - \|\text{Proj}_{H^\perp} \nu\|_2^2). \end{aligned}$$

Similarly, from Eq. (C.17), we can derive that, with probability at least  $(1 - 2e^{-\frac{t_2^2}{2}})(1 - \frac{1}{t_1^2})$

$$\begin{aligned} \left\|\text{Proj}_H z^{\hat{j}}\right\|_2^2 &> y^2 + (1 - \sqrt{\frac{2}{n}}t_1 - y^2)\left(\frac{1}{2} - \frac{t_2}{\sqrt{n}}\right) \\ &> \frac{1}{2} + y^2 \left(\frac{1}{2} + \frac{t_2}{\sqrt{n}}\right) - \frac{1}{\sqrt{n}} \left(\frac{t_1}{\sqrt{2}} + t_2\right) \\ &> \frac{1}{2} + \frac{y^2}{2} - \frac{1}{\sqrt{n}} \left(\frac{t_1}{\sqrt{2}} + t_2\right). \end{aligned}$$

Finally, from eq. (C.16) it follows that, for  $t_3 \leq \sqrt{\frac{d}{\pi}}$ , with probability at least  $(1 - e^{-\frac{t_3^2}{2}})(1 - 2e^{-\frac{t_2^2}{2}})(1 - \frac{1}{t_1^2})$

$$\left\|\text{Proj}_H z^{\hat{j}}\right\|_2^2 > \frac{1}{2} + \frac{\left(\sqrt{\frac{d}{\pi}} - t_3\right)^2}{2n} - \frac{\frac{t_1}{\sqrt{2}} + t_2}{\sqrt{n}}. \quad (\text{C.18})$$

With the same probability, the projection on  $H^\perp$  is given by

$$\begin{aligned} \left\| \text{Proj}_{H^\perp} z^{\hat{j}} \right\|_2^2 &= (\|z\|_2^2 - y^2) \|\text{Proj}_{H^\perp} \nu\|_2^2 \\ &\leq \|z\|_2^2 \|\text{Proj}_{H^\perp} \nu\|_2^2 \\ &< (1 + \sqrt{\frac{2}{n}} t_1) \left( \frac{1}{2} + \frac{t_2}{\sqrt{n}} \right) \\ &= \frac{1}{2} + \frac{\frac{t_1}{\sqrt{2}} + t_2}{\sqrt{n}} + \frac{\sqrt{2} t_1 t_2}{n}. \end{aligned}$$

Therefore, with an error probability at most  $1 - (1 - e^{-\frac{t_3^2}{2}})(1 - 2e^{-\frac{t_2^2}{2}})(1 - \frac{1}{t_1^2})$ , the following inequalities hold true

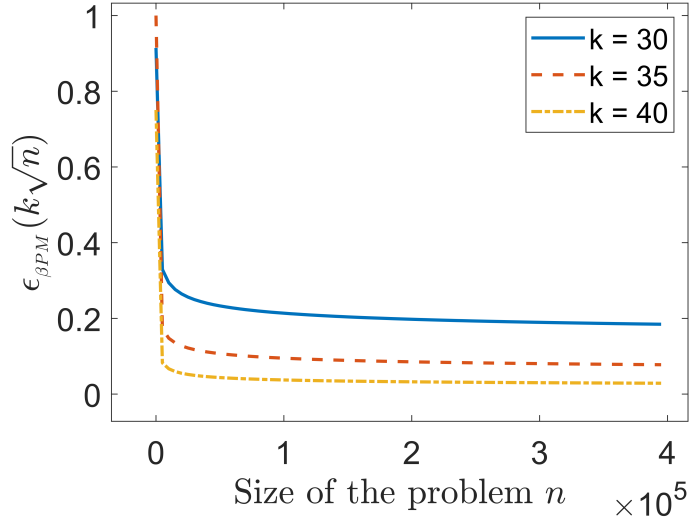
$$\begin{aligned} \left\| \text{Proj}_H z^{\hat{j}} \right\|_2^2 &> \frac{1}{2} + \frac{\left( \sqrt{\frac{d}{\pi}} - t_3 \right)^2}{2n} - \frac{\frac{t_1}{\sqrt{2}} + t_2}{\sqrt{n}} \\ \left\| \text{Proj}_{H^\perp} z^{\hat{j}} \right\|_2^2 &< \frac{1}{2} + \frac{\frac{t_1}{\sqrt{2}} + t_2}{\sqrt{n}} + \frac{\sqrt{2} t_1 t_2}{n}. \end{aligned}$$

The idea now is to select a valid value for  $t_3$  such that either we ensure that  $\left\| \text{Proj}_H z^{\hat{j}} \right\|_2^2 > \left\| \text{Proj}_{H^\perp} z^{\hat{j}} \right\|_2^2$ , thereby guaranteeing Bob's correct answer, or  $t_3 = 0$ , forcing the error probability to be at most 1. Therefore, we select  $t_3 = \frac{|T|+T}{2}$ , with  $T := \sqrt{\frac{d}{\pi}} - \sqrt{4\sqrt{n}(t_1 + t_2) + 2\sqrt{2}t_1 t_2}$ <sup>5</sup>, obtaining an error probability at most  $1 - (1 - e^{-\frac{(|T|+T)^2}{8}})(1 - 2e^{-\frac{t_2^2}{2}})(1 - \frac{1}{t_1^2})$  for any  $t_1, t_2 > 0$ . Now one can minimize the error probability with respect to  $t_1$  and  $t_2$  to conclude the proof.  $\square$

Just like in the  $\beta$ PM problem, we can solve this problem by transmitting  $d = \mathcal{O}(\sqrt{n})$  bits. In particular, in Figure C.2 we illustrate how to reach a desired error probability by appropriately selecting the multiplying factor.

---

<sup>5</sup>One can notice that  $t_3 \leq \sqrt{\frac{d}{\pi}}$  holds for any  $t_1, t_2 > 0$ .



**Figure C.2:** Error analysis of the best-known protocol for the VS problem. We analyze the impact of different multiplying factors ( $k \in \{30, 35, 40\}$ ) on error probabilities.

### C.3 General practical quantum protocol

In this section, we analyze a general quantum protocol for the  $\beta$ PM problem and the VS problem for a realistic noise model. We consider a case where Alice sends  $m$  copies of the quantum state in Eq. (5.17) for the  $\beta$ PM protocol and (5.23) for the VS. Let us call  $a \in \{0, 1\}$  the right answer. Bob then performs the measurement from the corresponding ideal protocol and outputs

- $b = \perp$  and aborts the protocol with probability  $p_{\text{abort}}$
- else,  $b = a$  with probability  $(1 - p_{\text{abort}})(1 - \text{QBER})$  or  $b \neq a$  with probability  $(1 - p_{\text{abort}}) \cdot \text{QBER}$ , where QBER is the quantum bit error rate, i.e. the error rate of a conclusive round.

Given a dimension  $n$  and a number of copies  $m$ , the physical implementation of the protocol determines the QBER and abort probability  $p_{\text{abort}}$ . In the following we will analyze these quantities for a physical implementation based on photonics.

#### C.3.1 QBER and $p_{\text{abort}}$ derivation

Consider a lossy channel, with  $T$  the transmittance of the channel, defined as  $T = 10^{-0.02L}$ , where  $L$  is the length of the quantum channel expressed in kilometers. Let  $\eta_{\text{det}}$  be the detector efficiency and  $P_{\text{dark}}$  the dark-count probability per detector. We will assume that the error rate is dominated by dark counts and that clicks due to signals and due to dark counts are independent. As described in Section 5.3, Bob can perform the measurement associated to his input with only two detectors. In this analysis we will not consider photon

counting detectors. Moreover, we shall consider the case where each copy of the quantum state is encoded in a photon with  $n$  optical modes. Now let us consider the probability of a photon sent by Alice being detected: it will be transmitted with probability  $T$  due to loss in the transmission channel; once it has successfully reached Bob's measurement apparatus, in the  $\beta$ PM case there is an extra probability  $1 - 2\beta$  of addressing one of the modes not described by the partial matching; finally, once it is rerouted to one of the two detectors, it will be detected only with probability  $\eta_{det}$ . Combining all these steps, the final probability for a photon to be detected is  $2\beta\eta_{det}T$  for the  $\beta$ PM protocol and  $\eta_{det}T$  for the VS protocol. Since each photon is independent, the probability that there is at least one click due to the signal is

$$P_s = 1 - \text{Bin}(0, m, \tilde{T}) = 1 - (1 - \tilde{T})^m,$$

with  $\tilde{T} := 2\beta\eta_{det}T$  for the  $\beta$ PM protocol and  $\tilde{T} := \eta_{det}T$  for the VS protocol. We called  $\text{Bin}(k, n, p) := \binom{n}{k}p^k(1-p)^{n-k}$  the Binomial distribution, where  $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ . Moreover, the probability of getting zero clicks is the probability of having at the same time no clicks from dark counts and no clicks due to the actual signal, i.e.

$$\begin{aligned} \text{Pr}(0 \text{ clicks}) &= \text{Pr}(\text{no dark counts}) \cdot \text{Pr}(0 \text{ clicks due to signal}) \\ &= (1 - 2P_{dark} + P_{dark}^2)(1 - P_s). \end{aligned}$$

On the other hand, the probability of getting a click in both detectors at the same time is

$$\begin{aligned} \text{Pr}(\text{both detectors click}) &= \text{Pr}(2 \text{ dark counts}) + \text{Pr}(\text{dark count in wrong detector})P_s \\ &= P_{dark}^2 + P_{dark}(1 - P_{dark})P_s. \end{aligned}$$

We now assume that Bob aborts the protocol every time he has 0 clicks or clicks in both detectors, i.e.

$$\begin{aligned} p_{\text{abort}} &= (1 - 2P_{dark} + P_{dark}^2)(1 - P_s) - (P_{dark}^2 + P_{dark}(1 - P_{dark})P_s) \\ &= P_{dark} - (1 - 3P_{dark} + 2P_{dark}^2)(1 - \tilde{T})^m. \end{aligned} \quad (\text{C.19})$$

Now we have that the QBER is the probability of giving a wrong answer after the sifting, i.e.

$$\text{QBER} = \frac{\text{Pr}(b \neq a \wedge b \neq \perp)}{1 - p_{\text{abort}}}, \quad (\text{C.20})$$

with  $\text{Prob}(b \neq a \wedge b \neq \perp) = P_{dark}(1 - P_{dark})(1 - P_s)$ , obtaining eventually by direct calculation

$$\text{QBER} = \frac{P_{dark} - P_{dark}^2}{1 - P_{dark} - (1 - 3P_{dark} + 2P_{dark}^2)(1 - \tilde{T})^m} (1 - \tilde{T})^m. \quad (\text{C.21})$$

Finally, we have evaluated the  $p_{\text{abort}}$ <sup>6</sup> and QBER as a function of the number of copies sent  $m$ .

---

<sup>6</sup>One can notice that even in the case where Alice is sending a large number of copies  $p_{\text{abort}}$  converges to  $P_{dark}$  instead of simply 0. This is due to the fact that we haven't considered an implementation with photon counting detectors.



# METHODS FOR RECONFIGURABLE OPTICAL LINEAR OPERATOR

## Contents

---

|            |   |            |
|------------|---|------------|
| <b>D.1</b> | <b>Input ports calibrations . . . . .</b> | <b>158</b> |
| D.1.1      | Active zone of the SLM . . . . .          | 158        |
| D.1.2      | Dividing the SLM in slices . . . . .      | 158        |

---



## D.1 Input ports calibrations

Before being able to characterize the TMs of each input port, we need to define how to subdivide our optical system into distinct input ports. While a division in square grids has already been proposed in [264], we decide to preserve the radial symmetry of the Gaussian input source by dividing the SLM into different pizza-shaped slices<sup>1</sup>, which allows to more easily equalize intensities. However, we need first to characterize the Gaussian beam coming from the superluminescent diode and how it couples to the MMF. To do this, we conduct a detailed scan of the SLM, mapping out how light from each pixel of the SLM impings the MMF.

### D.1.1 Active zone of the SLM

Our approach begins with displaying a phase ramp on the SLM and collecting the resultant speckle pattern. The key observation comes from noticing changes in the speckle pattern only when we vary the phase value of pixels that reflect light inside the MMF. Therefore, as illustrated in Figure D.1, by adding a phase shift of  $\pi$  to each macro pixel (each sized  $4 \times 4$ ) and analyzing the correlation  $C(X, Y)$  between the original speckle image (without any additional phase shift) and the modified image (with the phase shift at macro pixel  $(x, y)$ ) we can effectively reconstruct the Gaussian beam's profile. In particular, this technique allows us to accurately find the position of the beam's center, which is crucial to divide the SLM into well-balanced slices.

