Quantum cryptography in a hybrid security model

Nilesh Vyas

INSTITUT POLYTECHNIQUE DE PARIS

NNT : 2021IPPAT049

Thèse de doctorat

Quantum Cryptography in a Hybrid Security Model

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

École doctorale n°626 École doctorale IP Paris (ED IP Paris)
Spécialité de doctorat : Information, communications, électronique

Thèse présentée et soutenue à Palaiseau, le 21/12/2021, par

NILESH VYAS

Composition du Jury :

Alain COUVREUR INRIA	Président
Marco LUCAMARINI University of York	Rapporteur
Damian MARKHAM CNRS, Sorbonne University	Rapporteur
Marc-Olivier RENOU ICFO, Barcelona	Examinateur
Romain ALLEAUME Telecom Paris, Institut Polytechnique de Paris	Directeur de thèse

To my parents

Acknowledgements

The last four years in Paris, for my PhD, has been an eventful journey full of meaningful life experiences and adventurous surprises. I especially want to thank Telecom Paris, a great place to work, for providing me with a suitable work environment. I feel privileged and grateful to have the supportive and encouraging people around me at work and outside, who have guided me, inspired me, are fellow associates of my success, and encouraged me and pulled me up when I was down.

I want to express my sincere gratitude towards my thesis supervisor Prof. Romain Allèaume. He is an exceptional researcher and a very kind human being. I am thankful to him for his supportive guidance, patience, and persistence in pushing me to achieve perfection. Learning from his experience has been instrumental in making me a better scientist and person than I had imagined.

I am thankful to Prof. Isabelle Zaquine and Prof Filippo Miatto for their support and encouragement during my PhD. I am also grateful to my colleagues and friends at QIA, Raphaël Aymeric, Ravi Raghunathan, Francesco Mazzoncini, Yuan Yao, Guillaume Ricard, and Antoine Henry, for their support and countless technical, non-technical discussions in and outside the office. They all are very bright minds, and I wish them luck for their PhD.

I want to thank Prof. Marco Lucamarini, Prof. Damian Markham, Prof. Marc-Olivier Renou, and Prof. Alain Couvreur for kindly agreeing to be the jury members for my thesis.

I am grateful to the European Innovative Training Network QCALL (project 675662, funded by the Marie Sklodowska Curie Call H2020-MSCA-ITN-2015) for providing me with the funding to work on my PhD, allowing me to attend and present my work at different scientific schools, workshops and conferences. I am thankful to Prof. Mohsen Razavi, who has helped me to develop the time-limited quantum memory assumption, I visited at the University of Leeds for my secondment. I am grateful to all ESRs at QCALL for meaningful technical discussions and fun-filled times during various QCALL events.

I am incredibly thankful to Vaddina Kameswar Rao and Vamsi Krishna for their friendship and support to guide and show my ways when I first arrived in Paris. Along with them, I am also very grateful to my friends Prof. Keunwoo Lim, Dongmin Son, Wenqin Shao, and Yue Li for their support and interesting chats at lunchtime.

Outside work, I am grateful to have my close friends, specially Sidharth Sahdev, Gentle Dash, Shabbir Ali, Shovik Ghorai, Niraj Kumar, Praveer Singh, Mainak Jas, Aakanksha Rana, Hiba Yousef, Gabrysia Mozharovskyi, David Jan Mercado, Jonathan, Lucie, Tanuja Sawant, Pavel Mozharovsky, Kaushik, Srijani Mallik, Sougata Mallick, Sujit Panigrahi, Jiali, and Abhishek for making my stay in Paris extremely enjoyable and being a family. I am also grateful to my friends in India, Abhilash Chandra, Sunny Gautam, Jyotiraaditya Singh, Dheer Desai, Kaushal Gianchandani, Hardik, Chandra Prakash, and Sonam Kumari, who has been there for me whenever I needed them.

Lastly, I express my sincere gratitude and bow my head down to my family members, who have been a solid pillar of foundation in my life. I am thankful to them for supporting me in various paths of my life. Without their upbringing and blessing, I would not be where I am today.

Contents

List of publications and activities done during the PhD

Publications

- Nilesh Vyas, Romain Alléaume, Everlasting Secure Key Agreement with performance beyond QKD in a Quantum Computational Hybrid security model, arXiv:2004.10173

Conferences (talk and poster presentation)

- Oral Presentation: Journées Informatique Quantique 2017, 9 and 10 Novembre 2017 – Bordeaux, France
- Oral Presentation: QCALL Early-Stage Researchers Conference (ESRC), Mondello, Sicily, 16-19 September 2019.
- Oral Presentation: QCALL Final Symposium on Advances in Quantum Communications (Online), 2-5 May, 2021.
- Oral Presentation: The International Conference on Quantum Communication ICQOM 2021, Paris, France, 18-22 October 2021
- Poster Presentation: 15th Conference on the Theory of Quantum Computation, Communication and Cryptography. (Online conference)
- Poster Presentation: QCrypt 2020, 10-14 August. (Online conference)
- Poster Presentation: QCrypt 2019, 26-30 August, Montreal, Canada.
- Poster Presentation: QCrypt 2018, 27-31 August, Shanghai, China.
- Oral Presentation: QTech 2020 virtual edition, November 2-4, 2020. (Online conference)
- Poster Presentation: GDR IQFA – 11th Colloquium, December 2-4, 2020. (Online conference)

Summer school

- School of Quantum Secure Communications (SQSC) 7-11 May 2018, Baiona, Spain
- School of Quantum Communications Networks (SQCN) 19-22 September 2018, Padova, Italy

- QCALL Complementary-Skill Workshops CS1 on Project Management Was held in Leeds, 18-19 October 2017
- QCALL Complementary-Skill Workshops CS2 on Presentation Skills. Paduva Italy, 17-18 September 2018
- QCALL Complementary-Skill Workshops CS3 on Entrepreneurship. Mondello, Italy, 19-20 September 2019

Résumé en français

Introduction

Quantum Key Distribution (QKD) permet un accord de clé sécurisé avec une sécurité théorique de l'information. Cela contraste avec les protocoles d'accord de clé classiques, où la sécurité est basée sur des conjectures de dureté de calcul. QKD peut offrir *en principe* un avantage de sécurité distinctif par rapport aux techniques classiques, en particulier dans les contextes où la sécurité à long terme est recherchée.

Évaluer l'utilité de QKD pour servir des cas d'utilisation réels *en pratique* reste une question complexe et controversée. Elle a conduit à un débat d'autant plus difficile à trancher que des périmètres d'évaluation différents sont souvent envisagés [PPS04, ABB+14, MCG, oqst]. La difficulté de cette comparaison est également liée, dans une certaine mesure, à la diversité des objectifs poursuivis par les chercheurs et ingénieurs QKD. Ces objectifs sont principalement structurés autour de la dualité entre deux dimensions principales : la praticité (comment construire des systèmes QKD efficaces et rentables) et la sécurité (comment garantir un gain de sécurité adéquat par rapport aux techniques classiques existantes).

Des efforts considérables ont été investis pour faire des progrès sur les deux dimensions [PAB+20a]. Sur le plan pratique, des systèmes QKD présentant des performances accrues sont développés et déployés sur des réseaux optiques réels [PLL+09, SFI+11, DLQY16, ZXC+18]. Côté sécurité, un corpus de travaux stable et robuste pose les bases de la sécurité théorique de QKD [Ren05, SBPC+09, TL17]., tandis que la question de la sécurité de mise en œuvre est abordée avec des efforts dédiés [ML, XMZ+20] , ouvrant la voie à la certification des implémentations cryptographiques quantiques à court terme.

Malgré ces progrès remarquables, de nouvelles avancées décisives sont toutefois entravées. Cela est dû au problème récurrent que les aspects pratiques et de sécurité de QKD sont, dans une large mesure, abordés de manière disjointe, ce qui conduit à un dilemme. L'un des problèmes cruciaux de QKD est d'atteindre de longues distances à des taux raisonnablement élevés. D'une part, les compromis entre performances et coûts devraient guider l'ingénierie du système QKD. D'autre part, la recherche de la "sécurité ultime" contredit une telle approche. Ce constat a déjà été formulé il y a une dizaine d'années par Valerio Scarani et Christian Kurtsiefer dans leur " black paper on quantum cryptography" [SK14]. Ce dilemme, cependant, reste en suspens principalement aujourd'hui, entravant les progrès de QKD vers l'adoption et l'industrialisation à grande échelle.

Nous proposons une autre façon de résoudre le dilemme pratique de la cryptographie quantique. Notre approche consiste à concevoir un nouveau modèle de sécurité, le **Quantum Computational Timelock (QCT) security model**, qui tire parti de la sécurité informatique à court terme et du stockage quantique bruité pour améliorer les performances et la fonctionnalité de l'accord de clé basé sur le quantum. Fait intéressant, bien que notre modèle proposé soit plus faible que la sécurité inconditionnelle, il fournit néanmoins une *sécurité éternelle*, c'est-à-dire la sécurité de

l'établissement de la clé contre un adversaire sans limite de calcul, à condition qu'une communication cryptée éphémère initiale ne puisse pas être interrompue dans un court laps de temps. Comme la sécurité éternelle n'est pas réalisable à l'aide de constructions informatiques, notre approche hybride peut revendiquer un gain de sécurité strict par rapport aux techniques classiques, en plus d'étendre considérablement l'enveloppe de performance concernant la communication quantique sans répéteur, où des limites fondamentales limitent la capacité secrète.

En utilisant le modèle de sécurité QCT, nous proposons un protocole d'accord de clés que nous appelons **MUB-Quantum Computational Timelock** (MUB-QCT), où un bit est encodé sur l'état quantique de dimension d, en utilisant un ensemble complet de bases non biaisées (MUB) et un ensemble de permutations indépendantes par paires comme bases de codage. La sécurité du protocole est prouvée en calculant la borne sur l'information mutuelle de l'adversaire. Nous prouvons que la borne supérieure sur les échelles d'information d'Eve est $\mathcal{O}(1/d)$. Nous montrons les offres MUB-QCT : *haute résilience aux erreurs* (jusqu'à 50 $\%$ pour les gros d) avec des exigences matérielles fixes ; Sécurité indépendante de l'appareil de mesure (*MDI*), car la sécurité est indépendante de la surveillance des canaux et ne nécessite pas de faire confiance aux appareils de mesure. Nous prouvons également la sécurité du protocole MUB-QCT, avec plusieurs photons par utilisation de canal, contre deux scénarios d'écoute clandestine restreints où Eve mesure chaque copie individuellement en utilisant une mesure optimale fixe ou mesure de manière proactive chaque copie dans un MUB différent suivi d'une post-mesure classique décodage. Nous prouvons que le protocole MUB-QCT permet une distribution sécurisée des clés avec des états d'entrée contenant jusqu'à $O(d)$ photons, ce qui implique une amélioration significative des performances, caractérisée par une multiplication $O(d)$ du taux de clé. Nous affirmons que le protocole que nous considérons ici offre : une haute résilience aux erreurs, une garantie de sécurité qui ne nécessite pas de confiance dans la mise en œuvre du dispositif de mesure, et une haute tolérance à la perte de canal subie sur de longues distances.

Notre travail est en particulier lié au *Verrouillage des données quantiques* [LL14, LL15a] où la sécurité contre un adversaire avec une mémoire quantique limitée dans le temps peut être prouvée en majorant les informations accessibles [LL15b]. Cependant, les travaux existants sur le verrouillage des données quantiques sont limités au codage à photon unique [LL14] et ne peuvent pas étendre la distance ou recourir à des constructions basées sur des arguments de codage aléatoires [LL15a] pour lesquels une mise en œuvre pratique avec une mesure structurée n'est pas possible.

Modèle de sécurité Quantum Computational Timelock :

Comme proposé en 2015 [All15] un nouveau modèle de sécurité que nous avons plus tard inventé comme modèle de sécurité **Quantum Computational Timelock** (QCT). Il est représenté sur la figure 1 et se compose de deux hypothèses imbriquées :

1. Alice et Bob sont supposés avoir accès à une chaîne classique publique authentifiée et à un schéma de chiffrement qui est informatiquement sécurisé vis-à-vis de tout attaquant non autorisé Eve pendant un temps au moins t_{comp} après l'échange d'un texte chiffré sur le canal classique.

2. La mémoire quantique d-dimensionnelle d'Eve est t_{coh}-décohérante avec $t_{coh} << t_{comp}$. Considérant la mémoire quantique comme un canal, elle peut être écrite comme une carte positive complète et dépendante du temps $\mathcal{N}_t : \rho \to \mathcal{N}_t(\rho)$, tel que défini dans l'équation 5.2.

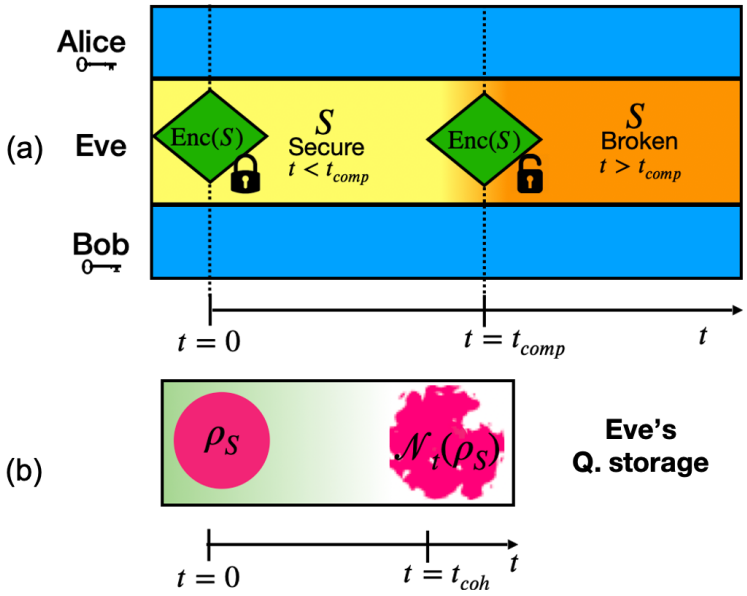


Figure 1: Modèle de sécurité QCT : Hypothèse (a) : Chiffrement sécurisé à court terme pendant le temps t_{comp}, pendant lequel Alice et Bob peuvent échanger un secret classique éphémère S. Hypothèse (b) : Mémoire quantique limitée dans le temps, avec temps de cohérence $t_{coh} << t_{comp}$

.

Il est intéressant de noter que ces deux catégories d'hypothèses, à savoir la sécurité computationnelle à court terme [Unr15b] et le stockage quantique bruité [KWW12b], ont jusqu'à présent déjà été considérées en cryptographie quantique, mais seulement de manière disjointe.

Dans le modèle de sécurité QCT, nous avons besoin d'une authentification initiale entre Alice et Bob, (voir la section 6.2 où le protocole d'établissement de clé basé sur le modèle de sécurité QCT est décrit). Cette authentification initiale peut être basée sur un canal authentifié (ce qui est alors une hypothèse). Une autre alternative nécessite la distribution d'un secret partagé (avec une authentification correcte) pour authentifier les communications sur un canal public. Dans ce dernier cas, l'hypothèse porte alors sur la possibilité de partager un secret initial, avec authentification.

Nous voulons définitivement que le schéma de cryptage soit sécurisé à court terme contre un ordinateur quantique. Cependant, nous n'avons pas précisé le type de schémas de chiffrement qui peuvent être pris en compte dans les hypothèses du modèle QCT. Nous pouvons affiner cette hypothèse du modèle QCT en considérant que le chiffrement sécurisé à court terme (qu'il soit basé sur un schéma symétrique ou asymétrique) est quantique sécurisé, c'est-à-dire sécurisé contre un ordinateur quantique. Malheureusement, il n'existe aucune construction connue pour les schémas de chiffrement à clé publique qui soient sécurisés (même sécurisés à court terme) contre un ordinateur quantique. Alors que les schémas de cryptage à clé secrète et les algorithmes de hachage sont connus pour offrir une sécurité contre un ordinateur quantique avec une grande confiance.

Le modèle de sécurité QCT explore un espace d'hypothèses, à savoir un monde dans lequel les schémas de chiffrement ne seraient pas sécurisés à long terme mais pourraient toujours être utilisés à court terme. Deuxièmement, les mémoires quantiques optiques sont technologiquement liées à la décohérence dans un délai plus court que lorsque le schéma de chiffrement est sécurisé. L'objectif de ce modèle de sécurité est de construire des protocoles cryptographiques capables d'augmenter les performances de la cryptographie quantique au-delà des limites de performances fondamentales [PLOB17a, TGW14], qui pourraient être trop restrictives pour une utilisation dans le monde réel

[Sas17].

Validity: Une limite inférieure pratique sur la valeur de t_{comp} peut être déduite de la sécurité à long terme supposée du schéma de chiffrement AES256, qui est considéré comme répondant aux exigences de confidentialité à long terme (30 ans) des données Top Secret [Hat03].

En ce qui concerne le temps de cohérence de la mémoire quantique adressable optiquement, comme examiné dans la section ci-dessus, des démonstrations expérimentales de stockage puis de récupération d'informations quantiques codées optiquement, au niveau du photon unique. Cela indique que la valeur de t_{coh} varie de quelques nanosecondes à microsecondes [SAA+10].

Étant donné le grand écart entre la borne supérieure sur t_{coh} et la borne inférieure sur t_{comp}, la validité du modèle de sécurité QCT peut être supposée avec une très grande confiance aujourd'hui. Cela laisse également une marge considérable pour sa validité dans le futur. Enfin, il convient de noter que le but ici est de construire un protocole de distribution de clés avec une sécurité éternelle, ce qui signifie en particulier que la validité du modèle de sécurité QCT ne doit être maintenue qu'au moment de l'exécution du protocole pour fournir une sécurité théorique de l'information dans l'avenir. Une comparaison de l'efficacité et du temps de cohérence de différents systèmes de mémoire quantique optique est présentée dans le tableau [5.1]. Ainsi, en supposant, par exemple, $t_{comp} = 10^5\, s \sim 1\,\mathrm{day}$, laisse une marge de sécurité raisonnable par rapport à l'état de l'art des capacités de stockage quantique, comme indiqué dans la Figure 5.2.

Protocol	**Information per channel use**	**Error-tolerance**	**Number of detectors**	**Trust assumptions on the hardware**
(P&M) HD-QKD	$\log_2 d$ bits	$\leq 50\%$ for large d	d	All devices in Alice and Bob's lab are trusted.
MUB-QCT	1 bit	$\leq 50\%$ for large d	2	Bob's measurement device does not need to be trusted.

Table 1: Comparison of the prepare and measure HD-QKD with the MUB-QCT protocol.

Distribution de la clé MUB-QCT dans le modèle de sécurité QCT :

nous discutons du protocole d'établissement de clé en utilisant le modèle de sécurité QCT. Nous présentons d'abord un cadre générique pour construire un protocole d'établissement de clés à d-dimensions. Nous proposons ensuite un protocole d'accord de clé, que nous appelons **MUB-Quantum Computational Timelock**(MUB-QCT).

Paramètres : Le protocole de distribution de clé m-MUB-QCT-(b, c) est paramétré par les paramètres suivants

- b : nombre de bits encodés sur un état quantique de dimension d.
- c : la capacité classique de l'encodage.
- m : nombre de copies de l'état du qudit envoyées par utilisation du canal.

Ingrédients : Un élément essentiel du protocole MUB-QCT consistera à randomiser l'un des états de base d'un espace de Hilbert à d-dimensions à l'aide d'un ensemble d'unités :

- Un ensemble complet de $d+1$ bases mutuellement non biaisées (MUB), dans la dimension d.
- Un ensemble complet de permutations indépendantes par paires.

Différents protocoles : En fonction du nombre de bits encodés sur un état quantique de dimension d et du nombre de copies de l'état qudit envoyées par canal utilisé, nous proposons différentes versions du protocole MUB-QCT.

- Dans la section 6.3.1, nous proposons le protocole 1-MUB-QCT-$(\log d, \log d)$, où pour une seule copie de l'état quantique envoyé par canal utiliser $\log d$ les bits sont encodé sur un qudit, en utilisant un ensemble complet de MUB.
- Dans la section 6.3.2 nous proposons le protocole 1-MUB-QCT-$(1, \log d)$, où pour une seule copie d'état quantique envoyée par canal, un bit est encodé sur un qudit, en utilisant un ensemble de MUBS et un ensemble complet de permutations indépendantes par paires.
- Dans la section 6.3.3, nous proposons le protocole MUB-QCT avec plusieurs copies par utilisation de canal, à savoir m-MUB-QCT-$(\log d, \log d)$ et le protocole m-MUB-QCT-$(1, \log d)$.

Ingrédients : Le protocole se compose de deux phases ;

- *Setting a computational timelock :* Alice et Bob partagent une information secrète $s \in \mathcal{S}$ (une information secrète classique correspondant à l'encodage unitaire) sur un canal de communication classique utilisant t_{comp}- schéma de cryptage sécurisé. Pour le protocole 1-MUB-QCT-$(\log d, \log d)$, s correspond à l'indice de la base mutuellement non biaisée, tandis que pour le 1-MUB-QCT-$(1, \log d\ )$, il correspond à l'indice de la base mutuellement non biaisée et à la permutation utilisée pour coder le bit classique sur le qudit.
- *Communication quantique :* Alice encode un bit $x \in \mathcal{X}$ sur un état quantique de d-dimensions en utilisant s comme

$$\rho_x = \frac{1}{|s|} \sum_s \rho_{xs} \tag{1}$$

  Alice envoie l'état ρ_x à Bob via un canal quantique non sécurisé, qui décode le bit en effectuant une mesure projective sur ρ_x, en utilisant s, et obtient $y \in \mathcal{Y}$.

Eve est supposée avoir un accès complet à l'entrée des canaux de communication d'Alice et Bob (similaire au verrouillage fort des données quantiques [Lup15]). Cependant, Eve ne peut pas casser le chiffrement timelock avant t_{comp}. De plus, elle ne peut pas stocker l'état ρ_x plus longtemps que t_{coh}. Eve ne peut utiliser qu'une seule des stratégies suivantes :

- **(I)** Eve stocke l'état quantique d'entrée ρ_x dans son stockage quantique et effectue ensuite une mesure au temps t_{comp}, connaissant le secret s, pour obtenir $z \in \mathcal{Z}$.

- **(II)** Eve effectue une mesure immédiate sur l'état d'entrée ρ_x et obtient un résultat classique ω. Au temps t_{comp}, elle effectue un décodage classique post-mesure en utilisant s et ω pour obtenir $z \in \mathcal{Z}$.

La sécurité des protocoles :

La sécurité des protocoles est prouvée en démontrant que sous les hypothèses QCT, la stratégie d'attaque optimale pour la partie non autorisée Eve consiste en une mesure immédiate suivie d'un post-traitement classique sur les données de mesure, c'est-à-dire la stratégie II. Cette stratégie est connue sous le nom de discrimination d'état avec des informations post-mesure comme décrit dans [GW10].

Pour les protocoles 1-MUB-QCT-$(\log d, \log d)$ et 1-MUB-QCT-$(1, \log d)$, nous prouvons que la stratégie d'écoute optimale est II. Pour le 1-MUB-QCT-$(\log d, \log d)$, nous prouvons que la probabilité de deviner pour Eve si elle exécute la stratégie II est $\mathcal{O}\left(\frac{1}{\sqrt{d}}\right)$. Pour le protocole 1-MUB-QCT-$(1, \log d)$, nous montrons qu'Eve n'a pas de choix préférable pour la mesure immédiate car l'ensemble complet des MUB forme un 2-design [GKR]. En conséquence, nous pouvons prouver que cette deuxième stratégie réduit, pour Eve, à accéder à la sortie d'un fort QC-extractor [BFW14] basé sur un ensemble complet de MUBs, et donc que sa probabilité de deviner est $\frac{1}{2} + \mathcal{O}\left(\frac{1}{d}\right)$.

À la fin du protocole MUB-QCT, Alice et Bob détiennent des variables aléatoires classiques X et Y, tandis qu'Eve détient une variable aléatoire classique Z et une mémoire quantique décohérée. La formule Csiszár et Körner [CK78a] $R \geq I(X;Y) - I(X;Z)$ peut donc être appliquée pour dériver la clé sécurisée taux. Prouver la sécurité du protocole MUB-QCT nécessite donc de borner les informations mutuelles d'Eve $I(X;Z)$. Étant donné que II est la meilleure stratégie, nous pouvons utiliser la probabilité de deviner pour calculer une borne sur l'information mutuelle d'Eve. Nous prouvons que pour le protocole 1-MUB-QCT-$(\log d, \log d)$ $I(X;Z) \sim \mathcal{O}(1/\sqrt{d})$, alors que pour -MUB-QCT-$(1, \log d)$ protocole $I(X;Z) \sim \mathcal{O}(1/d)$.
Très particulièrement, les informations liées à Eve peuvent être obtenues sous le modèle de sécurité QCT, en ne considérant que l'état d'entrée et non les résultats de la mesure de Bob.

Analyse de sécurité :

À la fin du protocole MUB-QCT, Alice et Bob détiennent des variables aléatoires classiques X et Y, tandis qu'Eve détient une variable aléatoire classique Z et une mémoire quantique décohérée. La formule Csiszár et Körner [CK78a] $R \geq I(X;Y) - I(X;Z)$ peut donc être appliquée pour dériver la clé sécurisée taux. Prouver la sécurité du protocole MUB-QCT nécessite donc de borner les informations mutuelles d'Eve $I(X;Z)$. Étant donné que II est la meilleure stratégie, nous pouvons utiliser la propriété d'extraction forte de [BFW14] pour prouver que $I(X;Z) \sim \mathcal{O}(1/d)$.
Très particulièrement, les informations liées à Eve peuvent être obtenues dans le cadre du modèle de sécurité QCT, en ne considérant que l'état d'entrée et non les résultats de la mesure de Bob.

Analyse des performances :

- **Tolérance au bruit :** Le codage à haute dimension dans le protocole MUB-QCT permet une grande résilience au bruit en offrant un taux d'erreur maximal tolérable allant jusqu'à 50 $\%$ pour les gros d.
- **Resources requises :** Le protocole MUB-QCT peut être implémenté avec seulement deux détecteurs, indépendamment de d . Cela assouplit les besoins en ressources par rapport aux schémas HD-QKD [LPD+13, LBZ+16a], nécessitant d-détecteurs à photon unique.
- **Sécurité MDI :** Dans le protocole MUB-QCT, les informations d'Eve ne peuvent être limitées qu'en considérant l'état saisi par Alice. Par conséquent, la mise en œuvre du dispositif de mesure de Bob n'a pas besoin d'être fiable pour garantir la sécurité.