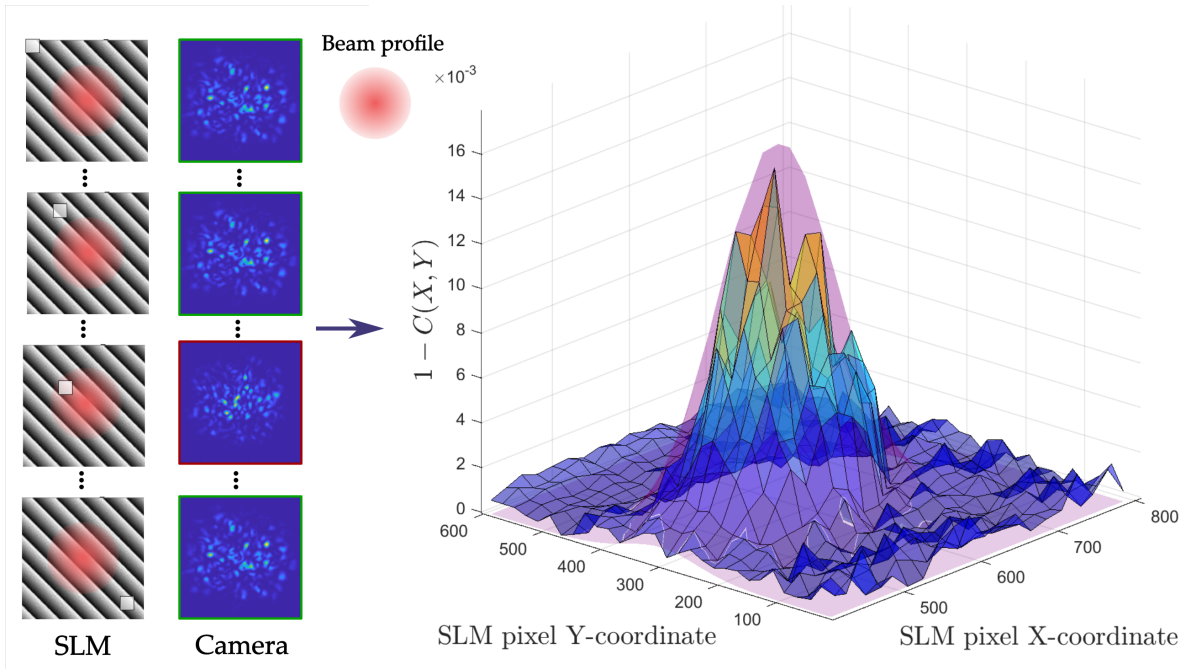
### D.1.2 Dividing the SLM in slices

Once we have characterized the active zone of the SLM, we can then divide it into  $m$  different slice-shaped ports, where our goal is to make sure that each port is controlling the same amount of light. In particular, this is crucial when we want to simulate a quantum state coming from Alice, such as the one for the  $\beta$ PM protocol in Eq. (5.17), which is a balanced superposition where the classical information is encoded in the phase.

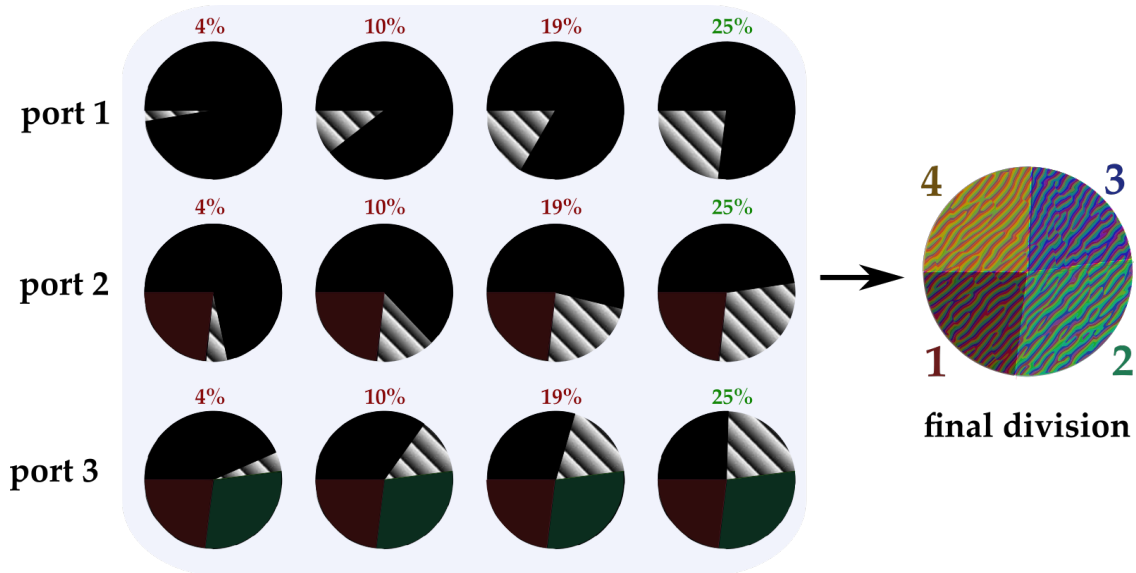
Our technique for dividing SLM into  $m$  well-balanced ports, illustrated in Figure D.2, works as follows. Initially, we display a uniform phase ramp across the entire SLM and record the total light intensity,  $I^{tot}$ . Next, we set the SLM to a completely black state (phase 0 across all areas), ensuring no light reaches the MMF as it aligns with the first diffraction order. We then apply the phase ramp to a specific slice of the SLM, defined by a starting angle  $\alpha_1^{in} = 0$  and a variable ending angle  $\alpha_1^{out}$ , initially set to 0. This angle is gradually increased until the light intensity collected from this section,  $I_1^{tot}$ , reaches  $I^{tot}/m$ . Subsequent ports are scanned in the same way starting from the ending angle of the previous port  $\alpha_p^{in} = \alpha_{p-1}^{out}$ . The final port  $m$  is uniquely defined by the start angle  $\alpha_m^{in} = \alpha_{m-1}^{out}$  and ends at  $\alpha_m^{out} = 2\pi$ , completing the circle.

---

<sup>1</sup>Despite the Ph.D. candidate being Italian, sadly the idea came from the French supervisor...



**Figure D.1:** Analysis of the active zone of the SLM. The reconstruction of the Gaussian beam's profile is achieved by applying a  $\pi$  phase shift to each macro pixel, identified by coordinates  $(x, y)$ , and examining the correlation  $C(X, Y)$  between the original and modified speckle images.



**Figure D.2:** Illustration of the division of the SLM into  $m = 4$  different ports. Due to the fact that the SLM active profile is not perfectly Gaussian, the angles of the four ports are not precisely  $90^\circ$  each.



---

# BIBLIOGRAPHY

- [1] Charles H. Bennett and Gilles Brassard. “Quantum cryptography: Public key distribution and coin tossing”. *Theoretical Computer Science* **560**, 7–11 (1984). (Cited on page [v](#), [1](#), [4](#), and [36](#)).
- [2] Dominique Unruh. “Everlasting Multi-party Computation”. In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013*. Pages 380–397. *Lecture Notes in Computer Science* Berlin, Heidelberg (2013). Springer. (Cited on page [vi](#), [4](#), [8](#), and [103](#)).
- [3] Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald de Wolf. “Exponential separations for one-way quantum communication complexity, with applications to cryptography”. In *Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing*. Pages 516–525. STOC ’07 New York, NY, USA (2007). Association for Computing Machinery. (Cited on page [vi](#), [7](#), [74](#), [75](#), [77](#), [98](#), and [147](#)).
- [4] Stefan Rotter and Sylvain Gigan. “Light fields in complex media: Mesoscopic scattering meets wave control”. *Reviews of Modern Physics* **89**, 015005 (2017). [arxiv:1702.05395](#). (Cited on page [vii](#), [9](#), [111](#), and [116](#)).
- [5] Sylvain Gigan, Ori Katz, Hilton B. de Aguiar, Esben Ravn Andresen, Alexandre Aubry, Jacopo Bertolotti, Emmanuel Bossy, Dorian Bouchet, Joshua Brake, Sophie Brasselet, Yaron Bromberg, Hui Cao, Thomas Chaigne, Zhongtao Cheng, Wonshik Choi, Tomáš Čížmár, Meng Cui, Vincent R. Curtis, Hugo Defienne, Matthias Hofer, Ryoichi Horisaki, Roarke Horstmeyer, Na Ji, Aaron K. LaViolette, Jerome Mertz, Christophe Moser, Allard P. Mosk, Nicolas C. Pégard, Rafael Piestun, Sebastien Popoff, David B. Phillips, Demetri Psaltis, Babak Rahmani, Hervé Rigneault, Stefan Rotter, Lei Tian, Ivo M. Vellekoop, Laura Waller, Lihong Wang, Timothy Weber, Sheng Xiao, Chris Xu, Alexey Yamilov, Changhui Yang, and Hasan Yilmaz. “Roadmap on wavefront shaping and deep imaging in complex media”. *Journal of Physics: Photonics* **4**, 042501 (2022). (Cited on page [vii](#) and [9](#)).
- [6] Gilles Brassard. “Brief History of Quantum Cryptography: A Personal Perspective”. In *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005*. Pages 19–23. (2005). (Cited on page [1](#)).

- [7] MIT Endicott House. “The Physics of Computation Conference”. (1981). url: <https://mitendicottthouse.org/physics-computation-conference/>. (Cited on page 1).
- [8] Peter W. Shor. “Algorithms for quantum computation: Discrete logarithms and factoring”. In Proceedings 35th Annual Symposium on Foundations of Computer Science. Pages 124–134. (1994). (Cited on page 1).
- [9] Whitfield Diffie and Martin Hellman. “New directions in cryptography”. *IEEE Transactions on Information Theory* **22**, 644–654 (1976). (Cited on page 2 and 31).
- [10] Ron Rivest, Adi Shamir, and Leonard Adleman. “A method for obtaining digital signatures and public-key cryptosystems”. *Communications of the ACM* **21**, 120–126 (1978). (Cited on page 2).
- [11] Colin D. Bruzewicz, John Chiaverini, Robert McConnell, and Jeremy M. Sage. “Trapped-ion quantum computing: Progress and challenges”. *Applied Physics Reviews* **6**, 021314 (2019). (Cited on page 2).
- [12] Nathalie P. de Leon, Kohei M. Itoh, Dohun Kim, Karan K. Mehta, Tracy E. Northup, Hanhee Paik, B. S. Palmer, N. Samarth, Sorawis Sangtawesin, and D. W. Steuerman. “Materials challenges and opportunities for quantum computing hardware”. *Science* **372**, eabb2823 (2021). (Cited on page 2).
- [13] Sergey Bravyi, Oliver Dial, Jay M. Gambetta, Darío Gil, and Zaira Nazario. “The future of quantum computing with superconducting qubits”. *Journal of Applied Physics* **132**, 160902 (2022). (Cited on page 2).
- [14] Sukhpal Singh Gill, Adarsh Kumar, Harvinder Singh, Manmeet Singh, Kamalpreet Kaur, Muhammad Usman, and Rajkumar Buyya. “Quantum computing: A taxonomy, systematic review and future directions”. *Software: Practice and Experience* **52**, 66–114 (2022). (Cited on page 2).
- [15] Michele Mosca. “Cybersecurity in an Era with Quantum Computers: Will We Be Ready?”. *IEEE Security & Privacy* **16**, 38–41 (2018). (Cited on page 2).
- [16] Daniel J. Bernstein and Tanja Lange. “Post-quantum cryptography”. *Nature* **549**, 188–194 (2017). (Cited on page 2).
- [17] Renato Renner. “Security of quantum key distribution”. *International Journal of Quantum Information* **06**, 1–127 (2008). (Cited on page 2, 4, 42, 51, and 88).
- [18] Marco Tomamichel and Anthony Leverrier. “A largely self-contained and complete security proof for quantum key distribution”. *Quantum* **1**, 14 (2017). (Cited on page 2).
- [19] Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. “Secure quantum key distribution with realistic devices”. *Reviews of Modern Physics* **92**, 025002 (2020). (Cited on page 2).