MUB-QCT avec plusieurs copies d'états quantiques :

Les protocoles précédents traitaient d'une copie de ρ_x encodée sur un seul photon. Nous explorons également si le protocole MUB-QCT offre une tolérance élevée à la perte de canal subie sur de longues distances en transmettant plusieurs photons par utilisation de canal. Alice prépare m copies de l'état qudit, ρ_x, en utilisant la même base θ. Nous prouvons la sécurité sous deux stratégies d'attaque restreintes pour Eve ;

1. **Attaque individuelle :** où Eve est limitée à effectuer la même mesure fixe individuelle sur chacune des m copies.
2. **Mesure MUB proactive :** où Eve mesure de manière proactive chaque copie séparément sur une base différente, choisie parmi l'ensemble complet de MUB, suivie d'un décodage post-mesure après le temps t_{comp}.

Nous prouvons que pour le protocole m-MUB-QCT-$(1, \log d)$, la mesure MUB proactive est plus efficace que la stratégie d'attaque individuelle. Dans le cas d'une stratégie d'attaque individuelle, les informations mutuelles d'Eve peuvent être limitées comme $I^{\mathrm{Fix}}(X;Z)_m \leq \mathcal{O}\left(\frac{\sqrt{m}}{d}\right)$, tandis que pour la mesure MUB proactive, les informations mutuelles d'Eve augmentent linéairement avec m comme $I^{\mathrm{Pro}}(X;Z) \sim \mathcal{O}(m/j)$.

Pour le protocole m-MUB-QCT-$(\log d, \log d)$, nous prouvons que la stratégie d'attaque individuelle est plus efficace que la mesure MUB proactive. Dans le cas d'une stratégie d'attaque individuelle, les informations mutuelles d'Eve peuvent être limitées comme $I^{\mathrm{Fix}}(X;Z)_m \leq \mathcal{O}\left(\frac{\sqrt{m}}{\sqrt{d}}\right)$, tandis que pour la mesure MUB proactive, les informations mutuelles d'Eve augmentent linéairement avec m comme $I^{\mathrm{Pro}}(X;Z) \sim \mathcal{O}(m/j)$.

Le protocole MUB-QCT offre les avantages suivants :

- **Tolérance au bruit :** Le codage à haute dimension dans le protocole MUB-QCT permet une grande résilience au bruit en offrant un taux d'erreur maximal tolérable allant jusqu'à 50 $\%$ pour les gros d.
- **Resources requises :** Le protocole MUB-QCT peut être implémenté avec seulement deux détecteurs, indépendamment de d . Cela assouplit les besoins en ressources par rapport aux schémas HD-QKD [LPD+13, LBZ+16a], nécessitant d-détecteurs à photon unique.

- **Sécurité MDI :** Dans le protocole MUB-QCT, les informations d'Eve ne peuvent être limitées qu'en considérant l'état saisi par Alice. Par conséquent, la mise en œuvre du dispositif de mesure de Bob n'a pas besoin d'être fiable pour garantir la sécurité.

La stratégie de mesure proactive du MUB apparaît plus efficace que la mesure fixe à copie unique. Il permet néanmoins une distribution sécurisée des clés avec des états d'entrée contenant jusqu'à $O(d)$ photons, ce qui implique une augmentation significative des performances, caractérisée par une $O(d)$-**multiplication des taux de clé** comme indiqué dans la figure 9.3. La possibilité d'envoyer plusieurs copies de l'état quantique par utilisation de canal peut en outre être exploitée pour réaliser **distribution de clé multipartite**. En principe, Alice peut transmettre m copies à jusqu'à m Bobs autorisés, leur permettant de distiller la même clé.

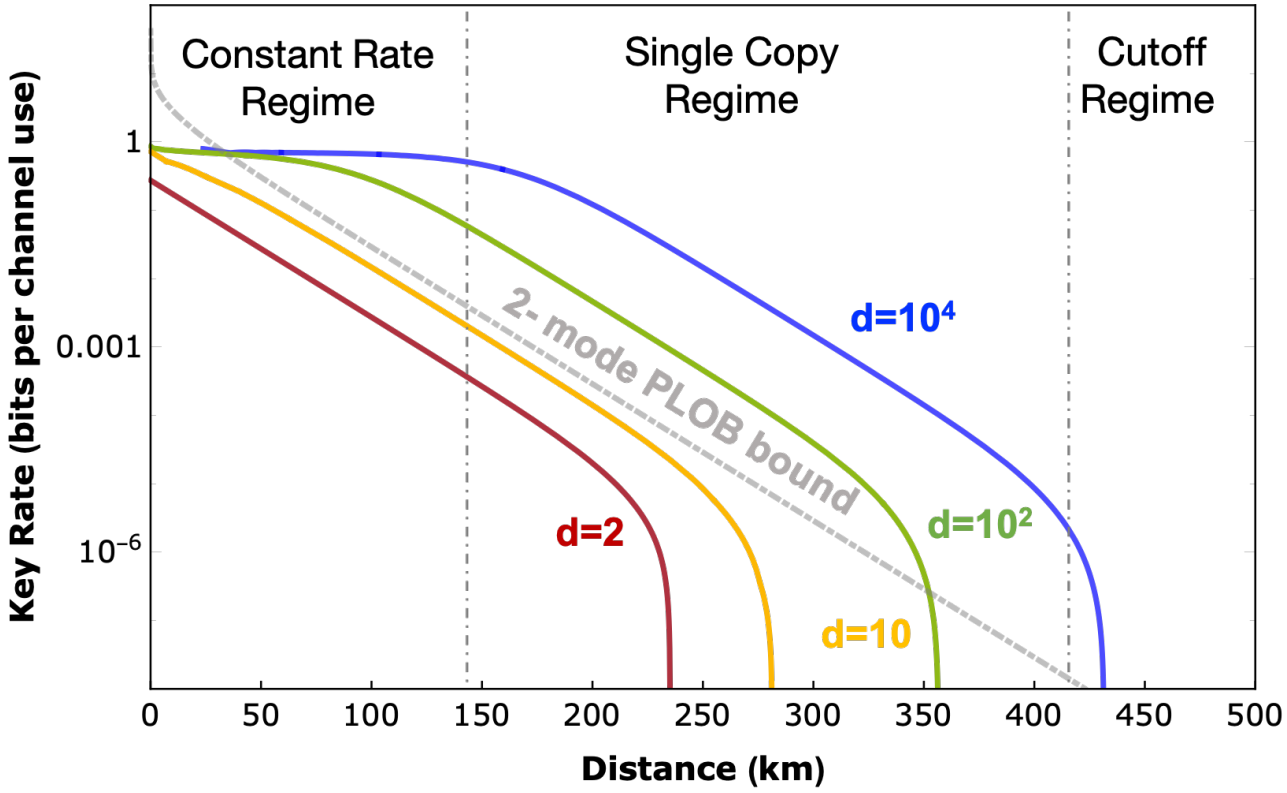


Figure 2: Key rate per channel use as a function of distance, for proactive MUB measurement strategy. The key rates are maximized against the photon number m. The parameters assumed in the plots are: Loss 0.2dB/Km; $P_{dark} = 10^{-6}$; efficiency of detectors $\eta = 25\%$; visibility $V = 98\%$. Since MUB-QCT can be implemented with 2 detection modes (2-single photon detectors) we also plot 2-modes PLOB bound [PLOB17a] as a benchmark..

Conclusion :

Nous avons proposé un nouveau modèle de sécurité *Quantum Computational Timelock* (QCT), où nous supposons qu'un schéma de chiffrement est informatiquement sécurisé pendant une durée supérieure au temps de décohérence des mémoires quantiques.
Nous construisons le protocole de distribution de clés MUB-QCT en utilisant un ensemble complet

de bases mutuellement non biaisées (MUB) et prouvons la sécurité en limitant les informations d'Eve sous la forme $I(X;Z) \sim \mathcal{O}(1/d)$, pour la stratégie d'attaque d'écoute optimale, qui réduit l'accès à la sortie d'un extracteur QC puissant. De plus, lorsqu'Alice envoie plusieurs copies par canal, les informations d'Eve sous des mesures MUB proactives restrictives sont délimitées par $I^{\mathrm{Pro}}(X;Z) \sim \mathcal{O}(m/d)$. En conséquence, offrant une *haute résilience aux erreurs* (jusqu'à 50 $\%$ pour les gros d) avec des exigences matérielles fixes, une sécurité *indépendante de l'appareil de mesure* (MDI) qui assouplit certaines contraintes d'ingénierie importantes concernant textitdistribution quantique des clés (QKD), et $O(d)$ multiplication des taux clés.
Notre travail est en particulier lié au *verrouillage quantique des données* [LL14, LL15a] où la sécurité contre un adversaire avec une mémoire quantique limitée dans le temps peut être prouvée en majorant l'information accessible [Lup15]. Cependant, les travaux existants sur le verrouillage des données quantiques sont limités au codage à photon unique [LL14] et ne peuvent pas étendre la distance ou recourir à des constructions basées sur des arguments de codage aléatoires [LL15a] pour lesquels une mise en œuvre pratique avec une mesure structurée n'est pas possible.
Nos résultats illustrent que les approches hybrides de la cryptographie quantique constituent une voie prometteuse et pratique pour étendre les performances et les fonctionnalités de la cryptographie quantique. En particulier, notre nouveau protocole MUB-QCT permet l'établissement d'une clé de sécurité permanente - non réalisable avec des moyens classiques - avec des performances nettement supérieures à celles de QKD.

Introduction

Cryptography

The Internet is the global system of interconnected computer networks consisting of private, public, academic, business, and government local to global scope, linked by a broad array of electronic, wireless, and optical networking technologies. Since the rise of the Internet, people worldwide have found themselves able to communicate with anyone at any time. Any message is transformed into a binary string and sent through different means of telecommunication (satellite, fibre, etc.) over the internet network.

The World Wide Web ("WWW" or "The Web") is a global information medium that users can access via computers connected to the Internet. Have you ever wondered what is *http://* or *https://* in front of the "WWW" of any website address? Well, HTTP is the abbreviation for hypertext transfer protocol. This is the primary method by which the data of web pages are transferred over a network. Web pages are stored on servers, then served to the client computer as the user accesses them. The resulting network of these connections creates the world wide web as we know it today. Without HTTP, the world wide web (WWW) as we know it would not exist. However, this powerful technology comes at a price. Whoever would tamper with the communication link would find himself able to read whatever message is passing through it, and if confidential or sensitive information is needed to be transferred, this will imply an impossibility to use such a link. For this reason, each message sent in the network must be encoded so that only the transmitter and receiver of the information will be able to read it.

HTTPS is the abbreviation for hypertext transfer protocol secure or secure hypertext transfer protocol. Unlike HTTP, HTTPS uses a secure certificate to secure a connection and verify that the site is legitimate. For example, when one wants to secure the transmission of credit card data or other sensitive information (such as someone's actual address and physical identity) or when you run a lead generation website that relies on someone's accurate information, in which case you want to use HTTPS to safeguard against malicious attacks on the user's data.

How to secure a message by encrypting it is the topic of interest of Cryptography. The art of hiding a message has been around for millennia. Nowadays, the most common encoding schemes are the so-called public-key schemes, where a service provider broadcasts a public key, and anyone with it could encode a message. However, the only one able to read it is the possessor of the private key. Meaning that the communication can be left secure if the private key is kept secret. These protocols, however, rely on the assumption that the computational power of a possible eavesdropper is limited. In fact, in principle, from the public key, it would be possible to retrieve the private one; the task is, however, computationally challenging, and it is usually set such as no current technology could crack it in a reasonable time. This means that the security of public-key encryption schemes does not rely only on the privacy of the private key but also on the limitation of the technology of a possible adversary.

One Time Pad offers one solution to this problem as it requires only the privacy of a private key in order to be perfectly secure. It works as follows: two honest parties have a secret key k (a binary string of dimension n). One of the two can then encode a message m (of dimension n) just by applying an XOR operation between the two strings and sending the resulting cyphertext $c = k + m$ (modulo 2) through the channel. If k is private, it will be known only by the two honest users and look entirely random for any other communication listener. This fact is also translated for c, meaning that the cyphertext look like a random string to anyone oblivious to the original key. This protocol seems to solve all the problems of the previous public-key encryption scheme. However, there are significant constraints that must be respected for it to work.

- The key is at least as long as the message or data that must be encrypted.
- The key is truly random (not generated by a simple computer function or such)
- The key is used only once, and both sender and receiver must destroy their key after use. (from this, the name One Time Pad).
- There should only be two copies of the key: one for the sender and one for the receiver, i.e., the key must own by the two honest parties.

Since each key can be used only once, each communication round must generate a new key. Randomness moreover must be ensured so that no one could foresee which key is produced. However, classical physics is deterministic, meaning that knowing the initial conditions of a system would result in knowing the results of the whole process, which means that we need another theory to guarantee the randomness of the generated key.

On the other hand, the key in the one-time pad should have the same length as the message and be private once generated. This means that the two honest parties must exchange the key beforehand and keep it secret. Nevertheless, how can they share it if they are far from each other? Should they meet and exchange it before? If this were the case, they would as well exchange the message itself! Unfortunately, classical information theory does not help in this regard. We need a new physics in order to do it as in the previous case.

What happens when quantum physics meets cryptography?