- [20] Christopher Portmann and Renato Renner. “Security in quantum cryptography”. *Reviews of Modern Physics* **94**, 025008 (2022). (Cited on page 2).
- [21] “VeriQloud – Unlocking Quantum Cybersecurity”. url: <https://veriqloud.com/>. (Cited on page 2).
- [22] “Toshiba Quantum Technology - Quantum-Safe Security Solutions”. url: <https://www.toshiba.eu/quantum/>. (Cited on page 2).
- [23] “ThinkQuantum”. url: <https://www.thinkquantum.com/>. (Cited on page 2).
- [24] “Quantum Cryptography Solutions - LuxQuanta”. url: <https://www.luxquanta.com/solutions>. (Cited on page 2).
- [25] “MAN QKD Products\_QuantumCTek– Quantum Secures Every Bit”. url: <http://www.quantum-info.com/English/product/>. (Cited on page 2).
- [26] “KETS Quantum”. url: <https://kets-quantum.com/>. (Cited on page 2).
- [27] “ID Quantique - The home of Quantum-Safe Crypto”. url: <https://www.idquantique.com/>. (Cited on page 2).
- [28] “Home | Quantum Cybersecurity from QuintessenceLabs”. url: <https://www.quintessencelabs.com>. (Cited on page 2).
- [29] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, S. Fasel, S. Fossier, M. Fürst, J.-D. Gautier, O. Gay, N. Gisin, P. Grangier, A. Happe, Y. Hasani, M. Hentschel, H. Hübel, G. Humer, T. Länger, M. Legré, R. Lieger, J. Lodewyck, T. Lorünser, N. Lütkenhaus, A. Marhold, T. Matyus, O. Maurhart, L. Monat, S. Nauerth, J.-B. Page, A. Poppe, E. Querasser, G. Ribordy, S. Robyr, L. Salvail, A. W. Sharpe, A. J. Shields, D. Stucki, M. Suda, C. Tamas, T. Themel, R. T. Thew, Y. Thoma, A. Treiber, P. Trinkler, R. Tualle-Brouri, F. Vannel, N. Walenta, H. Weier, H. Weinfurter, I. Wimberger, Z. L. Yuan, H. Zbinden, and A. Zeilinger. “The SECOQC quantum key distribution network in Vienna”. *New Journal of Physics* **11**, 075001 (2009). (Cited on page 2).
- [30] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, K. Yoshino, Y. Nambu, S. Takahashi, A. Tajima, A. Tomita, T. Domeki, T. Hasegawa, Y. Sakai, H. Kobayashi, T. Asai, K. Shimizu, T. Tokura, T. Tsurumar, M. Matsui, T. Honjo, K. Tamaki, H. Takesue, Y. Tokura, J. F. Dynes, A. R. Dixon, A. W. Sharpe, Z. L. Yuan, A. J. Shields, S. Uchikoga, M. Legré, S. Robyr, P. Trinkler, L. Monat, J.-B. Page, G. Ribordy, A. Poppe, A. Allacher, O. Maurhart, T. Länger, M. Peev, and A. Zeilinger. “Field test of quantum key distribution in the Tokyo QKD Network”. *Optics Express* **19**, 10387–10409 (2011). (Cited on page 2).
- [31] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, L. Monat, J.-B. Page, D. Perroud, G. Ribordy, A. Rochas,

- S. Robyr, J. Tavares, R. Thew, P. Trinkler, S. Ventura, R. Voirol, N. Walenta, and H. Zbinden. “Long-term performance of the SwissQuantum quantum key distribution network in a field environment”. *New Journal of Physics* **13**, 123001 (2011). (Cited on page 2).
- [32] Yu-Ao Chen, Qiang Zhang, Teng-Yun Chen, Wen-Qi Cai, Sheng-Kai Liao, Jun Zhang, Kai Chen, Juan Yin, Ji-Gang Ren, Zhu Chen, Sheng-Long Han, Qing Yu, Ken Liang, Fei Zhou, Xiao Yuan, Mei-Sheng Zhao, Tian-Yin Wang, Xiao Jiang, Liang Zhang, Wei-Yue Liu, Yang Li, Qi Shen, Yuan Cao, Chao-Yang Lu, Rong Shu, Jian-Yu Wang, Li Li, Nai-Le Liu, Feihu Xu, Xiang-Bin Wang, Cheng-Zhi Peng, and Jian-Wei Pan. “An integrated space-to-ground quantum communication network over 4,600 kilometres”. *Nature* **589**, 214–219 (2021). (Cited on page 2 and 50).
- [33] Teng-Yun Chen, Xiao Jiang, Shi-Biao Tang, Lei Zhou, Xiao Yuan, Hongyi Zhou, Jian Wang, Yang Liu, Luo-Kan Chen, Wei-Yue Liu, Hong-Fei Zhang, Ke Cui, Hao Liang, Xiao-Gang Li, Yingqiu Mao, Liu-Jun Wang, Si-Bo Feng, Qing Chen, Qiang Zhang, Li Li, Nai-Le Liu, Cheng-Zhi Peng, Xiongfeng Ma, Yong Zhao, and Jian-Wei Pan. “Implementation of a 46-node quantum metropolitan area network”. *npj Quantum Information* **7**, 1–6 (2021). (Cited on page 2).
- [34] P. Sibson, C. Erven, M. Godfrey, S. Miki, T. Yamashita, M. Fujiwara, M. Sasaki, H. Terai, M. G. Tanner, C. M. Natarajan, R. H. Hadfield, J. L. O’Brien, and M. G. Thompson. “Chip-based quantum key distribution”. *Nature Communications* **8**, 13984 (2017). (Cited on page 2).
- [35] Qiang Liu, Yinming Huang, Yongqiang Du, Zhengeng Zhao, Minming Geng, Zhenrong Zhang, and Kejin Wei. “Advances in Chip-Based Quantum Key Distribution”. *Entropy* **24**, 1334 (2022). (Cited on page 2).
- [36] Raphael Overbeck and Nicolas Sendrier. “Code-based cryptography”. In Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen, editors, *Post-Quantum Cryptography*. Pages 95–145. Springer, Berlin, Heidelberg (2009). (Cited on page 2).
- [37] Daniele Micciancio and Oded Regev. “Lattice-based Cryptography”. In Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen, editors, *Post-Quantum Cryptography*. Pages 147–191. Springer, Berlin, Heidelberg (2009). (Cited on page 2).
- [38] Jintai Ding and Bo-Yin Yang. “Multivariate Public Key Cryptography”. In Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen, editors, *Post-Quantum Cryptography*. Pages 193–241. Springer, Berlin, Heidelberg (2009). (Cited on page 2).
- [39] Johannes Buchmann, Erik Dahmen, and Michael Szydlo. “Hash-based Digital Signature Schemes”. In Daniel J. Bernstein, Johannes Buchmann, and Erik Dahmen, editors, *Post-Quantum Cryptography*. Pages 35–93. Springer, Berlin, Heidelberg (2009). (Cited on page 2).
- [40] “The Seventh International Conference on Post-Quantum Cryptography”. (2016). url: <https://pqcrypto2016.jp/>. (Cited on page 2).

- [41] Dan Goodin. “Post-quantum encryption contender is taken out by single-core PC and 1 hour”. (2022). url: <https://arstechnica.com/information-technology/2022/08/sike-once-a-post-quantum-encryption-contender-is-koed-in-nist-smackdown/>. (Cited on page 2).
- [42] Ward Beullens. “Breaking Rainbow Takes a Weekend on a Laptop”. In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology – CRYPTO 2022*. Pages 464–479. Cham (2022). Springer Nature Switzerland. (Cited on page 2).
- [43] Nina Bindel, Jacqueline Brendel, Marc Fischlin, Brian Goncalves, and Douglas Stebila. “Hybrid Key Encapsulation Mechanisms and Authenticated Key Exchange”. In Jintai Ding and Rainer Steinwandt, editors, *Post-Quantum Cryptography*. Pages 206–226. Cham (2019). Springer International Publishing. (Cited on page 2).
- [44] Eric Crockett, Christian Paquin, and Douglas Stebila. “Prototyping post-quantum and hybrid key exchange and authentication in TLS and SSH”. In NIST 2nd PQC Standardization Conference. Santa Barbara, California (2019). url: <https://eprint.iacr.org/2019/858>. (Cited on page 2).
- [45] David Ott, Christopher Peikert, and other workshop participants. “Identifying Research Challenges in Post Quantum Cryptography Migration and Cryptographic Agility”. Workshop report. Computing Community Consortium Washington D.C. (2019). [arxiv:1909.07353](https://arxiv.org/abs/1909.07353). (Cited on page 2).
- [46] David Joseph, Rafael Misoczki, Marc Manzano, Joe Tricot, Fernando Dominguez Pinuaga, Olivier Lacombe, Stefan Leichenauer, Jack Hidary, Phil Venables, and Royal Hansen. “Transitioning organizations to post-quantum cryptography”. *Nature* **605**, 237–243 (2022). (Cited on page 2).
- [47] “National Cyber Security Center (NCSC). Quantum security technologies”. (2020). url: <https://www.ncsc.gov.uk/whitepaper/quantum-security-technologies>. (Cited on page 3 and 133).
- [48] “National Security Agency (NSA). Quantum Key Distribution and Quantum Cryptography”. (2020). url: <https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/>. (Cited on page 3 and 133).
- [49] “ANSSI views on the Post-Quantum Cryptography transition”. (2022). url: <https://www.ssi.gov.fr/publication/anssi-views-on-the-post-quantum-cryptography-transition/>. (Cited on page 3).
- [50] Renato Renner and Ramona Wolf. “The debate over QKD: A rebuttal to the NSA’s objections” (2023). [arxiv:2307.15116](https://arxiv.org/abs/2307.15116). (Cited on page 3).
- [51] “Community Response to the NCSC 2020 Quantum Security Technologies White Paper”. (2020). url: <https://www.quantumcommshub.net/news/>



[community-response-to-the-ncsc-2020-quantum-security-technologies-white-paper/](#). (Cited on page 3).

- [52] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. “Decoy State Quantum Key Distribution”. *Physical Review Letters* **94**, 230504 (2005). (Cited on page 3, 44, and 104).
- [53] Samuel L. Braunstein and Stefano Pirandola. “Side-Channel-Free Quantum Key Distribution”. *Physical Review Letters* **108**, 130502 (2012). (Cited on page 3).
- [54] Vicente Martin, Jesus Martinez-Mateo, and Momtchil Peev. “Introduction to Quantum Key Distribution”. In *Wiley Encyclopedia of Electrical and Electronics Engineering*. Pages 1–17. John Wiley & Sons, Ltd (2017). (Cited on page 3).
- [55] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. “Quantum cryptography”. *Reviews of Modern Physics* **74**, 145–195 (2002). (Cited on page 3).
- [56] Valerio Scarani and Christian Kurtsiefer. “The black paper of quantum cryptography: Real implementation problems”. *Theoretical Computer Science* **560**, 27–32 (2014). (Cited on page 3).
- [57] “Common Methodology for Information Technology Security Evaluation” (2017). (Cited on page 3, 52, and 53).
- [58] Marco Lucamarini, Andrew Shields, Romain Alléaume, and Zhiliang Yuan. “Implementation Security of Quantum Cryptography - Introduction, challenges, solutions”. *ETSI White Paper No. 27* (2018). (Cited on page 3, 44, and 50).
- [59] Shihan Sajeed, Poompong Chaiwongkhot, Anqi Huang, Hao Qin, Vladimir Egorov, Anton Kozubov, Andrei Gaidash, Vladimir Chistiakov, Artur Vasiliev, Artur Gleim, and Vadim Makarov. “An approach for security evaluation and certification of a complete quantum communication system”. *Scientific Reports* **11**, 5110 (2021). (Cited on page 3).
- [60] Norbert Lutkenhaus and Patrick Guillemin. “Quantum Key Distribution (QKD); Common Criteria Protection Profile - Pair of Prepare and Measure Quantum Key Distribution Modules Protection Profile”. Technical Report DGS/QKD-016-PP. ETSI (2023). url: [https://portal.etsi.org/webapp/WorkProgram/Report\\_WorkItem.asp?WKI\\_ID=58004](https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=58004). (Cited on page 3 and 51).
- [61] Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, Information security, cybersecurity and privacy protection. “Information security — Security requirements, test and evaluation methods for quantum key distribution — Part 1: Requirements”. Technical Report ISO/IEC PRF 23837-1. ISO/IEC (2023). url: <https://www.iso.org/standard/77097.html>. (Cited on page 3 and 51).

- [62] Joint Technical Committee ISO/IEC JTC 1, Information technology, Subcommittee SC 27, Information security, cybersecurity and privacy protection. “Information security — Security requirements, test and evaluation methods for quantum key distribution — Part 2: Evaluation and testing methods”. Technical Report ISO/IEC PRF 23837-2. ISO/IEC (2023). url: <https://www.iso.org/standard/77309.html>. (Cited on page 3 and 51).
- [63] Juan Miguel Arrazola and Norbert Lütkenhaus. “Quantum communication with coherent states and linear optics”. *Physical Review A* **90**, 042335 (2014). (Cited on page 4, 22, 23, 121, and 127).
- [64] Frédéric Grosshans and Philippe Grangier. “Continuous Variable Quantum Cryptography Using Coherent States”. *Physical Review Letters* **88**, 057902 (2002). (Cited on page 4 and 37).
- [65] Igor Devetak and Andreas Winter. “Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum states. Proc. R. Soc. Lond. A 461, 207-235”. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* **461** (2003). (Cited on page 5, 42, and 100).
- [66] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. “Hacking commercial quantum cryptography systems by tailored bright illumination”. *Nature Photonics* **4**, 686–689 (2010). (Cited on page 5, 45, and 51).
- [67] Hao Qin, Rupesh Kumar, and Romain Alléaume. “Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution”. *Physical Review A* **94**, 012325 (2016). (Cited on page 5, 54, and 140).
- [68] Rupesh Kumar, Francesco Mazzoncini, Hao Qin, and Romain Alléaume. “Experimental vulnerability analysis of QKD based on attack ratings”. *Scientific Reports* **11**, 9564 (2021). (Cited on page 5).
- [69] Hao Qin, Rupesh Kumar, Vadim Makarov, and Romain Alléaume. “Homodyne-detector-blinding attack in continuous-variable quantum key distribution”. *Physical Review A* **98**, 012312 (2018). (Cited on page 5, 54, and 57).
- [70] Andrew Chi-Chin Yao. “Probabilistic computations: Toward a unified measure of complexity”. In 18th Annual Symposium on Foundations of Computer Science (Sfcs 1977). Pages 222–227. (1977). (Cited on page 6, 66, 69, and 74).
- [71] Francesco Mazzoncini, Balthazar Bauer, Peter Brown, and Romain Alléaume. “Hybrid Quantum Cryptography from Communication Complexity” (2023). [arxiv:2311.09164](https://arxiv.org/abs/2311.09164). (Cited on page 6).
- [72] Mark Braverman and Anup Rao. “Information Equals Amortized Communication” (2011). [arxiv:1106.3595](https://arxiv.org/abs/1106.3595). (Cited on page 6, 72, and 73).

- [73] Oded Regev and Bo’az Klartag. “Quantum one-way communication can be exponentially stronger than classical communication”. In Proceedings of the Annual ACM Symposium on Theory of Computing. Pages 31–40. (2011). (Cited on page 7, 74, and 78).
- [74] Cosmo Lupo and Seth Lloyd. “Quantum-Locked Key Distribution at Nearly the Classical Capacity Rate”. *Physical Review Letters* **113**, 160502 (2014). (Cited on page 7, 84, 85, and 95).
- [75] Ivan B. Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. “Cryptography in the Bounded-Quantum-Storage Model”. *SIAM Journal on Computing* **37**, 1865–1890 (2008). (Cited on page 7, 88, and 95).
- [76] Robert Koenig, Stephanie Wehner, and Juerg Wullschleger. “Unconditional security from noisy quantum storage”. *IEEE Transactions on Information Theory* **58**, 1962–1984 (2012). [arxiv:0906.1030](https://arxiv.org/abs/0906.1030). (Cited on page 7, 89, and 95).
- [77] Frédéric Dupuis, Omar Fawzi, and Stephanie Wehner. “Entanglement Sampling and Applications”. *IEEE Transactions on Information Theory* **61**, 1093–1112 (2015). (Cited on page 7, 90, and 95).
- [78] Nilesh Vyas and Romain Alléaume. “Everlasting Secure Key Agreement with performance beyond QKD in a Quantum Computational Hybrid security model” (2020). [arxiv:2004.10173](https://arxiv.org/abs/2004.10173). (Cited on page 7, 35, 81, 90, 95, and 107).
- [79] John Watrous. “The Theory of Quantum Information”. Cambridge University Press. (2018). 1 edition. (Cited on page 7, 20, and 91).
- [80] Ziv Bar-Yossef, T.s Jayram, and Iordanis Kerenidis. “Exponential separation of quantum and classical one-way communication complexity”. In Electronic Colloquium on Computational Complexity (ECCC). Pages 128–137. (2004). (Cited on page 8).
- [81] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. “Fundamental limits of repeaterless quantum communications”. *Nature Communications* **8**, 15043 (2017). (Cited on page 8, 43, 98, and 104).
- [82] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. “Measurement-device-independent quantum key distribution”. *Physical Review Letters* **108**, 130503 (2012). [arxiv:1109.1473](https://arxiv.org/abs/1109.1473). (Cited on page 9 and 34).
- [83] Saroch Leedumrongwatthanakun, Luca Innocenti, Hugo Defienne, Thomas Juffmann, Alessandro Ferraro, Mauro Paternostro, and Sylvain Gigan. “Programmable linear quantum networks with a multimode fibre”. *Nature Photonics* **14**, 139–142 (2020). (Cited on page 9, 110, 119, 120, and 125).
- [84] Adrian Makowski, Michał Dąbrowski, Ivan Michel Antolovic, Claudio Bruschini, Hugo Defienne, Edoardo Charbon, Radek Lapkiewicz, and Sylvain Gigan. “Large Reconfigurable Quantum Circuits with SPAD Arrays and Multimode Fibers” (2023). [arxiv:2305.16206](https://arxiv.org/abs/2305.16206). (Cited on page 9, 110, 119, and 120).

- [85] Ravikanth Pappu, Ben Recht, Jason Taylor, and Neil Gershenfeld. “Physical One-Way Functions”. *Science* **297**, 2026–2030 (2002). (Cited on page 9 and 117).
- [86] Sebastianus A. Goorden, Marcel Horstmann, Allard P. Mosk, Boris Škorić, and Pepijn W. H. Pinkse. “Quantum-secure authentication of a physical unclonable key”. *Optica* **1**, 421–424 (2014). (Cited on page 9, 117, and 135).
- [87] Qi-Hang Lu, Fang-Xiang Wang, Kun Huang, Xin Wu, Shuang Wang, De-Yong He, Zhen-Qiang Yin, Guang-Can Guo, Wei Chen, and Zheng-Fu Han. “Quantum key distribution over scattering channel”. *Physical Review Applied* **17**, 034045 (2022). [arxiv:2109.12282](https://arxiv.org/abs/2109.12282). (Cited on page 9 and 117).
- [88] Yiyu Zhou, Boris Braverman, Alexander Fyffe, Runzhou Zhang, Jiapeng Zhao, Alan E. Willner, Zhimin Shi, and Robert W. Boyd. “High-fidelity spatial mode transmission through a 1-km-long multimode fiber via vectorial time reversal”. *Nature Communications* **12**, 1866 (2021). (Cited on page 9, 110, 117, and 118).
- [89] Lyubov V. Amitonova, Tristan B. H. Tentrup, Ivo M. Vellekoop, and Pepijn W. H. Pinkse. “Quantum key establishment via a multimode fiber”. *Optics Express* **28**, 5965–5981 (2020). (Cited on page 9, 118, and 119).
- [90] A. Cavallès, P. Boucher, L. Daudet, I. Carron, S. Gigan, and K. Müller. “High-fidelity and large-scale reconfigurable photonic processor for NISQ applications”. *Optics Express* **30**, 30058–30065 (2022). (Cited on page 9 and 119).
- [91] Suraj Goel, Saroch Leedumrongwatthanakun, Natalia Herrera Valencia, Will McCutcheon, Armin Tavakoli, Claudio Conti, Pepijn W. H. Pinkse, and Mehul Malik. “Inverse design of high-dimensional quantum optical circuits in a complex medium”. *Nature Physics* Pages 1–8 (2024). (Cited on page 9 and 119).
- [92] Michael A. Nielsen and Isaac L. Chuang. “Quantum Computation and Quantum Information: 10th Anniversary Edition”. *Cambridge University Press*. Cambridge (2010). (Cited on page 16).
- [93] Thomas Vidick and Stephanie Wehner. “Introduction to Quantum Cryptography”. *Cambridge University Press*. Cambridge (2023). (Cited on page 18).
- [94] Alexander S. Holevo. “Statistical decision theory for quantum systems”. *Journal of Multivariate Analysis* **3**, 337–394 (1973). (Cited on page 20).
- [95] Carl W. Helstrom. “Quantum detection and estimation theory”. *Journal of Statistical Physics* **1**, 231–252 (1969). (Cited on page 20).
- [96] Alessio Serafini. “Quantum Continuous Variables: A Primer of Theoretical Methods”. *CRC Press*. Boca Raton (2017). (Cited on page 20, 24, and 142).
- [97] Mark M. Wilde. “Quantum Information Theory”. *Cambridge University Press*. Cambridge (2013). (Cited on page 24).

- [98] Claude E. Shannon. “A Mathematical Theory of Communication”. *Bell System Technical Journal* **27**, 379–423 (1948). (Cited on page 25 and 42).
- [99] Alfréd Rényi. “On Measures of Entropy and Information”. In *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics. Volume 4.1*, pages 547–562. University of California Press (1961). url: <https://projecteuclid.org/ebooks/berkeley-symposium-on-mathematical-statistics-and-probability/Proceedings-of-the-Fourth-Berkeley-Symposium-on-Mathematical-Statistics-and-chapter/On-Measures-of-Entropy-and-Information/bmsmp/1200512181>. (Cited on page 25).
- [100] Robert König, Renato Renner, and Christian Schaffner. “The Operational Meaning of Min- and Max-Entropy”. *IEEE Transactions on Information Theory* **55**, 4337–4347 (2009). (Cited on page 26).
- [101] Marco Tomamichel. “A framework for non-asymptotic quantum information theory”. *Doctoral Thesis*. ETH Zurich. (2012). (Cited on page 27).
- [102] Jonathan Katz and Yehuda Lindell. “Introduction to Modern Cryptography, Second Edition”. Chapman & Hall/CRC. (2014). 2nd edition. url: <https://dl.acm.org/doi/10.5555/2700550>. (Cited on page 30, 31, and 91).
- [103] Kazue Sako. “Semantic Security”. In Henk C. A. van Tilborg and Sushil Jajodia, editors, *Encyclopedia of Cryptography and Security. Pages 1176–1177*. Springer US, Boston, MA (2011). (Cited on page 32).
- [104] Gilles Brassard and Louis Salvail. “Secret-Key Reconciliation by Public Discussion”. In Tor Hellesest, editor, *Advances in Cryptology — EUROCRYPT ’93. Pages 410–423*. Lecture Notes in Computer Science Berlin, Heidelberg (1994). Springer. (Cited on page 33 and 99).
- [105] Charles H. Bennett, Gilles Brassard, Claude Crépeau, and Ueli Maurer. “Generalized privacy amplification”. *IEEE Trans. Inf. Theory* (1995). (Cited on page 33 and 99).
- [106] Roger Colbeck and Renato Renner. “No extension of quantum theory can have improved predictive power”. *Nature Communications* **2**, 411 (2011). (Cited on page 34).
- [107] Renato Renner and Ramona Wolf. “Quantum Advantage in Cryptography”. *AIAA Journal* **61**, 1895–1910 (2023). [arxiv:2206.04078](https://arxiv.org/abs/2206.04078). (Cited on page 34 and 40).
- [108] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. “Device-independent quantum key distribution secure against collective attacks”. *New Journal of Physics* **11**, 045021 (2009). (Cited on page 35).