The word "quantum" comes from the Latin for "how much" and refers to counter-intuitive properties of subatomic particles discovered beginning in the late 1800's and early 1900's CE. The field arose from the study of electromagnetism, where physicists found that electromagnetic waves such as light beams can be described both as waves and as streams of discrete particles, or "quanta". It turns out that the universe behaves in apparently contradictory ways when studied at the sub-atomic level. The physicist Richard Feynman stated that it is impossible to understand quantum mechanics due to the paradoxical ways the universe behaves at the subatomic level.

While it is challenging to understand quantum mechanics in the "commonsense" way we can understand classical, everyday physics, given the paradoxical results found at the subatomic level, it is still worthwhile to study. However, both for better understanding of the universe and promising applications the field offers for technology. Let us look at a few examples of basic principles of quantum mechanics to get a taste of the paradoxical ways the universe behaves at the quantum level.

1. **Superposition:** Quantum superposition is a fundamental principle of quantum mechanics. In classical physics, a wave describing a musical tone can be seen as several waves with different frequencies added together, superposed. Similarly, a quantum state in superposition can be seen as a linear combination of other distinct quantum states. This quantum state in superposition forms a new valid quantum state. The superposition principle is that a system is in all possible states simultaneously until it is measured. After measurement, it falls to one of the basis states that form the superposition, thus destroying the original configuration. The superposition principle explains the "quantum weirdness" observed with many experiments.

2. **Uncertainty principle:** The uncertainty principle also called the Heisenberg Uncertainty Principle, or Indeterminacy Principle was articulated (1927) by the German physicist Werner Heisenberg. This principle states that a conjugate pair of variables or properties, both values, cannot be precisely defined simultaneously for quantum objects. The most well-known pair is position and momentum (momentum being the mass times the particle's speed). Quantum particles, therefore, cannot have a precisely specified speed and exactly specified position at the same time. Consequently, another feature of quantum mechanics is that a measurement technique interferes with the system, thus changing its state.

3. **No-cloning theorem:** In quantum physics, the no-cloning theorem states that it is impossible to perfectly clone an unknown quantum state (the information content of the state) using unitary evolution. Even if one allows non-unitary cloning devices, the cloning of non-orthogonal pure states remains impossible unless one is willing to tolerate a finite loss of fidelity in the copied states. It is pretty standard that we could make precisely the duplicate copy of something in the classical world. However, in the quantum world, the laws of physics impose a severe restriction on copying: It is impossible to make a perfect copy of an unknown state.

4. **Randomness:** Quantum mechanics has randomness as a fundamental element of the theory. This is in contrast with classical mechanics models, where, the randomness is seen as the lack of knowledge. The evolution of a quantum mechanical state is not deterministic, and starting from the same conditions, one may end up with different results. Note that this is not due to the imprecision of the measurement device but rather an intrinsic property of quantum mechanics.

5. **Quantum entanglement:** The most striking and counter-intuitive feature of quantum mechanics is entanglement. This feature has no analogue in classical mechanics. Entanglement refers to the correlations among two or more quantum states, stronger than any possible classical correlations. Experiments and theoretical developments have shown that two subatomic particles can become "entangled" in such a way that, when a given property of one of the particles is observed, the opposite state will then be observed in the second particle regardless of the distance between the two. Quantum entanglement is a natural phenomenon that occurs when two particles originate at the same point in space and time, for example.

We have taken an overview of the preliminary results of quantum mechanics, the branch of physics that studies the universe's properties at the subatomic level. We now see how to use this to develop a cryptographic scheme that is secure against eavesdropping.

Quantum cryptography is one of the emerging topics in the field of the computer industry. It is a science that applies principles of quantum mechanics to data encryption and data transmission so that data cannot be accessed by hackers – even by those malicious actors that have quantum

computing of their own. Rather than depending on the complexity of factoring large numbers, quantum cryptography is based on quantum mechanics' fundamental and unchanging principles. Quantum cryptography rests on two pillars of 20th-century quantum mechanics – the Heisenberg Uncertainty principle and the no-cloning theorem. These principles allow two (or more) distant users to exchange a secret message by encoding it in the states of quantum systems and transmitting the systems between each other. Any tampering with the quantum transmission by an eavesdropper would necessarily change the state of the systems and thus be detected. This establishes one of the main differences between classical and quantum cryptography: in the latter, it is physically impossible to build a quantum cloning machine, that is, a machine able to clone the state of a quantum system in two perfect copies.

The broader application of quantum cryptography also includes creating and executing various cryptographic tasks using quantum computers' unique capabilities and power. Theoretically, quantum computers can aid the development of new, more robust, more efficient encryption systems that are impossible using existing, traditional computing and communication architectures.

Quantum key distribution

Quantum cryptography, or more specifically, quantum key distribution (QKD), promises in principle unconditional security - the Holy Grail of communication security based on the laws of physics only. Unconditional security means security against an Eve who is not limited by computational assumptions but only by physics laws. QKD is a unique solution to long-term security since, in principle, it offers security for eternity. Unlike conventional cryptography, which allows Eve to store a classical transcript of communications, in QKD, there is no classical transcript for Eve to store once a quantum transmission is done.

Suppose Alice would like to send a secret message to Bob through an open communication channel to a receiver. Encryption is needed. If they share a standard string of secret bits, called a key, Alice can use her key to transform a plaintext into a cyphertext, which is unintelligible to Eve. In contrast, Bob, with his key, can decrypt the cyphertext and recover the plain text. In cryptography, the security of a crypto-system should rely solely on the secrecy of the key. The question is: how to distribute a key securely? In conventional cryptography, this is often done by trusted couriers. Unfortunately, in classical physics, couriers may be bribed or compromised without the users noticing it. This motivates the development of quantum key distribution (QKD).

A generic "prepare and measure" QKD protocol can be divided into two main steps: quantum communication followed by classical post-processing. The sender (Alice) encodes random classical variable α into non-orthogonal quantum states during quantum communication. These states are sent over a quantum channel (optical fibre, free-space link) controlled by the eavesdropper (Eve), who tries to steal the encoded information linearity of quantum mechanics forbids to perform perfect cloning that Eve can only get partial information while disturbing the quantum signal. At the output of the communication channel, the receiver (Bob) measures the incoming signals and obtains a random classical variable β. After several uses of the channel, Alice and Bob share raw data described by two correlated variables α and β.

The remote parties use part of the raw data to estimate the channel's parameters, such as its transmissivity and noise. This parameter estimation stage is essential to evaluate the amount of post-processing to extract a private shared key from the remaining data. Depending on this information, they perform a stage of error correction, which allows them to detect and eliminate errors, followed by a stage of privacy amplification that reduces Eve's stolen information to a negligible amount.

The final result is the secret key.

Depending on which variable is guessed, we have direct or reverse reconciliation. In direct reconciliation, it is Bob that post-process its outcomes in order to infer Alice's encoding. This procedure is usually assisted by employing forward CC from Alice to Bob. By contrast, in reverse reconciliation, Alice post-processes her encoding variable to infer Bob's outcomes. This procedure is usually assisted by a final round of backward CC from Bob to Alice. Of course, one may more generally consider two-way procedures where the extraction of the key is helped by for and feedback CCs, which may be even interleaved with the various communication rounds of the protocol.

Let us remark that there may also be an additional post-processing routine, called sifting, where the remote parties communicate to agree on instances while discarding others, depending on the measurement bases they have independently chosen. In DV protocols, random switching is between the Z -basis and X -basis, and in CV protocols, the homodyne detection switching between the q and the p quadrature.

Sometimes QKD protocols are formulated entanglement-based representation. This means: that Alice' preparation of the input ensemble of states is replaced by an entangled state Ψ_{AB} part of which is measured by Alice. The measurement on part A affects to prepare a state on part B conditionally. The outcome of the measurement one-to-one with the classical variable encoded in the prepared states. This representation is beneficial for the study of QKD protocols so that their prepare and measure formulation is replaced by an entanglement-based formulation for assessing the security and deriving the secret key rate.

Practical challenges in quantum key distribution

Quantum Key Distribution (QKD) enables secure key agreement with information-theoretic security. This is in contrast with classical key agreement protocols, where security is based on computational hardness conjectures. QKD can offer *in principle* a distinctive security advantage over classical techniques, in particular in contexts where long-term security is sought.

Assessing the usefulness of QKD to serve real-world use cases *in practice* remains a complex and disputed question. It has led to a debate that is all the more difficult to settle that different assessment perimeter are often considered [PPS04, ABB+14, MCG, oqst]. The difficulty of this comparison is also related, to some extent, to the diversity of the goals pursued by QKD researchers and engineers. These goals are mainly structured around the duality between two main dimensions: practicality (how to build efficient and cost-effective QKD systems) and security (how to guarantee an adequate security gain with respect to existing classical techniques).

Significant efforts have been invested in making progress on both dimensions [PAB+20a]. On the practical side, QKD systems that exhibit increased performances are being developed and deployed over real-world optical networks [PLL+09, SFI+11, DLQY16, ZXC+18]. On the security side, a stable and robust body of work lays the foundations of the theoretical security of QKD [Ren05, SBPC+09, TL17]., while the question of implementation security is tackled with dedicated efforts [ML, XMZ+20], paving the way towards the certification of quantum cryptographic implementations in the near-term.

Despite this remarkable progress, further decisive advancements are, however, hindered. This is due to the recurring issue that practicality and security aspects of QKD are, to a large extent, tackled disjointly, leading to a dilemma. One of the crucial problems in QKD is to achieve long distances at reasonably high rates. On the one hand, trade-offs between performance and cost are expected to drive QKD system engineering. On the other hand, the quest for 'ultimate security"

contradicts such an approach. This observation has already been voiced a decade ago by Valerio Scarani and Christian Kurtsiefer in their "black paper on quantum cryptography" [SK14]. This dilemma, however, remains unsettled mainly today, hampering QKD progress towards large-scale adoption and industrialization.

Our contribution: Results presented in this Thesis

We propose an alternative way to address the practical quantum cryptography dilemma. Our approach consists in devising a new security model, the **Quantum Computational Timelock (QCT) security model**, that leverages short-term computational security and noisy quantum storage to boost the performance and functionality of quantum-based key agreement. Interestingly, although our proposed model is weaker than the unconditional security, yet it provides *everlasting security*, i.e., security of key establishment against a computationally unbounded adversary, provided an initial ephemeral encrypted communication cannot be broken within a short time. As everlasting security is not achievable using computational constructions, our hybrid approach can claim a strict security gain compared to classical techniques, in addition to significantly extending the performance envelope concerning repeaterless quantum communication, where fundamental bounds limit secret capacity.

Using the QCT security model, we propose a key agreement protocol that we call **MUB-Quantum Computational Timelock** (MUB-QCT), where a bit is encoded on the d dimensional quantum state, using a complete set of mutually unbiased bases (MUBs) and a set of pair-wise independent permutations as encoding bases. The security of the protocol is proved by calculating the bound on the adversary's mutual information. We prove that upper bound on Eve's information scales as $\mathcal{O}(1/d)$. We show MUB-QCT offers: *high resilience to error* (up to 50% for large d) with fixed hardware requirements; Measurement Device Independent (*MDI*) security, as security is independent of channel monitoring and does not require to trust measurement devices. We also prove the security of the MUB-QCT protocol, with multiple photons per channel use, against two restricted eavesdropping scenarios where Eve measures each copy individually using a fixed optimal measurement or proactively measures each copy in a different MUB followed by post-measurement classical decoding. We prove that the MUB-QCT protocol allows secure key distribution with input states containing up to $O(d)$ photons which imply a significant performance boost, characterized by a $O(d)$ multiplication of key rate. We claim that the protocol we consider here offers: high resilience to error, a security guarantee that does not require trust in the measurement device's implementation, and high tolerance to the channel loss incurred at long distances.

Our work is in particular related to *Quantum data locking* [LL14, LL15a] where the security against an adversary with time-limited quantum memory can be proved by upper bounding the accessible information [LL15b]. However, existing work on quantum data locking is restricted to single-photon encoding [LL14] and cannot extend the distance or resort to constructions based on random coding arguments [LL15a] for which practical implementation with structured measurement is not possible.

Outline of the thesis

The thesis is divided into two parts. The first part *"from quantum information to quantum cryptography"* introduces the preliminary concepts such as classical and quantum information theory,

classical and quantum cryptography, different quantum key distribution protocols and some other important concepts that are necessary to understand the quantum cryptography in the quantum computational timelock security model.

The second part of the thesis is *"quantum computational hybrid cryptography"*, which presents the important result of this thesis. We describe our hybrid security model quantum-computational time-lock, construct the key distribution protocol under this security model and present a detailed analysis of the results.

Part I: From Quantum information to quantum cryptography

Chapter 1: Quantum information and communication

In this chapter, we briefly describe the main tools of "Quantum Mechanics" and "Quantum Information Theory" that we will use for the study of Quantum Key Distribution. We begin with a brief introduction to Quantum mechanics, followed by basic tools and aspects of classical information theory, and finally, we introduce topics in quantum information theory.

Chapter 2: Cryptography

The objective of this chapter is to highlight the salient features of security definitions in classical cryptography schemes and provide a reasonable basis for comparison with information-theoretic schemes

Chapter 3: Quantum cryptography

The present chapter aims to provide an overview of the most important and most recent advances in quantum cryptography, both theoretically and experimentally. After a brief introduction of the general notions, we will review the main QKD protocols based on discrete- and continuous-variable systems. We will consider standard QKD, device-independent, and measurement-device independent QKD. We will then discuss the ultimate limits of point-to-point private communications and how quantum repeaters and networks may overcome these restrictions. Finally, we will treat topics beyond QKD, including Twin-Field QKD, Flood Light QKD, and Quantum Data Locking.