- [109] Víctor Zapatero, Tim van Leent, Rotem Arnon-Friedman, Wen-Zhao Liu, Qiang Zhang, Harald Weinfurter, and Marcos Curty. “Advances in device-independent quantum key distribution”. *npj Quantum Information* **9**, 1–11 (2023). (Cited on page 35).
- [110] Yichen Zhang, Yiming Bian, Zhengyu Li, Song Yu, and Hong Guo. “Continuous-variable quantum key distribution system: A review and perspective” (2024). [arxiv:2310.04831](https://arxiv.org/abs/2310.04831). (Cited on page 36).
- [111] Stephen Wiesner. “Conjugate coding”. *ACM SIGACT News* **15**, 78–88 (1983). (Cited on page 36).
- [112] Peter W. Shor and John Preskill. “Simple Proof of Security of the BB84 Quantum Key Distribution Protocol”. *Physical Review Letters* **85**, 441–444 (2000). (Cited on page 37 and 42).
- [113] Alberto Carrasco-Casado, Verónica Fernández, and Natalia Denisenko. “Free-Space Quantum Key Distribution”. In Murat Uysal, Carlo Capsoni, Zabih Ghassemlooy, Anthony Boucouvalas, and Eszter Udvary, editors, *Optical Wireless Communications: An Emerging Technology*. Pages 589–607. Signals and Communication Technology. Springer International Publishing, Cham (2016). (Cited on page 37).
- [114] Frédéric Grosshans and Philippe Grangier. “Reverse reconciliation protocols for quantum cryptography with continuous variables” (2002). [arxiv:quant-ph/0204127](https://arxiv.org/abs/quant-ph/0204127). (Cited on page 38).
- [115] Andrew M. Lance, Thomas Symul, Vikram Sharma, Christian Weedbrook, Timothy C. Ralph, and Ping Koy Lam. “No-Switching Quantum Key Distribution Using Broadband Modulated Coherent Light”. *Physical Review Letters* **95**, 180503 (2005). (Cited on page 38).
- [116] Anthony Leverrier and Philippe Grangier. “Unconditional Security Proof of Long-Distance Continuous-Variable Quantum Key Distribution with Discrete Modulation”. *Physical Review Letters* **102**, 180504 (2009). (Cited on page 38).
- [117] Jie Lin, Twesh Upadhyaya, and Norbert Lütkenhaus. “Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution”. *Physical Review X* **9**, 041064 (2019). (Cited on page 38).
- [118] Jaromír Fiurášek and Nicolas J. Cerf. “Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution”. *Physical Review A* **86**, 060302 (2012). (Cited on page 38).
- [119] Michael Ben-Or, Michał Horodecki, Debbie W. Leung, Dominic Mayers, and Jonathan Oppenheim. “The Universal Composable Security of Quantum Key Distribution”. In Joe Kilian, editor, *Theory of Cryptography*. Pages 386–406. Lecture Notes in Computer Science Berlin, Heidelberg (2005). Springer. (Cited on page 40).

- [120] Eleni Diamanti. “Security and implementation of differential phase shift quantum key distribution systems”. PhD thesis. Stanford University. (2006). (Cited on page 41).
- [121] Robert König, Renato Renner, Andor Bariska, and Ueli Maurer. “Small Accessible Quantum Information Does Not Imply Security”. *Physical Review Letters* **98**, 140502 (2007). (Cited on page 42 and 84).
- [122] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters. “Mixed State Entanglement and Quantum Error Correction”. *Physical Review A* **54**, 3824–3851 (1996). [arxiv:quant-ph/9604024](#). (Cited on page 42).
- [123] Valerio Scarani and Renato Renner. “Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing”. *Physical Review Letters* **100**, 200501 (2008). (Cited on page 42).
- [124] Patrick J. Coles, Eric M. Metodiev, and Norbert Lütkenhaus. “Numerical approach for unstructured quantum key distribution”. *Nature Communications* **7**, 11712 (2016). [arxiv:1510.01294](#). (Cited on page 42).
- [125] Adam Winick, Norbert Lütkenhaus, and Patrick J. Coles. “Reliable numerical key rates for quantum key distribution”. *Quantum* **2**, 77 (2018). (Cited on page 42).
- [126] Marco Tomamichel, Roger Colbeck, and Renato Renner. “A Fully Quantum Asymptotic Equipartition Property”. *IEEE Transactions on Information Theory* **55**, 5840–5847 (2009). (Cited on page 42).
- [127] Matthias Christandl, Robert König, and Renato Renner. “Postselection Technique for Quantum Channels with Applications to Quantum Cryptography”. *Physical Review Letters* **102**, 020504 (2009). (Cited on page 42).
- [128] Marco Tomamichel and Renato Renner. “The Uncertainty Relation for Smooth Entropies”. *Physical Review Letters* **106**, 110506 (2011). [arxiv:1009.2015](#). (Cited on page 42).
- [129] Frédéric Dupuis, Omar Fawzi, and Renato Renner. “Entropy Accumulation”. *Communications in Mathematical Physics* **379**, 867–913 (2020). (Cited on page 42).
- [130] Ian George, Jie Lin, Thomas van Himbeek, Kun Fang, and Norbert Lütkenhaus. “Finite-Key Analysis of Quantum Key Distribution with Characterized Devices Using Entropy Accumulation” (2022). [arxiv:2203.06554](#). (Cited on page 42).
- [131] Tony Metger and Renato Renner. “Security of quantum key distribution from generalised entropy accumulation”. *Nature Communications* **14**, 5272 (2023). [arxiv:2203.04993](#). (Cited on page 42).
- [132] Anthony Leverrier. “Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction”. *Physical Review Letters* **118**, 200501 (2017). (Cited on page 42).

- [133] Charles H. Bennett, Gilles Brassard, Claude Crépeau, Richard Jozsa, Asher Peres, and William K. Wootters. “Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels”. *Physical Review Letters* **70**, 1895–1899 (1993). (Cited on page 43 and 74).
- [134] Koji Azuma, Sophia E. Economou, David Elkouss, Paul Hilaire, Liang Jiang, Hoi-Kwong Lo, and Ilan Tzitrin. “Quantum repeaters: From quantum networks to the quantum internet”. *Reviews of Modern Physics* **95**, 045006 (2023). (Cited on page 43).
- [135] Yang Liu, Zong-Wen Yu, Weijun Zhang, Jian-Yu Guan, Jiu-Peng Chen, Chi Zhang, Xiao-Long Hu, Hao Li, Cong Jiang, Jin Lin, Teng-Yun Chen, Lixing You, Zhen Wang, Xiang-Bin Wang, Qiang Zhang, and Jian-Wei Pan. “Experimental Twin-Field Quantum Key Distribution through Sending or Not Sending”. *Physical Review Letters* **123**, 100505 (2019). (Cited on page 43).
- [136] Xiaoqing Zhong, Jianyong Hu, Marcos Curty, Li Qian, and Hoi-Kwong Lo. “Proof-of-Principle Experimental Demonstration of Twin-Field Type Quantum Key Distribution”. *Physical Review Letters* **123**, 100506 (2019). (Cited on page 43).
- [137] Yang Liu, Wei-Jun Zhang, Cong Jiang, Jiu-Peng Chen, Chi Zhang, Wen-Xin Pan, Di Ma, Hao Dong, Jia-Min Xiong, Cheng-Jun Zhang, Hao Li, Rui-Chun Wang, Jun Wu, Teng-Yun Chen, Lixing You, Xiang-Bin Wang, Qiang Zhang, and Jian-Wei Pan. “Experimental Twin-Field Quantum Key Distribution over 1000 km Fiber Distance”. *Physical Review Letters* **130**, 210801 (2023). (Cited on page 43).
- [138] Sheng-Kai Liao, Wen-Qi Cai, Johannes Handsteiner, Bo Liu, Juan Yin, Liang Zhang, Dominik Rauch, Matthias Fink, Ji-Gang Ren, Wei-Yue Liu, Yang Li, Qi Shen, Yuan Cao, Feng-Zhi Li, Jian-Feng Wang, Yong-Mei Huang, Lei Deng, Tao Xi, Lu Ma, Tai Hu, Li Li, Nai-Le Liu, Franz Koidl, Peiyuan Wang, Yu-Ao Chen, Xiang-Bin Wang, Michael Steindorfer, Georg Kirchner, Chao-Yang Lu, Rong Shu, Rupert Ursin, Thomas Scheidl, Cheng-Zhi Peng, Jian-Yu Wang, Anton Zeilinger, and Jian-Wei Pan. “Satellite-relayed intercontinental quantum network”. *Physical Review Letters* **120**, 030501 (2018). [arxiv:1801.04418](https://arxiv.org/abs/1801.04418). (Cited on page 43).
- [139] Sebastian Ecker, Bo Liu, Johannes Handsteiner, Matthias Fink, Dominik Rauch, Fabian Steinlechner, Thomas Scheidl, Anton Zeilinger, and Rupert Ursin. “Strategies for achieving high key rates in satellite-based QKD”. *npj Quantum Information* **7**, 1–7 (2021). (Cited on page 43).
- [140] Charles Ci-Wen Lim, Feihu Xu, Jian-Wei Pan, and Artur Ekert. “Security analysis of quantum key distribution with small block length and its application to quantum space communications”. *Physical Review Letters* **126**, 100501 (2021). [arxiv:2009.04882](https://arxiv.org/abs/2009.04882). (Cited on page 43).
- [141] Wei Li, Likang Zhang, Hao Tan, Yichen Lu, Sheng-Kai Liao, Jia Huang, Hao Li, Zhen Wang, Hao-Kun Mao, Bingze Yan, Qiong Li, Yang Liu, Qiang Zhang, Cheng-Zhi Peng, Lixing You, Feihu Xu, and Jian-Wei Pan. “High-rate quantum key distribution



- exceeding 110 Mb s<sup>-1</sup>". *Nature Photonics* **17**, 416–421 (2023). (Cited on page 44 and 104).
- [142] Amanda Weerasinghe, Muataz Alhusein, Adam Alderton, Adrian Wonfor, and Richard Penty. "Practical, high-speed Gaussian coherent state continuous variable quantum key distribution with real-time parameter monitoring, optimised slicing, and post-processed key distillation". *Scientific Reports* **13**, 21543 (2023). (Cited on page 44).
- [143] Heng Wang, Yang Li, Yaodi Pi, Yan Pan, Yun Shao, Li Ma, Yichen Zhang, Jie Yang, Tao Zhang, Wei Huang, and Bingjie Xu. "Sub-Gbps key rate four-state continuous-variable quantum key distribution within metropolitan area". *Communications Physics* **5**, 1–10 (2022). (Cited on page 44).
- [144] Yan Pan, Heng Wang, Yun Shao, Yaodi Pi, Yang Li, Bin Liu, Wei Huang, and Bingjie Xu. "Experimental demonstration of high-rate discrete-modulated continuous-variable quantum key distribution system". *Optics Letters* **47**, 3307–3310 (2022). (Cited on page 44).
- [145] Bing Qi, Chi-Hang Fred Fung, Hoi-Kwong Lo, and Xiongfeng Ma. "Time-shift attack in practical quantum cryptosystems". *Quantum Information & Computation* **7**, 73–82 (2007). (Cited on page 44 and 45).
- [146] Paul C. Kocher. "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems". In Neal Koblitz, editor, *Advances in Cryptology — CRYPTO '96*. Pages 104–113. Lecture Notes in Computer Science Berlin, Heidelberg (1996). Springer. (Cited on page 44).
- [147] Nitin Jain, Birgit Stiller, Imran Khan, Dominique Elser, Christoph Marquardt, and Gerd Leuchs. "Attacks on practical quantum key distribution systems (and how to prevent them)". *Contemporary Physics* **57**, 366–387 (2016). (Cited on page 44).
- [148] Shihai Sun and Anqi Huang. "A Review of Security Evaluation of Practical Quantum Key Distribution System". *Entropy* **24**, 260 (2022). (Cited on page 44).
- [149] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry C. Sanders. "Limitations on Practical Quantum Cryptography". *Physical Review Letters* **85**, 1330–1333 (2000). (Cited on page 44 and 51).
- [150] Christian Kurtsiefer, Patrick Zarda, Sonja Mayer, and Harald Weinfurter. "The breakdown flash of silicon avalanche photodiodes-back door for eavesdropper attacks?". *Journal of Modern Optics* **48**, 2039–2047 (2001). (Cited on page 44).
- [151] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy. "Trojan-horse attacks on quantum-key-distribution systems". *Physical Review A* **73**, 022320 (2006). (Cited on page 44).
- [152] Vadim Makarov \* and Dag R. Hjelm. "Faked states attack on quantum cryptosystems". *Journal of Modern Optics* **52**, 691–705 (2005). (Cited on page 45).