Chapter 4: QKD against bounded adversary

In this chapter we review the *Bounded Quantum Storage Model* (BQSM), where Eve is assumed to be able to store only a limited number of qubits. Second, we consider the effect of *Quantum Data Locking* (QDL) and its application to QKD and secure communication under the assumption that Eve can store unlimited qubits in quantum memory, however, only for a finite time.

Part II: Quantum Computational Hybrid Cryptography

Chapter 5: Quantum Computational Time-lock security model

We introduce a novel *Quantum Computational Timelock* (QCT) security model, which consists of two nested assumptions:

1. Alice and Bob are assumed to have access to an encryption scheme, computationally secure for a short time t_{comp}, to do private communication against Eve.

2. Eve's quantum memory is t_{coh}-decohering, i.e., the evolution is described by a complete positive trace-preserving map $\mathcal{N}_{t_{coh}} : \rho \to \mathcal{N}_{t_{coh}}(\rho)$, such that $\frac{1}{2}\left|\left|\mathcal{N}_{t_{coh}}(\rho_x) - \frac{\mathbb{I}_d}{d}\right|\right|_1 = o\left(\frac{1}{d}\right)$, and it is assumed that $t_{coh} < t_{comp}$.

These assumptions, in particular, are well motivated by the reality, as the coherence time of a state of the art quantum memory, $t_{coh} \sim \mathcal{O}(1)$sec, is much smaller than the computational time, $t_{comp} \sim 10^9$sec, for which a current classical cryptographic scheme is secure.

Chapter 6: From QCT to a key Establishment Protocol

In this chapter, we discuss key-establishment protocol using the QCT security model. We first present a generic framework to construct a d-dimensional key-establishment protocol. We then propose a key agreement protocol, that we call **MUB-Quantum Computational Timelock**(MUB-QCT).

Parameters: The m-MUB-QCT-(b, c) key distribution protocol is parametrized by the following parameters

- b : number of bits encoded on a d-dimensional quantum state.
- c : the classical capacity of the encoding.
- m : number of copies of the qudit state sent per channel use.

Ingredients: An essential element of the MUB-QCT protocol will consist in randomizing one of the basis states of a d-dimensional Hilbert space using set of unitaries:

- A complete set of $d + 1$ mutually unbiased bases (MUB), in dimension d.
- A full set of pair-wise independent permutations.

Different Protocols: Based on the number of bits encoded on a d-dimensional quantum state and the number of copies of the qudit state sent per channel use, we propose different versions of MUB-QCT protocol.

- In section 6.3.1, we propose 1-MUB-QCT-$(\log d, \log d)$ protocol, where for a single copy of quantum state sent per channel use $\log d$ bits are encoded on a qudit, using a full set of MUBs.
- In section 6.3.2 we propose 1-MUB-QCT-$(1, \log d)$ protocol, where for a single copy of quantum state sent per channel use a bit is encoded on a qudit, using a full set of MUBS and a full set of pair-wise independent permutations.
- In section 6.3.3, we propose MUB-QCT protocol with multiple copies per channel use, namely m-MUB-QCT-$(\log d, \log d)$ and m-MUB-QCT-$(1, \log d)$ protocol.

Ingredients: The protocol consists of two phases;

- *Setting a computational timelock:* Alice and Bob share a secret information $s \in \mathcal{S}$ (a classical secret information corresponding to the encoding unitary) over a classical communication channel using t_{comp}-secure encryption scheme. For the 1-MUB-QCT-$(\log d, \log d)$ protocol, s corresponds to the index of the mutually unbiased base, while for the 1-MUB-QCT-$(1, \log d)$ protocol, it corresponds to the index of the mutually unbiased base and the permutation used to encode the classical bit on the qudit.

- *Quantum communication:* Alice encodes a bit $x \in \mathcal{X}$ on a d-dimensional quantum state using s as

$$\rho_x = \frac{1}{|s|} \sum_s \rho_{xs} \tag{2}$$

  Alice sends the state ρ_x to Bob via an insecure quantum channel, who decodes the bit by performing a projective measurement on ρ_x, using s, and obtains $y \in \mathcal{Y}$.

Eve is assumed to have full access to the input of Alice and Bob's communication channels (similar to strong quantum data locking [Lup15]). However, Eve can not break timelock encryption before t_{comp}. Moreover, she cannot store state ρ_x for time longer than t_{coh}. Eve can use one only of the following strategies:

- **(I)** Eve stores the input quantum state ρ_x in her quantum storage and later performs a measurement at time t_{comp}, knowing the secret s, to obtain $z \in \mathcal{Z}$.

- **(II)** Eve performs an immediate measurement on input state ρ_x and obtains a classical outcome ω. At time t_{comp}, she performs post-measurement classical decoding using s and ω to obtain $z \in \mathcal{Z}$.

Chapter 7: Security of MUB-QCT protocol

In this chapter we present the security of the MUB-QCT protocols. The security of the protocols is proved by demonstrating that under the QCT assumptions, the optimal attack strategy for non-authorized party Eve consists in an immediate measurement followed by classical post-processing on measurement data i.e., strategy II. This strategy is known as state discrimination with post measurement information as described in [GW10].

For both, the 1-MUB-QCT-$(\log d, \log d)$ and the 1-MUB-QCT-$(1, \log d)$ protocol, we prove that the the optimal eavesdropping strategy is II. For the 1-MUB-QCT-$(\log d, \log d)$, we prove the the guessing probability for Eve if she perform the strategy II is $\mathcal{O}\left(\frac{1}{\sqrt{d}}\right)$. For the 1-MUB-QCT-$(1, \log d)$ protocol, we show that, Eve has no preferable choice for the immediate measurement as the full set of MUBs forms a 2-design [GKR]. As a result, we can prove that this second strategy reduced, for Eve, to access the output of a strong QC-extractor [BFW14] based on a full set of MUBs, and therefore that her guessing probability is $\frac{1}{2} + \mathcal{O}\left(\frac{1}{d}\right)$.

At the end of the MUB-QCT protocol, Alice and Bob hold classical random variables X and Y, while Eve holds a classical random variable Z and a decohered quantum memory. Csiszár and Körner formula [CK78a] $R \geq I(X;Y) - I(X;Z)$ can thus be applied to derive the secure key rate. Proving the security of the MUB-QCT protocol hence requires to bound Eve's mutual information $I(X;Z)$. Given that II is the best strategy, we can use the guessing probability to calculate a

bound on eve's mutual information. We prove that for the 1-MUB-QCT-$(\log d, \log d)$ protocol $I(X;Z) \sim \mathcal{O}(1/\sqrt{d})$, while for -MUB-QCT-$(1, \log d)$ protocol $I(X;Z) \sim \mathcal{O}(1/d)$.
Very notably, the bound on Eve information can be achieved under QCT security model, by only considering the input state and not Bob measurement's results.

Chapter 8: Security of MUB-QCT with multiple copies per channel use

The previous chapter deals with one copy of ρ_x encoded on a single photon. In this chapter we explore if the MUB-QCT protocol offers high tolerance to the channel loss incurred at long-distance by transmitting multiple photons per channel use. Alice prepares m copies of the qudit state, ρ_x, using same basis θ. We prove security under two restricted attack strategies for Eve;

1. **individual attack:** where Eve is restricted to perform the same individual fixed measurement on each of the m copies.

2. **Proactive MUB measurement:** where Eve proactively measures each copy separately in a different basis, chosen from the full set of MUBs, followed by post-measurement decoding after time t_{comp}.

We prove that for m-MUB-QCT-$(1, \log d)$ protocol, the proactive MUB measurement is more efficient than the individual attack strategy. In the case of individual attack strategy Eve's mutual information can be upper bounded as as $I^{\text{Fix}}(X;Z)_m \leq \mathcal{O}\left(\frac{\sqrt{m}}{d}\right)$, while for the proactive MUB measurement, Eve's mutual information increases linearly with m as $I^{\text{Pro}}(X;Z) \sim \mathcal{O}(m/d)$.

For for m-MUB-QCT-$(\log d, \log d)$ protocol, we prove that the individual attack strategy is more efficient than the proactive MUB measurement. In the case of individual attack strategy Eve's mutual information can be upper bounded as as $I^{\text{Fix}}(X;Z)_m \leq \mathcal{O}\left(\frac{\sqrt{m}}{\sqrt{d}}\right)$, while for the proactive MUB measurement, Eve's mutual information increases linearly with m as $I^{\text{Pro}}(X;Z) \sim \mathcal{O}(m/d)$.

Chapter 9: Performance analysis of the MUB-QCT protocol

MUB-QCT protocol offers following advantages:

- **Noise tolerance:** High dimensional encoding in the MUB-QCT protocol allows high resilience to noise by offering a maximum tolerable error rate of up to 50% for large d.

- **Resource requirements:** The MUB-QCT protocol can be implemented with only two detectors, irrespectively of d . This relaxes resource requirements compared to HD-QKD schemes [LPD+13, LBZ+16a], requiring d-single-photon detectors.

- **MDI security:** In the MUB-QCT protocol, Eve's information can be upper bounded only by considering the state that Alice inputs. Consequently, the implementation of Bob's measurement device is not required to be trusted to guarantee security.

The proactive MUB measurement strategy appears more efficient than the single copy fixed measurement. It nevertheless allows secure key distribution with input states containing up to $O(d)$ photons, implying a significant performance increase, characterized by a $O(d)$-**multiplication of key rates** as shown in Figure 9.3. The possibility of sending multiple copies of the quantum state per channel use moreover can be leveraged to realize **multiparty key distribution**. In principle, Alice can transmit m copies to up to m authorized Bobs, allowing them to distill the same key.

Chapter 10: Conclusion

In this chapter we briefly review the results presented in the thesis and we compare the results with the other existing works.

Chapter 11: Perspectives

In this final chapter we present some open questions and possible direction for the future work. We first preset the new direction to construct the QCT key distribution protocol using the communication complexity problems. We consider two such communication complexity problems namely Hidden matching problem a[BYJK08, GKRW06, GKK+07, Gav09] and Khot-Vishnoi game [BRSD11]. These games have special property that they offer exponential separation between the classical and the quantum communication complexity. We show a possible direction for future work on how this exponential separation can be used to send multiple copies per channel use and prove the security of the protocol.

In this chapter we also explains some open question to improve the security of the MUB-QCT protocol, especially with respect the short-term secure computational assumption. We describe two ways to redefine the assumption by considering either the public key or private-key encryption scheme to be short-term secure.

Finally, we explore the possible implementation of the MUB-QCT protocol. We first explain the important experimental challenges for the implementation of the protocol. We then briefly review different high-dimensional encodings that have been demonstrated experimentally. We then propose a sketch of a possible high dimensional MUB-QCT protocol using spatial modes and finally we discuss the suitability of QCT key distribution protocol with coherent state encoding.

Part I

From Quantum information to Quantum Cryptography

Chapter 1

Quantum information and communication

The word 'information' refers to a poly-semantic concept associated with many different phenomenons, such as communication, knowledge, reference, and meaning. It can be some facts provided or learned about something or someone or can be that, which is conveyed or represented by a particular arrangement or a sequence of things. In an everyday sense, characteristic use of the term 'information' is in phrases of the form: 'information about p', where p might be some object, event, or topic; or in terms of the form: 'information that q'. Concerning information, we can distinguish between possessing information, which is to know; acquiring information, gaining knowledge; and containing information, which is sometimes the same as knowing.

Information is Physical
-Rolf Landauer

In physics, information refers to the information of a physical system, generally considered to specify the system's 'true' state. Information is encoded in the state of a physical system. In information theory, it is a mathematical quantity expressing the probability of a particular sequence of symbols, impulses as against that of alternative sequences.

In this chapter, we briefly describe the main tools of "Quantum Mechanics" and "Quantum Information Theory" that we will use for the study of Quantum Key Distribution. We begin with a brief introduction to Quantum mechanics, followed by basic tools and aspects of classical information theory, and finally, we introduce topics in quantum information theory.

Most of this chapter's content is present in Nielsen and Chuang's textbook [NCC00] and Lecture notes on Quantum Information and Computation by J. Preskill [Pre15].

1.1 Brief introduction to quantum mechanics

The twentieth century's opening heralded an unprecedented era of turnover and re-evaluation of the classical theory that governed Physics since pre-Newtonian times. Two grand revolutionary ideas changed the face of physics in the early decades of the twentieth century: the *Theory of Relativity* and the *Quantum Mechanics*. Einstein's Theory of Relativity called for radical changes in the classical Newtonian concepts of space and time. These two were considered independent entities in the description of the physical world and let to the unified four-dimensional world in which time is regarded as the fourth coordinate, though not quite equivalent to the three space coordinates.

The story of Quantum Theory, on the other hand, is the result of the creative work of several great scientists that went through many evolutionary stages. It gives us today a deep insight into

the structure of atoms and atomic nuclei and that of bodies of the sizes familiar to our everyday experience.

On December 14, 1900, Max Plank stated that paradoxes persisting the classical theory of the emission and absorption of light by material bodies could be removed if one assumes that *radiant energy can exist only in the form of discreet packages*. He called these packages *light quanta*. Five years later, Albert Einstein successfully applied the idea to explain the empirical law of *photoelectric effect*; the emission of electron from metallic surfaces when irradiated by light with energy greater than the wave-function of the metallic surface. Later, Arthur Compton experimentally showed *X-ray scattering by free electron* follow the same law as the collision between two elastic spheres.