- [153] Nitin Jain, Christoffer Wittmann, Lars Lydersen, Carlos Wiechers, Dominique Elser, Christoph Marquardt, Vadim Makarov, and Gerd Leuchs. “Device Calibration Impacts Security of Quantum Key Distribution”. *Physical Review Letters* **107**, 110501 (2011). (Cited on page 45).
- [154] “The European Quantum Communication Infrastructure (EuroQCI) Initiative | Shaping Europe’s digital future”. url: <https://digital-strategy.ec.europa.eu/en/policies/european-quantum-communication-infrastructure-euroqci>. (Cited on page 50).
- [155] Ilja Gerhardt, Qin Liu, Antía Lamas-Linares, Johannes Skaar, Christian Kurtsiefer, and Vadim Makarov. “Full-field implementation of a perfect eavesdropper on a quantum cryptography system”. *Nature Communications* **2**, 349 (2011). (Cited on page 51).
- [156] Alexander I. Lvovsky, Barry C. Sanders, and Wolfgang Tittel. “Optical quantum memory”. *Nature Photonics* **3**, 706–714 (2009). (Cited on page 51).
- [157] C. Simon, M. Afzelius, J. Appel, A. Boyer de la Giroday, S. J. Dewhurst, N. Gisin, C. Y. Hu, F. Jelezko, S. Kröll, J. H. Müller, J. Nunn, E. S. Polzik, J. G. Rarity, H. De Riedmatten, W. Rosenfeld, A. J. Shields, N. Sköld, R. M. Stevenson, R. Thew, I. A. Walmsley, M. C. Weber, H. Weinfurter, J. Wrachtrup, and R. J. Young. “Quantum memories”. *The European Physical Journal D* **58**, 1–22 (2010). (Cited on page 51).
- [158] Khabat Heshami, Duncan G. England, Peter C. Humphreys, Philip J. Bustard, Victor M. Acosta, Joshua Nunn, and Benjamin J. Sussman. “Quantum memories: Emerging applications and recent advances”. *Journal of Modern Optics* **63**, 2005–2028 (2016). (Cited on page 51 and 91).
- [159] Debra S. Herrmann. “Using the Common Criteria for IT Security Evaluation”. *Auerbach Publications*. New York (2019). (Cited on page 51).
- [160] “Application of Attack Potential to Smartcards and Similar Devices” (2020). (Cited on page 53 and 60).
- [161] Jérôme Lodewyck, Thierry Debuisschert, Raúl García-Patrón, Rosa Tualle-Brouri, Nicolas J. Cerf, and Philippe Grangier. “Experimental Implementation of Non-Gaussian Attacks on a Continuous-Variable Quantum-Key-Distribution System”. *Physical Review Letters* **98**, 030503 (2007). (Cited on page 55).
- [162] Niraj Kumar, Iordanis Kerenidis, and Eleni Diamanti. “Experimental demonstration of quantum advantage for one-way communication complexity surpassing best-known classical protocol”. *Nature Communications* **10**, 4152 (2019). (Cited on page 66 and 104).
- [163] Juan Miguel Arrazola and Norbert Lütkenhaus. “Quantum fingerprinting with coherent states and a constant mean number of photons”. *Physical Review A* **89**, 062305 (2014). (Cited on page 66).

- [164] Anup Rao and Amir Yehudayoff. “Communication Complexity: And Applications”. Cambridge University Press. (2020). (Cited on page 67, 68, 72, and 143).
- [165] Ilan Newman. “Private vs. common random bits in communication complexity”. *Information Processing Letters* **39**, 67–71 (1991). (Cited on page 68).
- [166] R. Bar-Yehuda, B. Chor, E. Kushilevitz, and A. Orlitsky. “Privacy, additional information and communication”. *IEEE Transactions on Information Theory* **39**, 1930–1943 (1993). (Cited on page 70).
- [167] A. Chakrabarti, Yaoyun Shi, A. Wirth, and A. Yao. “Informational complexity and the direct sum problem for simultaneous message complexity”. In Proceedings 42nd IEEE Symposium on Foundations of Computer Science. Pages 270–278. (2001). (Cited on page 70).
- [168] Ziv Bar-Yossef, T. S. Jayram, Ravi Kumar, and D. Sivakumar. “An information statistics approach to data stream and communication complexity”. *Journal of Computer and System Sciences* **68**, 702–732 (2004). (Cited on page 70).
- [169] Mark Braverman. “Interactive Information Complexity”. *SIAM Review* **59**, 803–846 (2017). (Cited on page 70 and 72).
- [170] O. Weinstein. “Information Complexity and the Quest for Interactive Compression”. *ACM SIGACT News* **46**, 41–64 (2015). (Cited on page 70).
- [171] Mark Braverman and Ankit Garg. “Public vs Private Coin in Bounded-Round Information”. In Automata, Languages, and Programming. Volume 8572, pages 502–513. Springer Berlin Heidelberg, Berlin, Heidelberg (2014). (Cited on page 71).
- [172] Mark Braverman and Dor Minzer. “New separations results for external information”. In Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing. Pages 248–258. Virtual Italy (2021). ACM. (Cited on page 71 and 72).
- [173] Ran Raz. “A Parallel Repetition Theorem”. *SIAM Journal on Computing* **27**, 763–803 (1998). (Cited on page 72).
- [174] Boaz Barak, Mark Braverman, Xi Chen, and Anup Rao. “How to Compress Interactive Communication”. *SIAM Journal on Computing* **42**, 1327–1363 (2013). (Cited on page 72).
- [175] Prahladh Harsha, Rahul Jain, David McAllester, and Jaikumar Radhakrishnan. “The Communication Complexity of Correlation”. *IEEE Transactions on Information Theory* **56**, 438–449 (2010). (Cited on page 72 and 73).
- [176] Richard Cleve and Harry Buhrman. “Substituting quantum entanglement for communication”. *Physical Review A* **56**, 1201–1204 (1997). (Cited on page 74).

- [177] Ran Raz. “Exponential separation of quantum and classical communication complexity”. In Proceedings of the Thirty-First Annual ACM Symposium on Theory of Computing. Pages 358–367. STOC ’99 New York, NY, USA (1999). Association for Computing Machinery. (Cited on page 74 and 78).
- [178] Harry Buhrman, Richard Cleve, John Watrous, and Ronald de Wolf. “Quantum Fingerprinting”. *Physical Review Letters* **87**, 167902 (2001). (Cited on page 74).
- [179] Dmitry Gavinsky. “Bare quantum simultaneity versus classical interactivity in communication complexity”. In Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing. Pages 401–411. STOC 2020 New York, NY, USA (2020). Association for Computing Machinery. (Cited on page 74).
- [180] Ilan Kremer. “Quantum communication”. Master’s thesis. Hebrew University of Jerusalem. (1995). url: <https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=d3f4b7f77d920554202672dc81398ac2ee8bea79>. (Cited on page 78).
- [181] Uri Grupel. “Sampling on the Sphere by Mutually Orthogonal Subspaces”. *Proceedings of the Twenty-Eighth Annual ACM-SIAM Symposium on Discrete Algorithms* Pages 973–983 (2017). arxiv:1607.03714. (Cited on page 78).
- [182] Iordanis Kerenidis, Sophie Laplante, Virginie Lerays, Jeremie Roland, and David Xiao. “Lower Bounds on Information Complexity via Zero-Communication Protocols and Applications”. In Proceedings of the 2012 IEEE 53rd Annual Symposium on Foundations of Computer Science. Pages 500–509. FOCS ’12 USA (2012). IEEE Computer Society. (Cited on page 78).
- [183] Zixin Huang, Pieter Kok, and Cosmo Lupo. “Fault-tolerant quantum data locking”. *Physical Review A* **103**, 052611 (2021). (Cited on page 83).
- [184] Aaron D. Wyner. “The wire-tap channel”. *The Bell System Technical Journal* **54**, 1355–1387 (1975). (Cited on page 84).
- [185] David DiVincenzo, Michal Horodecki, Debbie Leung, John Smolin, and Barbara Terhal. “Locking Classical Correlations in Quantum States”. *Physical review letters* **92**, 067902 (2004). (Cited on page 84 and 85).
- [186] Cosmo Lupo, Mark M. Wilde, and Seth Lloyd. “Robust quantum data locking from phase modulation”. *Physical Review A* **90**, 022326 (2014). (Cited on page 85).
- [187] Patrick Hayden, Debbie Leung, Peter W. Shor, and Andreas Winter. “Randomizing Quantum States: Constructions and Applications”. *Communications in Mathematical Physics* **250**, 371–391 (2004). (Cited on page 85).
- [188] Omar Fawzi, Patrick Hayden, and Pranab Sen. “From Low-Distortion Norm Embeddings to Explicit Uncertainty Relations and Efficient Information Locking”. *Journal of the ACM* **60**, 44:1–44:61 (2013). (Cited on page 85).

- [189] Daniel J. Lum, John C. Howell, M. S. Allman, Thomas Gerrits, Varun B. Verma, Sae Woo Nam, Cosmo Lupo, and Seth Lloyd. “Quantum enigma machine: Experimentally demonstrating quantum data locking”. *Physical Review A* **94**, 022315 (2016). (Cited on page 85).
- [190] Scott Aaronson and Alex Arkhipov. “The computational complexity of linear optics”. In Proceedings of the Forty-Third Annual ACM Symposium on Theory of Computing. Pages 333–342. STOC ’11 New York, NY, USA (2011). Association for Computing Machinery. (Cited on page 85).
- [191] Zixin Huang, Peter P. Rohde, Dominic W. Berry, Pieter Kok, Jonathan P. Dowling, and Cosmo Lupo. “Photonic quantum data locking”. *Quantum* **5**, 447 (2021). (Cited on page 85).
- [192] Dominic Mayers. “Unconditionally Secure Quantum Bit Commitment is Impossible”. *Physical Review Letters* **78**, 3414–3417 (1997). (Cited on page 86).
- [193] Manuel B. Santos, Paulo Mateus, and Armando N. Pinto. “Quantum oblivious transfer: A short review”. *Entropy* **24**, 945 (2022). [arxiv:2206.03313](https://arxiv.org/abs/2206.03313). (Cited on page 86).
- [194] Nelly Huei Ying Ng, Siddarth K. Joshi, Chia Chen Ming, Christian Kurtsiefer, and Stephanie Wehner. “Experimental implementation of bit commitment in the noisy-storage model”. *Nature Communications* **3**, 1326 (2012). (Cited on page 86).
- [195] C. Erven, N. Ng, N. Gigo, R. Laflamme, S. Wehner, and G. Weihs. “An experimental implementation of oblivious transfer in the noisy storage model”. *Nature Communications* **5**, 3418 (2014). (Cited on page 86).
- [196] Fabian Furrer, Tobias Gehring, Christian Schaffner, Christoph Pacher, Roman Schnabel, and Stephanie Wehner. “Continuous-variable protocol for oblivious transfer in the noisy-storage model”. *Nature Communications* **9**, 1450 (2018). (Cited on page 86).
- [197] Manuel A. Ballester, Stephanie Wehner, and Andreas Winter. “State Discrimination with Post-Measurement Information”. *IEEE Transactions on Information Theory* **54**, 4183–4198 (2008). [arxiv:quant-ph/0608014](https://arxiv.org/abs/quant-ph/0608014). (Cited on page 88).
- [198] Stephanie Wehner, Christian Schaffner, and Barbara Terhal. “Cryptography from Noisy Storage”. *Physical Review Letters* **100**, 220502 (2008). [arxiv:0711.2895](https://arxiv.org/abs/0711.2895). (Cited on page 88).
- [199] Ivan B. Damgård, Serge Fehr, Renato Renner, Louis Salvail, and Christian Schaffner. “A Tight High-Order Entropic Quantum Uncertainty Relation with Applications”. In Alfred Menezes, editor, Advances in Cryptology - CRYPTO 2007. Pages 360–378. Lecture Notes in Computer Science Berlin, Heidelberg (2007). Springer. (Cited on page 88).
- [200] Robert König and Stephanie Wehner. “A Strong Converse for Classical Channel Coding Using Entangled Inputs”. *Physical Review Letters* **103**, 070504 (2009). (Cited on page 89).

- [201] Romain Alléaume. “Quantum cryptography and its application frontiers”. Habilitation à diriger des recherches. Télécom Paris. (2021). url: <https://perso.telecom-paristech.fr/alleaume/HDRMainv10final.pdf>. (Cited on page 90).
- [202] Dominique Unruh. “Revocable Quantum Timed-Release Encryption”. *Journal of the ACM* **62**, 49:1–49:76 (2015). (Cited on page 91).
- [203] Craig Gidney and Martin Ekerå. “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits”. *Quantum* **5**, 433 (2021). (Cited on page 92).
- [204] Michael Epping, Hermann Kampermann, Chiara Macchiavello, and Dagmar Bruß. “Multi-partite entanglement can speed up quantum key distribution in networks”. *New Journal of Physics* **19**, 093012 (2017). (Cited on page 105).
- [205] Federico Grasselli, Hermann Kampermann, and Dagmar Bruß. “Finite-key effects in multipartite quantum key distribution protocols”. *New Journal of Physics* **20**, 113014 (2018). (Cited on page 105).
- [206] Jianwei Wang, Fabio Sciarrino, Anthony Laing, and Mark G. Thompson. “Integrated photonic quantum technologies”. *Nature Photonics* **14**, 273–284 (2020). (Cited on page 110).
- [207] Caterina Taballione, Malaquias Correa Anguita, Michiel de Goede, Pim Venderbosch, Ben Kassenberg, Henk Snijders, Narasimhan Kannan, Ward L. Vleeshouwers, Devin Smith, Jörn P. Epping, Reinier van der Meer, Pepijn W. H. Pinkse, Hans van den Vlekert, and Jelmer J. Renema. “20-Mode Universal Quantum Photonic Processor”. *Quantum* **7**, 1071 (2023). (Cited on page 110).
- [208] Joseph W. Goodman. “Speckle Phenomena in Optics: Theory and Applications”. *Roberts and Company Publishers*. (2007). (Cited on page 110).
- [209] Yoseph Imry. “Active Transmission Channels and Universal Conductance Fluctuations”. *Europhysics Letters* **1**, 249 (1986). (Cited on page 111).
- [210] S. M. Popoff, G. Lerosey, R. Carminati, M. Fink, A. C. Boccara, and S. Gigan. “Measuring the Transmission Matrix in Optics: An Approach to the Study and Control of Light Propagation in Disordered Media”. *Physical Review Letters* **104**, 100601 (2010). (Cited on page 111, 113, and 115).
- [211] John Senior. “Optical Fiber Communications: Principles and Practice”. Pearson Education. (2009). url: <https://shijuinpallotti.files.wordpress.com/2019/07/optical-fiber-communications-principles-and-pr.pdf>. (Cited on page 112).
- [212] David J. Richardson, John M. Fini, and Lynn E. Nelson. “Space Division Multiplexing in Optical Fibres”. *Nature Photonics* **7**, 354–362 (2013). [arxiv:1303.3908](https://arxiv.org/abs/1303.3908). (Cited on page 112).

- [213] Jiawei Luo, Jiajun Liang, Daixuan Wu, Yin Huang, Zhiwei Chen, Zhibing Liu, Dongdong Zou, Fan Li, and Yuecheng Shen. “Simultaneous dual-channel data transmission through a multimode fiber via wavefront shaping”. *Applied Physics Letters* **123**, 151106 (2023). (Cited on page 112).
- [214] Martin Plöschner, Tomáš Tyc, and Tomáš Čižmár. “Seeing through chaos in multimode fibres”. *Nature Photonics* **9**, 529–535 (2015). (Cited on page 112 and 113).
- [215] Babak Rahmani, Damien Loterie, Georgia Konstantinou, Demetri Psaltis, and Christophe Moser. “Multimode optical fiber transmission with a deep learning network”. *Light: Science & Applications* **7**, 69 (2018). (Cited on page 112).
- [216] Zijie Liu. “Convolutional Neural Networks for Multimode Fiber Study: A Review”. In 2020 International Conference on Computing and Data Science (CDS). Pages 174–178. (2020). (Cited on page 112).
- [217] Changyan Zhu, Eng Aik Chan, You Wang, Weina Peng, Ruixiang Guo, Baile Zhang, Cesare Soci, and Yidong Chong. “Image reconstruction through a multimode fiber with a simple neural network architecture”. *Scientific Reports* **11**, 896 (2021). (Cited on page 112).
- [218] Keang-Po Ho and Joseph Kahn. “Mode Coupling and its Impact on Spatially Multiplexed Systems”. *Optical Fiber Telecommunications VIB: Systems and Networks: Sixth Edition* (2013). (Cited on page 112).
- [219] K. Kitayama, S. Seikai, and N. Uchida. “Impulse response prediction based on experimental mode coupling coefficient in a 10-km long graded-index fiber”. *IEEE Journal of Quantum Electronics* **16**, 356–362 (1980). (Cited on page 112).
- [220] D. Gloge. “Optical power flow in multimode fibers”. *The Bell System Technical Journal* **51**, 1767–1783 (1972). (Cited on page 112).
- [221] Robert Olshansky. “Mode Coupling Effects in Graded-Index Optical Fibers”. *Applied Optics* **14**, 935–945 (1975). (Cited on page 112).
- [222] Mahdih B. Shemirani. “Modeling and Compensation of Modal Dispersion in Graded-Index Multimode Fiber”. PhD thesis. PhD thesis, Stanford University. (2010). (Cited on page 113).
- [223] Mahdih B. Shemirani, Wei Mao, Rahul Alex Panicker, and Joseph M. Kahn. “Principal Modes in Graded-Index Multimode Fiber in Presence of Spatial- and Polarization-Mode Coupling”. *Journal of Lightwave Technology* **27**, 1248–1261 (2009). (Cited on page 113).
- [224] Mahdih B. Shemirani and Joseph M. Kahn. “Higher-Order Modal Dispersion in Graded-Index Multimode Fiber”. *Journal of Lightwave Technology* **27**, 5461–5468 (2009). (Cited on page 113).

- [225] Adrian A. Juarez, Edgar Krune, Stefan Warm, Christian A. Bunge, and Klaus Petermann. “Modeling of Mode Coupling in Multimode Fibers With Respect to Bandwidth and Loss”. *Journal of Lightwave Technology* **32**, 1549–1558 (2014). (Cited on page 113).
- [226] Keang-Po Ho and Joseph M. Kahn. “Statistics of Group Delays in Multimode Fiber With Strong Mode Coupling”. *Journal of Lightwave Technology* **29**, 3119–3128 (2011). (Cited on page 113 and 116).
- [227] P. Chiarawongse, H. Li, W. Xiong, C. W. Hsu, H. Cao, and T. Kottos. “Statistical Description of Transport in Multimode Fibers with Mode-Dependent Loss”. *New Journal of Physics* **20**, 113028 (2018). [arxiv:1806.11149](https://arxiv.org/abs/1806.11149). (Cited on page 113).
- [228] Yaxin Li, Doron Cohen, and Tsampikos Kottos. “Coherent Wave Propagation in Multimode Systems with Correlated Noise”. *Physical Review Letters* **122**, 153903 (2019). (Cited on page 113).
- [229] Dirk E. Boonzajer Flaes, Jan Stopka, Sergey Turtaev, Johannes F. de Boer, Tomáš Tyc, and Tomáš Čižmár. “Robustness of Light-Transport Processes to Bending Deformations in Graded-Index Multimode Waveguides”. *Physical Review Letters* **120**, 233901 (2018). (Cited on page 113).
- [230] Sébastien M. Popoff. “Wavefrontshaping/pyMMF” (2023). (Cited on page 113).
- [231] Maxime W. Matthès, Yaron Bromberg, Julien De Rosny, and Sébastien M. Popoff. “Learning and Avoiding Disorder in Multimode Fibers”. *Physical Review X* **11**, 021060 (2021). (Cited on page 113).
- [232] H. W. Babcock. “The possibility of compensating astronomical seeing”. *Publications of the Astronomical Society of the Pacific* **65**, 229 (1953). (Cited on page 113).
- [233] I. M. Vellekoop and A. P. Mosk. “Focusing coherent light through opaque strongly scattering media”. *Optics Letters* **32**, 2309–2311 (2007). (Cited on page 113 and 114).
- [234] “Texas Instruments DLP products”. url: <https://www.ti.com/dlp-chip/overview.html>. (Cited on page 114).
- [235] Louisiane Devaud. “Matricial approach for field correlation and temporal control of light propagation through strongly scattering media”. These de doctorat. Sorbonne université. (2021). url: <https://www.theses.fr/2021SORUS311>. (Cited on page 114).
- [236] Hugo Defienne. “Quantum walks of photons in disordered media”. These de doctorat. Paris 6. (2015). url: <https://www.theses.fr/2015PA066630>. (Cited on page 115, 116, and 122).
- [237] Saroch Leedumrongwatthanakun. “Quantum information processing with a multimode fibre”. These de doctorat. Sorbonne université. (2019). url: <http://www.theses.fr/2019SORUS526>. (Cited on page 115, 116, and 123).



- [238] I. M. Vellekoop and A. P. Mosk. “Phase control algorithms for focusing light through turbid media”. *Optics Communications* **281**, 3071–3080 (2008). (Cited on page 114).
- [239] Antoine Boniface, Baptiste Blochet, Jonathan Dong, and Sylvain Gigan. “Noninvasive light focusing in scattering media using speckle variance optimization”. *Optica* **6**, 1381–1385 (2019). (Cited on page 114).
- [240] Zahra Fayyaz, Nafiseh Mohammadian, M. Reza Rahimi Tabar, Rayyan Manwar, and Kamran Avanaki. “A comparative study of optimization algorithms for wavefront shaping”. *Journal of Innovative Optical Health Sciences* **12**, 1942002 (2019). (Cited on page 114).
- [241] Robert A. Fisher. “Optical Phase Conjugation”. *Academic Press*. (1983). (Cited on page 115).
- [242] Arnaud Derode, Arnaud Tourin, and Mathias Fink. “Random multiple scattering of ultrasound. II. Is time reversal a self-averaging process?”. *Physical Review E* **64**, 036606 (2001). (Cited on page 116).
- [243] V. A. Marčenko and L. A. Pastur. “Distribution of Eigenvalues for Some Sets of Random Matrices.”. *Mathematics of the USSR-Sbornik* **1**, 457 (1967). (Cited on page 116).
- [244] Wen Xiong, Chia Wei Hsu, Yaron Bromberg, Jose Enrique Antonio-Lopez, Rodrigo Amezcua Correa, and Hui Cao. “Complete polarization control in multimode fibers with polarization and mode coupling”. *Light: Science & Applications* **7**, 54 (2018). (Cited on page 116).
- [245] O. N. Dorokhov. “Transmission coefficient and the localization length of an electron in N bound disordered chains”. *Soviet Journal of Experimental and Theoretical Physics Letters* **36**, 318 (1982). url: <https://ui.adsabs.harvard.edu/abs/1982JETPL..36..318D>. (Cited on page 116).
- [246] P. A Mello, P Pereyra, and N Kumar. “Macroscopic approach to multichannel disordered conductors”. *Annals of Physics* **181**, 290–317 (1988). (Cited on page 116).
- [247] Roarke Horstmeyer, Haowen Ruan, and Changhui Yang. “Guidestar-assisted wavefront-shaping methods for focusing light into biological tissue”. *Nature Photonics* **9**, 563–571 (2015). (Cited on page 116).
- [248] “4D Imaging radar”. (Cited on page 116).
- [249] Antoine Liutkus, David Martina, Sébastien Popoff, Gilles Chardon, Ori Katz, Geoffroy Lerosey, Sylvain Gigan, Laurent Daudet, and Igor Carron. “Imaging With Nature: Compressive Imaging Using a Multiply Scattering Medium”. *Scientific Reports* **4**, 5552 (2014). (Cited on page 116).

- [250] Donald B. Conkey, Albert N. Brown, Antonio M. Caravaca-Aguirre, and Rafael Piestun. “Genetic algorithm optimization for focusing through turbid media in noisy environments”. *Optics Express* **20**, 4840–4849 (2012). (Cited on page 117).
- [251] Ivo M. Vellekoop. “Feedback-based wavefront shaping”. *Optics Express* **23**, 12189–12206 (2015). (Cited on page 117).
- [252] Etienne Cuche, Pierre Marquet, and Christian Depeursinge. “Spatial filtering for zero-order and twin-image elimination in digital off-axis holography”. *Applied Optics* **39**, 4070–4075 (2000). (Cited on page 118).
- [253] Daniele Cozzolino, Beatrice Da Lio, Davide Bacco, and Leif Katsuo Oxenløwe. “High-Dimensional Quantum Communication: Benefits, Progress, and Future Challenges”. *Advanced Quantum Technologies* **2**, 1900038 (2019). (Cited on page 118).
- [254] Stefan Rothe, Karl-Ludwig Besser, David Krause, Robert Kuschmierz, Nektarios Koukourakis, Eduard Jorswieck, and Jürgen W. Czarske. “Securing Data in Multi-mode Fibers by Exploiting Mode-Dependent Light Propagation Effects”. *Research* **6**, 0065 (2023). (Cited on page 118 and 119).
- [255] Matthieu Bloch and João Barros. “Physical-Layer Security: From Information Theory to Security Engineering”. *Cambridge University Press*. Cambridge (2011). (Cited on page 119).
- [256] Aaron D. Wyner. “The wire-tap channel”. *The Bell System Technical Journal* **54**, 1355–1387 (1975). (Cited on page 119).
- [257] Thomas J. Huisman, Simon R. Huisman, Allard P. Mosk, and Pepijn W. H. Pinkse. “Controlling single-photon Fock-state propagation through opaque scattering media”. *Applied Physics B* **116**, 603–607 (2014). (Cited on page 119).
- [258] H. Defienne, M. Barbieri, B. Chalopin, B. Chatel, I. A. Walmsley, B. J. Smith, and S. Gigan. “Nonclassical light manipulation in a multiple-scattering medium”. *Optics Letters* **39**, 6090–6093 (2014). (Cited on page 119).
- [259] Tom A. W. Wolterink, Ravitej Uppu, Georgios Ctistis, Willem L. Vos, Klaus-J. Boller, and Pepijn W. H. Pinkse. “Programmable two-photon quantum interference in  $\{10\}^3$  channels in opaque scattering media”. *Physical Review A* **93**, 053817 (2016). (Cited on page 119).
- [260] Hugo Defienne, Marco Barbieri, Ian A. Walmsley, Brian J. Smith, and Sylvain Gigan. “Two-photon quantum walk in a multimode fiber”. *Science Advances* **2**, e1501054 (2016). (Cited on page 119).
- [261] Ichirou Yamaguchi and Tong Zhang. “Phase-shifting digital holography”. *Optics Letters* **22**, 1268–1270 (1997). (Cited on page 122).