In the year 1913, Niels Bohr extended Plank's idea of quantization of radiant energy to the description of mechanical energy of electrons with an atom by introducing specific *quantization rules* for such mechanical systems. Bohr was able to explain the spectral lines of hydrogen and heavier elements in great detail, a problem that for decades had mystified the spectroscopists. However, successful as Bohr's theory, it was still not a final theory since it could not explain, for example, describe the transition process of an electron from one quantum state to another, and there was no way to calculate the intensities of various lines in optical spectra.

In 1925, a French physicist, Louis de Broglie, gave an entirely unexpected interpretation of the Bohr's theory, where he explained that in a Bohr quantum orbit, the motion of each electron is governed by some mysterious *pilot wave*, whose propagation and length depends on the velocity of the electron in question. Assuming that these pilot waves are inversely proportional to the electron's velocity, de Broglie showed that various quantum orbits in Bohr's model of a hydrogen atom were those that could accommodate an *integral number* of pilot wave. This idea was extended by Erwin Schrodinger, whose theory is popularly known as *Wave Mechanics*. Simultaneously, W. Heisenberg developed the treatment of quantum problem using non-commutative algebra to give the uncertainty principle asserting a fundamental limit to the precision with which the values for specific pairs of physical quantities of a particle, known as complementary variables or canonically conjugate variables such as position x and momentum p, can be predicted from initial conditions.

But with all development, there remained one sharp thorn in the crown of the Quantum Theory, it was painful whenever one tried to quantized the mechanical system, which, because of the very high velocity involved (close to the speed of light), required relativistic treatment. The relief from this pain came in 1929 when P. A. M. Dirac wrote his famous *Relativistic Wave Equation*. The solution to this equation gave a perfect description of the atomic electron's motion at velocities close to that of light and explained their linear and angular mechanical momenta and magnetic moments. His equation also suggested that along with ordinary negatively charged electrons *there must also exist positively charged anti-electron*. This brilliant prediction was later verified when anti-electrons were found in cosmic rays.

Thus, by 1930, only three decades after Plank's announcement, the Quantum Theory took the final shape with which we are now familiar.

1.1.1 Description of a quantum physical system

In this section the postulates of quantum mechanics will be stated out and discussed in broad term to bring out the essential features of quantum theory.

Postulate 1: State space; Associated to any isolated physical system is a complex vector space with inner product (that is, a Hilbert space) known as the *state space* of the system. The

system is completely described by its *state vector*, which is a unit vector in the system's state space.

The first postulate states that a particle is represented by a ket vector $\psi\rangle$ in a Hilbert space $\mathcal{H}$. It has an inner product $\langle\psi|\phi\rangle$ that maps an ordered pair of vectors to a vector space over the complex numbers $\mathbb{C}$, defined by the properties

1. Positivity: $\langle\psi|\psi\rangle > 0$ for $\psi\rangle = 0$
2. Linearity: $\langle\phi|(a|\psi_1\rangle + b|\psi_2\rangle) = a\langle\phi|\psi_1\rangle + b\langle\phi|\psi_2\rangle$
3. Skew symmetry: $\langle\phi|\psi\rangle = \langle\psi|\phi\rangle^*$

The state $|\psi\rangle$ is complete in the norm $||\psi|| = \langle\psi|\phi\rangle^{1/2}$. An alternative description of the postulate is captured by the *principle of superposition*, which states that if $|\psi\rangle$ and $|\phi\rangle$ represents two possible states of a particle then so does $\alpha|\psi\rangle + \beta|\phi\rangle$, such that $|\alpha|^2 + |\beta|^2 = 1$.

Postulate 2: Observable; An observable is a property of a physical system that in principle can be measured. In quantum mechanics an observable is a *self adjoint operator*.

An operator is a linear map taking vectors to vectors $A : |\psi\rangle \to A|\psi\rangle$. The adjoint of the operator A is defined by

$$\langle\phi|A\psi\rangle = \langle A^\dagger\phi|\psi\rangle \tag{1.1}$$

for all vectors $|\phi\rangle$, $|\psi\rangle$. If A and B are self adjoint, then so $(A+B)^\dagger = A^\dagger + B^\dagger$, but since $(AB)^\dagger = B^\dagger A^\dagger$, so AB is self adjoint only if A and B commute.

Postulate 3: Measurement; If the particle is in the state $|\psi\rangle$, the measurement of the observable A, will yield one of the eigenvalue a of A, with probability $P(a) \propto |\langle a|\psi\rangle|^2$. The state of the system will change from $|\psi\rangle$ to $|a\rangle$ as a result of the measurement.

The theory makes only probabilistic prediction for the results of a measurement. Further, it assigns (relative) probabilities only for obtaining some eigenvalue a_i of A. And as the operator is required to be Hermitian, these eigenvalues are real. Since we told that $P(a) \propto |\langle a_i|\psi\rangle|^2$, the quantity $|\langle a_i|\psi\rangle|^2$ is only the relative probability. To get the absolute probability, we divide $|\langle a_i|\psi\rangle|^2$ by the sum of all relative probabilities:

$$P(a_i) = \frac{|\langle a_i|\psi\rangle|^2}{\sum_i |\langle a_i|\psi\rangle|^2} \tag{1.2}$$

Projective measurement versus POVM: A *projective measurement* is described by an observable, A, a Hermitian operator on the state space of the system being observed. The observable has a spectral decomposition, $A = \sum_a aP_a$, where $P_a = |a\rangle\langle a|$ is the projector onto the eigenspace of A with eigenvalue a. The possible outcomes of the measurement corresponding to the eigenvalues, a, of the observable. Upon measuring the state $|\psi\rangle$, the probability of getting result a is

$$P(a) \propto |\langle a|\psi\rangle|^2 = \langle\psi|a\rangle\langle a|\psi\rangle = \langle\psi|P_a|\psi\rangle = \langle\psi|P_a^\dagger P_a|\psi\rangle = ||P_a|\psi\rangle||^2 \tag{1.3}$$

Projective measurements are restrictive and not always possible. Sometimes we destroy a quantum state in the process of measurement; thus, the repeatability of a projective measurement is violated. For example, a photon may be absorbed by a polarization filter and no longer available

for measurements. In such cases where the system is measured only once, the post-measurement state of the system is no longer of interest and the probabilities of the measurement outcomes are the ones that count. A generalized type of measurement, the *positive operator-valued measure*, or POVM, is concerned only with the measurement statistics. The POVM operators are not necessarily orthogonal or commutative and allow measurement outcomes associated with non-orthogonal states. Recall that measurement operators corresponding to non-orthogonal states do not commute and are therefore not simultaneously observable. The number of POVM operators may differ from the dimension of the Hilbert space, while the number of projective operators is precisely equal to the Hilbert space's dimension.

Given the set of measurement operators, $\{M_i\}$, describing a measurement performed on a quantum system in the state, $|\psi\rangle$, a POVM has the elements, E_i, defined by

$$E_i = M_i^\dagger M_i, \quad \text{and,} \quad \sum_i E_i = I \tag{1.4}$$

. The operator E_i have several properties, including:

1. They are positively defined, i.e., a positively defined operator has real and positive eigenvalues. This property follows immediately from the definition of E_i.

2. $P(i) = \langle\psi|E_i|\psi\rangle$. This follows immediately from the fact that $P(i) = \langle\psi|M_i^\dagger M_i|\psi\rangle$. The set of operators, $\{E_i\}$, can be used, instead of $\{M_i\}$, to estimate the probability of various measurement outcomes.

Postulate 4; Dynamics: The state vector $|\psi\rangle$ obeys the *Schrödinger equation*

$$i\hbar\frac{d}{dt}|\psi(t)\rangle = H|\psi(t)\rangle \tag{1.5}$$

where, H is the Hamiltonian of the system.

Time evolution of a quantum state is unitary it is generated by a self-adjoint operator called the Hamiltonian of the system. We may express the above equation, to first order in the infinitesimal quantity dt, as

$$|\psi(t+dt)\rangle = (1 - iHdt)|\psi(t)\rangle = U(dt)|\psi(t)\rangle \tag{1.6}$$

The operator $U(dt)$ is unitary; because H is self-adjoint it satisfies $U^\dagger U = 1$ to linear order in dt. Since a product of unitary operator is finite, the time evolution over a finite interval is also unitary

$$|\psi(t)\rangle = U(t)|\psi(0)\rangle \tag{1.7}$$

In the case, where H is time independent; we may write $U = e^{-itH}$

1.1.2 Density operator

We have formulated quantum mechanics using the language of state vectors. An alternate formulation is possible using a tool known as the density operator or density matrix. This alternate formulation is mathematically equivalent to the state vector approach, but it provides a much more convenient language for thinking about some commonly encountered quantum mechanics scenarios.

The density operator language provides a convenient means for describing quantum systems whose state is not completely known. More precisely, suppose a quantum system is in one of many states $|\psi_i\rangle$, where i is an index, with respective probabilities p_i. We shall call $\{p_i, |\psi_i\rangle\}$ an ensemble of pure states. Then the state of a quantum mechanical system is represented by a normalized nonnegative operator ρ, called density operator, on a Hilbert space H, defined as

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \tag{1.8}$$

The normalization is with respect to the trace norm, i.e., $||\rho||_1 = \mathsf{Tr}(\rho) = 1$. When measuring a system in the state ρ with respect to POVM, i.e., a family $\{E_i\}$, the probability distribution of the outcome is given by $P(i) := \mathsf{Tr}(E_i\rho)$

1.1.3 Product system and purification

To analyze complex physical systems, it is often convenient to consider partitioning into several subsystems. This is particularly useful if one is interested in studying operations that act on the parts of the system individually. Mathematically, a quantum system's partition into subsystems induces a product structure on the underlying Hilbert space. *The state space of a composite physical system is the tensor product of the state spaces of the component physical systems.* Moreover, if we have systems numbered 1 through n, and system i is prepared in the state ρ, then the joint state of the total system is $\rho_1 \otimes \rho_2 \otimes \ldots \otimes \rho_n$. For example, consider a bipartite state, if the Hilbert space describes the individual systems $\mathcal{H}_A$ and $\mathcal{H}_B$, the Hilbert space $\mathcal{H}_{AB}$ of the hybrid system $\rho_{AB} = \rho_A \otimes \rho_B$ is the tensor product of individual systems, $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$. The state of one part of a product system is then obtained by taking the corresponding partial trace of the overall state, i.e.,

$$\rho_A = \mathsf{Tr}_B(\rho_{AB}) \tag{1.9}$$

A density operator ρ on $\mathcal{H}$ is said to be pure if it has rank one, that is, $\rho = |\psi\rangle\langle\psi|$, for some $|\psi\rangle \in \mathcal{H}$. If it is normalized, ρ is a projector onto $|\psi\rangle$. This implies that a pure state contains no classical randomness. That is, it cannot be correlated with any other system. The fact that a pure state cannot be correlated with the environment plays a crucial role in cryptography. It implies, for example, that the randomness obtained from the measurement of a pure state is independent of any other system and thus guaranteed to be secret. More generally, let ρ_A be an arbitrary operator on $\mathcal{H}_A$ and let ρ_{AE} be a purification of ρ_A, i.e., ρ_{AE} is a pure state on a product system $\mathcal{H}_A \otimes \mathcal{H}_E$ such that $\mathrm{tr}_E(\rho_{AE}) = \rho_A$. Then, because ρ_{AE} is uncorrelated with any other system, the partial system $\mathcal{H}_E$ comprises everything that might be correlated with the system $\mathcal{H}_A$ (including the knowledge of a potential adversary).

1.2 Classical information

This section aims to discuss and understand the main concepts in classical information theory before we delve into the analogous quantum information-theoretic ideas. We present a very rapid overview of the topic, and a more detailed presentation can be found for instance in the textbooks "Elements of information theory" by Cover and Thomas [CT06] and "Information theory, inference, and learning algorithms" by MacKay [MMKP03].

Definition 1.2.1 (Shannon entropy) *Let X be a random variable distributed over a finite set $\mathcal{X}$ according to the probability distribution P_X. Then, a natural measure of the uncertainty of a random variable X is its (Shannon) entropy $H(X)$ defined as follows:*

$$H(X) = -\sum_{x\in\mathcal{X}} P_X(x)\log_2 P_X(x) \tag{1.10}$$

This notion can be generalized to n-tuples of random variables $X_1,\ldots,X_n$, with the *joint entropy*:

$$H(X_1,\ldots,X_n) = -\sum_{x_1\in\mathcal{X}_1}\cdots\sum_{x_n\in\mathcal{X}_n} P_{X_1,\ldots,X_n}(x_1,\ldots,x_n)\log_2 P_{X_1,\ldots,X_n}(x_1,\ldots,x_n) \tag{1.11}$$

From this definition, one can immediately deduce the following properties:

Theorem 1.2.2 (Properties of the entropy) *following are the basic properties of the Shannon entropy,*

1. *$H(X)\geq 0$, with equality if and only if X is certain.*
2. *H is subadditive: $H(X_1,\ldots,X_n)\leq H(X_1)+\ldots+H(X_n)$, with equality if and only if the X_i are independent.*
3. *If $\mathcal{X}$ is finite, $H(X)\leq\log_2|\mathcal{X}|$ with equality if and only if X is uniformly distributed over $\mathcal{X}$.*

In a cryptographic setting, the Shannon entropy is not always a desirable measure as it merely captures our uncertainty about X *on average*. Often, the Rényi entropy allows us to make stronger statements. The *Rényi entropy* of order α is defined as

$$H_\alpha(X) = \frac{1}{1-\alpha}\log_2\Big[\Big(\sum_{x\in\mathcal{X}} P_X(x)^\alpha\Big)^{\frac{1}{\alpha-1}}\Big] \tag{1.12}$$

Indeed, the Shannon entropy forms a special case of Rényi entropy by taking the limit $\alpha\to 1$, i.e., $H_1(\cdot)=H(\cdot)$. Among other values of α, ones with particular interests are

1. *Max entropy*
$$H_{max}(X) = H_0(X) := \log_2|\mathcal{X}| \tag{1.13}$$
2. *Collision entropy*, which plays a role for *privacy amplification* protocols
$$H_2(X) := -\log_2\sum_{x\in\mathcal{X}} P_x^2 \tag{1.14}$$
3. *Min entropy*, which is determined by the highest peak in the distribution and most closely captures the notion of "*guessing*" x.
$$H_{min}(X) = H_\infty(X) = -\log_2(\max_{x\in\mathcal{X}} P_X(x)) \tag{1.15}$$

Following which, we have

$$\log_2|\mathcal{X}|\geq H(X)\geq H_2(X)\geq H_\infty(X) \tag{1.16}$$

i.e.,for a given random variable X, $(\alpha \mapsto H_\alpha(X))$ is a decreasing function of α. All the Rényi entropy are *additive*, meaning $H_\alpha(X,Y) = H_\alpha(X) + H_\alpha(Y)$ for independent random variables X and Y. Furthermore, we can quantify the uncertainty about X given Y by the means of the *conditional entropy*

$$H(X|Y) = H(X,Y) - H(Y) \tag{1.17}$$

A fundamental property of the conditioning is that it reduces the entropy:

$$H(X|Y) \leq H(X) \tag{1.18}$$

with equality if X and Y are independent random variables. To quantify the amount of information X and Y may have in common we use*mutual information*

$$I(X,Y) = H(X) + H(Y) - H(X,Y) = H(X) - H(X|Y) \tag{1.19}$$

Intuitively, the mutual information captures the amount of information we gain about X by learning Y. The mutual information between two random variables is a measure of their correlation. In particular, one has $I(X;Y) = 0$ for independent variables. In should be noted that Equation (1.18) also holds for conditional entropies

$$H(X|Y,Z) \leq H(H|Y) \tag{1.20}$$

which is called the *strong subadditivity property*. This property can equivalently be written:

$$H(X,Y) + H(Y,Z) \geq H(X,Y,Z) + H(Y). \tag{1.21}$$

1.3 Quantum information

1.3.1 Von Neumann entropy

Similar to the Shannon entropy, the *von Neumann entropy* of a quantum state ρ_x is given by

$$S(\rho) = -\mathsf{Tr}(\rho \log_2 \rho) \tag{1.22}$$

Taking the eigen-decomposition of $\rho_x = \sum_x \lambda_x |x\rangle\langle x|$ we can also write

$$S(\rho) = -\sum_x \lambda_x \log_x \lambda_x, \tag{1.23}$$

which corresponds to the Shannon entropy arising from measuring ρ in the given basis $\{|x\rangle\langle x|\}$.

Theorem 1.3.1 (Properties of von Neumann entropy) *Following are the properties of S:*

1. *$S(\rho) \geq 0$, with equality if and only if ρ is pure.*
2. *In a finite dimensional Hilbert space $\mathcal{H}$ of dimension d, $S(\rho) \leq \log_2 d$, with equality if and only if $\rho = \mathbb{1}_{\mathcal{H}}/d$.*
3. *S is invariant under unitary operation: for any unitary U, $S(U\rho U^\dagger) = S(\rho)$.*
4. *If a composite system AB is pure then $S(A) = S(B)$.*

5. *If* $\rho = \sum_k P_K(k)\rho_k$, *where* $P_K(k)$ *have support on orthogonal subspaces, then*

$$S(\rho) = H(P_K(k)) + \sum_k P_K(k)S(\rho_k). \tag{1.24}$$

6. S *is subadditive:* $S(\rho_{AB}) \leq S(\rho_A) + S(\rho_B)$, *with equality if and only if* $\rho_{AB} = \rho_A \otimes \rho_B$

Similar to classical joint and conditional entropies, one can define quantum joint and conditional entropies as well as quantum mutual information for composite system. Let a quantum state of a composite system AB be represented by the density matrix ρ_{AB}, one defines the *joint entropy* of the system AB as

$$S(A, B) = -(Tr)(\rho_{AB} \log_2 \rho_{AB}), \tag{1.25}$$

The *quantum conditional entropy* of A given B is

$$S(A|B) = S(A, B) - S(B), \tag{1.26}$$

and the *quantum mutual information* between systems A and B is

$$S(A : B) = S(A) + S(B) - S(A, B) = S(A) - S(A|B) = S(B) - S(B|A). \tag{1.27}$$

An important difference with the classical setting is that the conditional von Neumann entropy can be negative. A non trivial property of the von Neumann entropy is given by the following theorem:

Theorem 1.3.2 (Strong subadditivity.) *For any three quantum system,* A, B *and* C, *one has:*

$$S(A, B, C) + S(B) \leq S(A, B) + S(B, C) \tag{1.28}$$

Corollaries of this results are:

1. *Conditioning reduces entropy:* $S(A|B, C) \leq S(A|B)$.
2. *Discarding quantum system never increases mutual information:* $S(A : B) \leq S(A : B : C)$.
3. *Quantum operations never increases mutual information:* if the system AB is mapped to $A'B'$ through a quantum operation, then $S(A' : B') \leq S(S : B)$. Here, a quantum operation refers to a linear completely positive trace non-increasing map.

1.3.2 Encoding quantum information

Recall that a qubit is represented as a vector in a two dimensional Hilbert space, which is drawn by the following basic vectors:

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \tag{1.29}$$

Any pure qubit state can thus be expressed as a linear superposition of these basis states,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle = \cos(\theta/2)|0\rangle + e^{i\phi}\sin(\theta/2)|1\rangle \tag{1.30}$$

with $\theta \in (0, \pi), \phi \in (0, 2\pi)$ and i the imaginary unit. This state can be pictorially represented as a vector in the so-called "Bloch sphere". When $\theta = 0$ or $\theta = \pi$, we recover the basis states $|0\rangle$ and

$|1\rangle$, respectively, which are placed at the poles of the sphere. When $\theta = \pi/2$, the qubit pure state is a vector lying on the equator of the sphere. Here we can identify the four vectors aligned along the $\hat{x}$ and $\hat{y}$ axes, which are obtained in correspondence of four specific values of ϕ, i.e., we have:

$$\phi = 0 : |+\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \quad \phi = \pi : |-\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix} \tag{1.31}$$

$$\phi = \pi/2 : |+i\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}, \quad \phi = 3\pi/2 : |-i\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}, \tag{1.32}$$

The basis vectors in Eq. (1.29) are eigen states of the Pauli matrix σ_z, referred as "$\mathbb{Z}$ basis". Similarly states in Eq. (3.3) are eigenstates of σ_x, known as "$\mathbb{X}$ basis" and states in Eq. (3.4) are eigenstates of σ_y, referred as "$\mathbb{Y}$ basis". It is worth noting that each of these pairs of eigenstates forms a basis which are mutually unbiased to one another, referred to as mutually unbiased bases (MUB). Formally defined as,

Definition 1.3.3 (Mutually Unbiased Bases) *Let $\mathcal{B}^{\theta_1} = \{|e_0^{\theta_1}\rangle, \ldots, |e_{d-1}^{\theta_1}\rangle\}$ and $\mathcal{B}^{\theta_2} = \{|e_0^{\theta_2}\rangle, \ldots, |e_{d-1}^{\theta_2}\rangle\}$ be two orthonormal bases in a d dimensional Hilbert space. Then, θ_1 and θ_2 are mutually unbiased if and only if*

$$\forall (i,j) \in [d], \quad \left|\langle e_i^{\theta_1} | e_j^{\theta_2}\rangle\right| = \frac{1}{\sqrt{d}} \tag{1.33}$$

In a d dimension Hilbert space, there exist at most $(d+1)$ mutually unbiased bases [BBRV02]. Explicit construction of a full set of MUBs is known for prime power dimension and square dimensions [WB05].

To give a physical meaning to the representation of a qubit, we can interpret the qubit state in Eq. (1.30) as the polarization state of a photon. In this case, the Bloch sphere is conventionally called the Poincaré sphere, but its meaning is unchanged. The basis vectors on the poles of the Poincaré sphere are usually associated with the linear polarization states $|H\rangle = |0\rangle$ and $|V\rangle = |1\rangle$, where H and V refer to the horizontal or vertical direction of oscillation of the electromagnetic field, respectively, with respect to a given reference system. The $\mathbb{X}$ basis states are also associated with linear polarization but along diagonal ($|D\rangle = |+\rangle$) and anti-diagonal ($|A\rangle = |-\rangle$) directions. Finally, the $\mathbb{Y}$ basis states are associated with right-circular ($|R\rangle = |+i\rangle$) and left-circular ($|L\rangle = |-i\rangle$) polarization states. Any other state is an elliptical polarization state and can be represented by suitably choosing the parameters θ and ϕ.

1.3.3 Distance between quantum states

Intuitively, we say that two states of a physical system are similar if any observation of them leads to identical results, except with small probability. For two operators $\rho, \sigma \in \mathcal{P}(\mathcal{H})$ representing the state of a quantum system, this notion of similarity is captured by the L_1 -distance, i.e., the trace distance defined as

Definition 1.3.4 (Trace distance.) *The trace distance between two states ρ and σ is given by*

$$D(\rho, \sigma) = \frac{1}{2}||\rho - \sigma||_1, \tag{1.34}$$

where $||A||_1 = Tr(\sqrt{A^\dagger A})$ is the trace norm of A.

Alternatively, the trace distance may also be expressed as

$$D(\rho,\sigma) = \max_M \mathsf{Tr}(M(\rho-\sigma)), \tag{1.35}$$

where the maximization is taken over all $M \geq 0$. Indeed, D is really a "distance" measure, as it is clearly a metric on the space of density matrices: We have $D(\rho,\sigma) = 0$ if and only if $\rho = \sigma$, and evidently $D(\rho,\sigma) = D(\sigma,\rho)$. Finally, the triangle inequality holds:

$$\begin{aligned} D(\rho,\sigma) &= \max_M \mathsf{Tr}(M(\rho-\sigma)) = \max_M(\mathsf{Tr}(M(\rho-\gamma)) + \mathsf{Tr}(M(\gamma-\rho))) \\ &\leq D(\rho,\gamma) + D(\gamma,\sigma) \end{aligned} \tag{1.36}$$

The trace distance for operators can be seen as the quantum version of the trace distance for probability distributions (or, more generally, nonnegative functions), which is defined by

$$D(P_X(x), Q_X(x)) = ||P-Q||_1 := \frac{1}{2}\sum_x |P_X(x) - Q_X(x)| \tag{1.37}$$

between two classical probability distribution $P_X(x)$ and $Q_X(x)$. Under the action of a quantum operation, the trace distance between two density operators ρ and σ cannot increase. Because any measurement can be seen as a quantum operation, this immediately implies that the distance $\|P-Q\|_1$ between the distributions $P_X(x)$ and $Q_X(x)$ obtained from (identical) measurements of two density operators ρ and σ respectively, is bounded by $\|\rho-\sigma\|_1$.

The following proposition provides a very simple interpretation of the trace distance: If two probability distributions $P_X(x$ and $Q_X(x$ have trace-distance at most 2ε, then the two settings described by $P_X(x)$ and $Q_X(x)$, respectively, cannot differ with probability more than ε.

Proposition 1.3.1 *Let $P_X(x), Q_X(x)$ be probability distributions. Then there exists a joint distribution $P_{XX'}(x,x')$ such that $P_X(x)$ and $Q_X(x)$ are the marginals of $P_{XX'}(x,x')$ and, for (x,x') chosen according to $P_{XX'}((x,x')$*

$$\Pr[x \neq x'] \leq \frac{1}{2}\|P-Q\|_1 \tag{1.38}$$

In particular, if the trace distance between two states is bounded by 2ε then they cannot be distinguished with probability more than ε.

1.3.4 Distinguishability of quantum states

A consequence of quantum mechanics' linearity is the *no cloning theorem*, stating that there cannot exist an operation that clones an arbitrary quantum state since the operation $|\psi\rangle \mapsto |\psi\rangle|\psi\rangle$ is not unitary. A corollary to this result is that one cannot distinguish correctly between non-orthogonal quantum states.

Now the question arises that how can we distinguish several quantum states? To answer this, we introduce some of the necessary distinguishability measures, such as the Helstrom bound, the quantum Chernoff bound, and the quantum fidelity.