- [262] Matthias Hofer and Sophie Brasselet. “Manipulating the transmission matrix of scattering media for nonlinear imaging beyond the memory effect”. *Optics Letters* **44**, 2137–2140 (2019). (Cited on page 122).
- [263] Anthony Laing and Jeremy L. O’Brien. “Super-stable tomography of any linear optical device” (2012). [arxiv:1208.2868](https://arxiv.org/abs/1208.2868). (Cited on page 123).
- [264] Maxime W. Matthès, Philipp del Hougne, Julien de Rosny, Geoffroy Lerosey, and Sébastien M. Popoff. “Optical complex media as universal reconfigurable linear operators”. *Optica* **6**, 465–472 (2019). (Cited on page 124 and 158).
- [265] Tommaso Gagliardini, Andreas Hülsing, and Christian Schaffner. “Semantic Security and Indistinguishability in the Quantum World”. In Matthew Robshaw and Jonathan Katz, editors, *Advances in Cryptology – CRYPTO 2016*. Pages 60–89. Lecture Notes in Computer Science Berlin, Heidelberg (2016). Springer. (Cited on page 133).
- [266] Céline Chevalier, Ehsan Ebrahimi, and Quoc-Huy Vu. “On Security Notions for Encryption in a Quantum World”. In Takanori Isobe and Santanu Sarkar, editors, *Progress in Cryptology – INDOCRYPT 2022*. Pages 592–613. Lecture Notes in Computer Science Cham (2022). Springer International Publishing. (Cited on page 133).
- [267] Nikhil Bansal and Makrand Sinha. “K-forrelation optimally separates Quantum and classical query complexity”. In *Proceedings of the 53rd Annual ACM SIGACT Symposium on Theory of Computing*. Pages 1303–1316. Virtual Italy (2021). ACM. (Cited on page 134).
- [268] Arkadev Chattopadhyay, Yuval Filmus, Sajin Koroth, Or Meir, and Toniann Pitassi. “Query-To-Communication Lifting for BPP Using Inner Product”. In *46th International Colloquium on Automata, Languages, and Programming (ICALP 2019)*. Schloss Dagstuhl - Leibniz Zentrum für Informatik (2019). (Cited on page 134).
- [269] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. “Pseudorandom Quantum States”. In *Advances in Cryptology – CRYPTO 2018: 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19–23, 2018, Proceedings, Part III*. Pages 126–152. Berlin, Heidelberg (2018). Springer-Verlag. (Cited on page 134).
- [270] Zvika Brakerski and Omri Shmueli. “(Pseudo) Random Quantum States with Binary Phase”. In Dennis Hofheinz and Alon Rosen, editors, *Theory of Cryptography*. Pages 229–250. Lecture Notes in Computer Science. Springer International Publishing (2019). (Cited on page 134).
- [271] Giulio Gianfelici, Hermann Kampermann, and Dagmar Bruß. “Theoretical framework for physical unclonable functions, including quantum readout”. *Physical Review A* **101**, 042337 (2020). (Cited on page 135).
- [272] Myrto Arapinis, Mahshid Delavar, Mina Doosti, and Elham Kashefi. “Quantum Physical Unclonable Functions: Possibilities and Impossibilities”. *Quantum* **5**, 475 (2021). (Cited on page 135).

- [273] Niraj Kumar, Rawad Mezher, and Elham Kashefi. “Efficient Construction of Quantum Physical Unclonable Functions with Unitary  $t$ -designs” (2021). [arxiv:2101.05692](https://arxiv.org/abs/2101.05692). (Cited on page 135).
- [274] Vladlen Galetsky, Soham Ghosh, Christian Deppe, and Roberto Ferrara. “Comparison of Quantum PUF models”. In 2022 IEEE Globecom Workshops (GC Wkshps). Pages 820–825. (2022). (Cited on page 135).
- [275] Kaushik Chakraborty, Mina Doosti, Yao Ma, Chirag Wadhwa, Myrto Arapinis, and Elham Kashefi. “Quantum Lock: A Provable Quantum Communication Advantage”. *Quantum* **7**, 1014 (2023). (Cited on page 135).
- [276] Boris Škorić. “Quantum Readout of Physical Unclonable Functions”. In Daniel J. Bernstein and Tanja Lange, editors, Progress in Cryptology – AFRICACRYPT 2010. Pages 369–386. Lecture Notes in Computer Science Berlin, Heidelberg (2010). Springer. (Cited on page 135).
- [277] Boris Škorić, Allard P. Mosk, and Pepijn W. H. Pinkse. “Security of Quantum-Readout PUFs against quadrature based challenge estimation attacks”. *International Journal of Quantum Information* **11**, 1350041 (2013). (Cited on page 135).
- [278] Yao Yao, Ming Gao, Mo Li, and Jian Zhang. “Quantum cloning attacks against PUF-based quantum authentication systems”. *Quantum Information Processing* **15**, 3311–3325 (2016). (Cited on page 135).
- [279] Pepijn W. H. Pinkse and Matthijs Velsink. “Key holder for an optical key and system comprising the key holder for authenticating an optical key by verifying a match of challenge-response pairs”. Patent number US20240039740A1 (2024). url: <https://patents.google.com/patent/US20240039740A1/en>. (Cited on page 135).
- [280] Yue-Meng Chi, Bing Qi, Wen Zhu, Li Qian, Hoi-Kwong Lo, Sun-Hyun Youn, A. I. Lvovsky, and Liang Tian. “A balanced homodyne detector for high-rate Gaussian-modulated coherent-state quantum key distribution”. *New Journal of Physics* **13**, 013003 (2011). (Cited on page 138).
- [281] Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, and Eleni Diamanti. “Experimental demonstration of long-distance continuous-variable quantum key distribution”. *Nature Photonics* **7**, 378–381 (2013). (Cited on page 138).
- [282] Matteo G. A. Paris. “Displacement operator by beam splitter”. *Physics Letters A* **217**, 78–80 (1996). (Cited on page 139).
- [283] Jing-Zheng Huang, Christian Weedbrook, Zhen-Qiang Yin, Shuang Wang, Hong-Wei Li, Wei Chen, Guang-Can Guo, and Zheng-Fu Han. “Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack”. *Physical Review A* **87**, 062329 (2013). (Cited on page 139).

- [284] Xiang-Chun Ma, Shi-Hai Sun, Mu-Sheng Jiang, and Lin-Mei Liang. “Local oscillator fluctuation opens a loophole for Eve in practical continuous-variable quantum-key-distribution systems”. *Physical Review A* **88**, 022339 (2013). (Cited on page 139).
- [285] Jing-Zheng Huang, Sébastien Kunz-Jacques, Paul Jouguet, Christian Weedbrook, Zhen-Qiang Yin, Shuang Wang, Wei Chen, Guang-Can Guo, and Zheng-Fu Han. “Quantum hacking on quantum key distribution using homodyne detection”. *Physical Review A* **89**, 032304 (2014). (Cited on page 139).
- [286] Anthony Leverrier and Philippe Grangier. “A simple proof that Gaussian attacks are optimal among collective attacks against continuous-variable quantum key distribution with a Gaussian modulation”. *Physical Review A* **81**, 062314 (2010). [arxiv:0912.4132](https://arxiv.org/abs/0912.4132). (Cited on page 142).
- [287] Fabian Laudenbach, Christoph Pacher, Chi-Hang Fred Fung, Andreas Poppe, Momtchil Peev, Bernhard Schrenk, Michael Hentschel, Philip Walther, and Hannes Hübel. “Continuous-Variable Quantum Key Distribution with Gaussian Modulation—The Theory of Practical Implementations”. *Advanced Quantum Technologies* **1**, 1800011 (2018). (Cited on page 142).
- [288] Robert J. Adler and Jonathan E. Taylor. “Gaussian Inequalities”. In *Random Fields and Geometry*. Pages 49–64. Springer Monographs in Mathematics. Springer, New York, NY (2007). (Cited on page 151).
- [289] Gautam Kamath. “Bounds on the Expectation of the Maximum of Samples from a Gaussian”. url: [http://www.gautamkamath.com/writings/gaussian\\_max.pdf](http://www.gautamkamath.com/writings/gaussian_max.pdf). (Cited on page 151).
- [290] Guillaume Aubrun and Stanisław Szarek. “Alice and Bob Meet Banach”. *Volume 223 of Mathematical Surveys and Monographs*. American Mathematical Society. Providence, Rhode Island (2017). (Cited on page 151).

**Titre :** Communications quantiques multimodes et cryptographie hybride

**Mots clés :** Communications quantiques, Cryptographie quantique, Optique quantique

**Résumé :** La cryptographie quantique a été largement définie comme une forme novatrice de cryptographie ne reposant sur aucune hypothèse de difficulté computationnelle. Cependant, avec l'évolution du domaine, et en particulier alors que la distribution quantique de clé (QKD) atteint des niveaux élevés de préparation technologique, il semble qu'il faille trouver un équilibre critique. D'une part, il y a la quête du niveau de sécurité théorique le plus élevé. D'autre part, une seconde direction consiste à optimiser la sécurité et la performance pour une utilisation réelle, tout en offrant un avantage par rapport à la cryptographie classique. Dans cette thèse, nous avons exploré de nouvelles voies vers cette seconde direction, à savoir la cryptographie quantique en conditions réelles. Dans le premier projet, nous défendons un message simple mais puissant : les attaques les plus dangereuses contre la QKD, pour lesquelles le développement de contre-mesures est crucial, sont les plus faciles à mettre en œuvre. Par conséquent, nous effectuons une évaluation de la vulnérabilité d'un dispositif de QKD à variables continues, proposant une nouvelle méthodologie pour la certification de sécurité basée sur le classement des attaques.

Dans le deuxième projet, nous introduisons une construction explicite pour un protocole de distribution de clés dans le modèle de sécurité Quantum Computational Timelock (QCT), où l'on suppose que le chiffrement sécurisé computationnellement ne peut être rompu qu'après un temps bien plus long que le temps de cohérence des mémoires quantiques disponibles. En tirant parti des hypothèses QCT, nous construisons un protocole de distribution de clés basé sur le problème de Hidden Matching, pour lequel il existe un écart exponentiel en complexité de communication unidirectionnelle entre les stratégies classiques et quantiques. En particulier, en exploitant cet écart exponentiel, nous débloquons la possibilité d'envoyer plusieurs copies du même état pour réaliser un établissement de clé avec des performances qui vont au-delà de la QKD standard.

Dans le dernier projet expérimental, nous étudions la faisabilité de démontrer un avantage quantique en complexité de communication. En particulier, nous exploitons le mélange de modes complexe inhérent aux fibres multimodes en employant des techniques de wavefront shaping pour aborder les problèmes de complexité de communication quantique.

**Title :** Multimode quantum communications and hybrid cryptography

**Keywords :** Quantum communication, Quantum cryptography, Quantum optics

**Abstract :** Quantum cryptography has been largely defined as a novel form of cryptography that would not rely on any computational hardness assumption. However, as the field progresses, and in particular as Quantum Key Distribution (QKD) reaches high technological readiness levels, it appears that there might be a critical balance to strike. On the one hand, we have the quest for the highest theoretical security level. On the other, a second direction consists in optimizing security and performance for real-world use, while still providing an edge over classical cryptography. In this thesis, we have explored new paths towards this second direction, namely real-world quantum cryptography.

In the first project, we promote a simple yet powerful message: the most dangerous attacks against QKD, for which the development of countermeasures is crucial, are the easiest ones to implement. Hence, we perform a vulnerability assessment of a Continuous-Variable QKD system device, proposing a novel methodology for security certification based on attack rating.

In the second project, we introduce an explicit construction for a key distribution protocol in the Quantum Computational Timelock (QCT) security model, where one assumes that computationally secure encryption may only be broken after a time much longer than the coherence time of available quantum memories. Taking advantage of the QCT assumptions, we build a key distribution protocol on top of the Hidden Matching problem, for which there exists an exponential gap in one-way communication complexity between classical and quantum strategies. In particular, by exploiting this exponential gap, we unlock the possibility of sending multiple copies of the same state to perform key establishment with performances that go beyond standard QKD.

In the last experimental project we investigate the feasibility of demonstrating a quantum advantage in communication complexity. In particular, we leverage the intricate mode mixing inherent in multimode fibers by employing wavefront shaping techniques to tackle quantum communication complexity problems.