Helstrom bound

Let us suppose that a quantum system is described by an un- known quantum state ρ which can take two possible forms, ρ_0 or ρ_1, with the same probability. For discriminating between ρ_0 and ρ_1, we can apply an arbitrary quantum measurement to the system. Without loss of generality, we can consider a dichotomic POVM $\{\Pi_0, \Pi_1 := I - \Pi_0\}$ whose outcome $u = 0, 1$ is a logical bit solving the discrimination. This happens up to an error probability

$$p_e = \frac{p(u = 0|\rho = \rho_1) + p(u = 1|\rho = \rho_0)}{2}, \tag{1.39}$$

where $p(u|\rho)$ is the conditional probability of getting the out- come u given the state ρ. Then we ask: what is the minimum error probability we can achieve by optimizing over the (dichotomic) POVMs? The answer to this question is provided by the Helstrom bound [Hel76]. Helstrom showed that an optimal POVM is given by $\Pi_1 = P(\gamma_+)$, which is a projector onto the positive part γ_+ of the non-positive operator $\gamma := \rho_0 - \rho_1$, known as the Helstrom matrix. As a result, the minimum error probability is equal to the Helstrom bound

$$p_{e,\min} = \frac{1}{2}\left[1 - D\left(\rho_0, \rho_1\right)\right] \tag{1.40}$$

where,$D\left(\rho_0, \rho_1\right)$ is the trace distance between the two quantum states.

Quantum Chernoff bound

The quantum Chernoff bound [ANSV08, CMnTM+08, NS09] is an upper bound $p_{e,\min} \leq p_{QC}$, defined by

$$p_{QC} := \frac{1}{2}\Big(\inf_{0\leq s\leq 1} C_s\Big), C_s = \mathsf{Tr}(\rho_0^s \rho_1^{1-s}) \tag{1.41}$$

Note that the quantum Chernoff bound involves a minimization in $\mathrm{s} \in [0, 1]$. In particular, we must use an infimum because of possible discontinuities of C_s at the border $s = 0, 1$. By ignoring the minimization and setting $s = 1/2$, we derive a weaker but easier-to-compute upper bound. This is known as the quantum Bhattacharyya bound [PL08]

$$p_B := \frac{1}{2}\mathsf{Tr}\Big(\sqrt{\rho_0}\sqrt{\rho_1}\Big). \tag{1.42}$$

Quantum fidelity

Further bounds can be constructed using the quantum fidelity. The fidelity F is a commonly used measure to compare the input state to the output state. Given two quantum states, ρ_0 and ρ_1, their fidelity is defined by

$$F(\rho_0, \rho_1) := \left[\mathsf{Tr}\Big(\sqrt{\sqrt{\rho_0}\rho_1\sqrt{\rho_0}}\Big)\right]^2, \tag{1.43}$$

which ranges from zero for orthogonal states to one for identical states.

Multicopy discrimination

Let us assume we have M copies of an unknown quantum state ρ, which again can take the two possible forms ρ_0 or ρ_1, with the same probability. In other words, we have the two equiprobable hypotheses

$$H_0 : \rho^{\otimes M} = \rho_0^{\otimes M} := \overbrace{\rho_0 \otimes \cdots \otimes \rho_0}^{M} \tag{1.44}$$

$$H_1 : \rho^{\otimes M} = \rho_1^{\otimes M} := \underbrace{\rho_1 \otimes \cdots \otimes \rho_1}_{M} \tag{1.45}$$

The optimal quantum measurement for discriminating the two cases is now a collective measurement involving all the M copies. This is same dichotomic POVM as before, now projecting on the positive part of tge Helstrom matrix $\gamma = \rho_0^{\otimes M} - \rho_1^{\otimes M}$. Correspondingly, the Helstrom bound for the M-copy state discrimination takes the form.

$$p_{e,\min}^{(M)} = \frac{1}{2}[1 - D(\rho_0^{\otimes M}, \rho_1^{\otimes M})]. \tag{1.46}$$

Similarly, the M-copy quantum Chernoff bound

$$p_{QC}^{(M)} := \frac{1}{2}\Big(\inf_{0 \le s \le 1} C_s\Big) \tag{1.47}$$

following which, the M-copy quantum Bhattacharyya bound is

$$p_B^{(M)} = \frac{1}{2}\Big[\mathsf{Tr}\Big(\sqrt{\rho_0}\sqrt{\rho_1}\Big)\Big]^M. \tag{1.48}$$

1.4 State discrimination with post-measurement information

This problem was considered by S. Wehner et.al [GW10] and is described in Figure 1.1. We formally define this problem again here. Let $\mathcal{X}$ and $\mathcal{B}$ be finite sets and and let $P_{X,\Theta} = \{p_{x\theta}\}$ be a probability distribution over $\mathcal{X} \times \mathcal{B}$. Consider an ensemble of quantum state $\mathcal{E} = \{p_{x\theta}, \rho_{x\theta}\}$. We assume that $\mathcal{X}, \mathcal{B}, \mathcal{E}$ and $P_{X,\Theta}$ are known to both Alice and Bob. Suppose now that Alice chooses $xy \in \mathcal{X} \times \mathcal{B}$ according to the probability distribution $P_{X,\Theta}$, and sends the state $\rho_{x\theta}$ to Bob. We can then define the tasks:

Definition 1.4.1 (State discrimination) *It is the following task for Bob. Given the state $\rho_{x\theta}$, determine x, by performing any measurement on $\rho_{x\theta}$ immediately upon receipt.*

Definition 1.4.2 (State discrimination using post-measurement information) *It is the following task for Bob. Given the state $\rho_{x\theta}$, determine x, by using the following source of information in succession.*

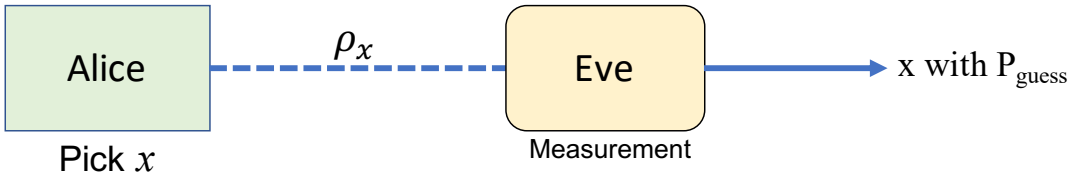
1. *He can perform any measurement on $\rho_{x\theta}$ immediately upon reception and obtain an outcome Ω. Afterward, he can stores the measurement outcome Ω in unlimited classical storage.*

2. *After Bob's measurement, Alice announces θ.*

3. *Then, Bob performs post-measurement decoding by using the measurement outcome Ω and θ to obtain an outcome z as a guess of x.*

In order to illustrate the problem formally we now present in advance the core of the problem of *State discrimination using post-measurement information*. As defined, Eve can perform any measurement immediately on the incoming quantum state and store the outcome in her classical storage. In this regard, the best immediate measurement corresponds to a measurement using the POVM ($\hat{\Pi} := \{\hat{\Pi}_\Omega\}$), with $|\mathcal{X}|^{|\mathcal{B}|}$ outcomes, each labeled by the strings $\Omega = (\omega_0, \ldots, \omega_{|\mathcal{B}|})$ i.e., $\{\hat{\Pi}_{\omega_0,\ldots,\omega_{|\mathcal{B}|}}\}$. Where, each outcome Ω is a string of length $|\mathcal{B}|$, which equip Eve with possible outputs $\omega_i \in \mathcal{X}$ for each basis $i \in \mathcal{B}$.

- Standard state discrimination



- State discrimination using post-measurement information

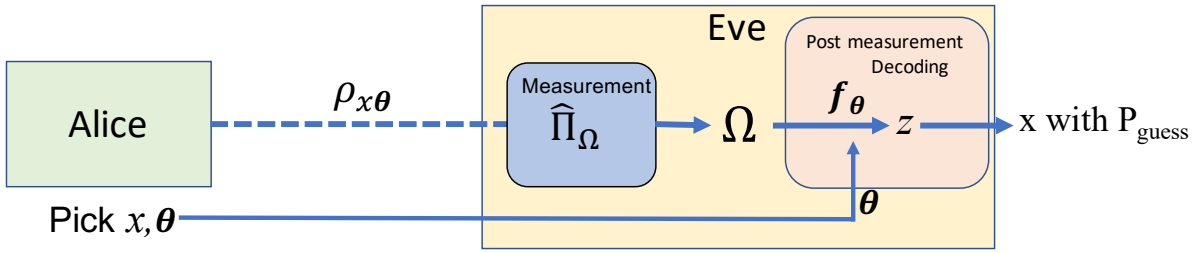


Figure 1.1: Problem of state discrimination with and without using post-measurement information as depicted in [GW10]

Later when Alice reveals the basis θ, Eve outputs $z = \omega_\theta$. This corresponds to applying the following map f_θ on the string Ω, which corresponds to an output $z = f_\theta(\Omega) = (\omega_\theta | i = \theta)$ i.e., the assignment is done by selecting the value ω_i corresponding to $i = \theta$. Finally, Eve guesses the value of x from the output $z = \omega_b$.

Now Eve succeeds at discriminating the state $\rho_{x\theta}$ using post-measurement information θ with probability P_{guess}, if and only P_{guess} is the average success probability, which is calculated as,

$$P_{guess} = \sum_{x\theta} P_{x\theta} P(z = x | \rho_{x\theta}) \tag{1.49}$$

Now, for a given $\rho_{x\theta}$ the probability to guess x is the product of two events (a) the probability to obtain the measurement outcome Ω i.e., $P(\Omega|\rho_{x\theta})$, and (b) probability to output $x = z = \omega_\theta$ from Ω, i.e., $P(\omega_\theta = x|\Omega)$, sum over all the possible value of Ω.

$$P(z = x|\rho_{x\theta}) = \sum_{\Omega} P(\Omega|\rho_{x\theta}) P(\omega_\theta = z = x|\Omega) \tag{1.50}$$

Now, $P(\omega_\theta = x|\Omega) = P(\omega_\theta = x|(\omega_0, \cdots, \omega_d)) = P(\omega_\theta = x|\omega_\theta) = \delta_{\omega_\theta x}$. The success probability is then,

$$P_{guess} = \frac{1}{|\mathcal{X}|}\frac{1}{|\mathcal{B}|}\sum_{x\theta}\sum_{\Omega} P(\Omega|\rho_{x\theta})\delta_{\omega_\theta x} = \frac{1}{|\mathcal{X}|}\frac{1}{|\mathcal{B}|}\sum_{\theta}\sum_{\Omega} P(\Omega|\rho_{\omega_\theta\theta}) \tag{1.51}$$

in the above equation $P(\Omega|\rho_{\omega_\theta\theta}) = \mathsf{Tr}(\hat{\Pi}_\Omega\rho_{\omega_\theta\theta})$ Thus,

$$P_{guess} = \frac{1}{|\mathcal{X}|}\frac{1}{|\mathcal{B}|}\sum_{\Omega}\mathsf{Tr}\Big(\hat{\Pi}_\Omega\sum_{\theta}\rho_{\omega_\theta\theta}\Big) \tag{1.52}$$

Chapter 2

Cryptography

Cryptography is about communication in the presence of an adversary. It encompasses many problems (encryption, authentication, key distribution, to name a few). The field of modern cryptography provides a theoretical foundation based on which we may understand what exactly these problems are, how to evaluate protocols that purport to solve them, and how to build protocols in whose security we can have confidence.

The objective of this chapter is to highlight the salient features of security definitions in classical cryptography schemes and provide a reasonable basis for comparison with information-theoretic schemes. Most of the content in this chapter is repeated and is present in many books [KL14, BR05, GB01]

2.1 Secure communication: a short summary

The most ancient and fundamental problem of cryptography is secure communication over an insecure channel. Party A wants to send to party B a secret message over a communication line that an adversary may tap.

The traditional solution to this problem is called *private key encryption*. In private key encryption, A and B hold a meeting before the remote transmission takes place and agree on a pair of encryption and decryption algorithms Enc and Dec, and an additional piece of information S to be kept secret. We shall refer to S as the shared secret key. The adversary may know the encryption and decryption algorithms Enc and Dec which are being used but does not know S.

After the initial meeting when A wants to send B the *cleartext* or *plaintext* message m over the insecure communication line, A *encrypts* m by computing the cyphertext $c = \mathrm{Enc}(S, m)$ and sends c to B. Upon receipt, B decrypts c by computing $m = \mathrm{Dec}(S, c)$. The line-tapper (or adversary), who does not know S, should not be able to compute m from c.

Let us illustrate this general and informal setup with an example of substitution cipher. In this method A and B meet and agree on some secret permutation $f : \Sigma \to \Sigma$ (where Σ is the alphabet of the messages to be sent). To encrypt message $m = m_1 \dots m_n$ where $m_i \in \Sigma, A$ computes $\mathrm{Enc}(f, m) = f(m_1) \dots f(m_n)$. To decrypt $c = c_1 \dots c_n$ where $c_i \in \Sigma, B$ computes $\mathrm{Dec}(f, c) = f^{-1}(c_1) \dots f^{-1}(c_n) = m_1 \dots m_n = m$. In this example the common secret key is the permutation f. The encryption and decryption algorithms Enc and D are as specified, and are known to the adversary. We note that the substitution cipher is easy to break by an adversary who sees a moderate (as a function of the size of the alphabet Σ) number of cyphertexts. A rigorous theory of perfect secrecy based on information theory was developed by Shannon [Sha49] in 1943.

The theory assumes that the adversary has unlimited computational resources. Shannon showed that a secure (adequately defined) encryption system can exist if the size of the secret information S that A and B agree on before remote transmission is as large as the number of secret bits ever exchanged remotely using the encryption system.

An example of a private key encryption method which is secure even in presence of a computationally unbounded adversary is the one time pad. A and B agree on a secret bit string $pad = b_1 b_2 \dots b_n$, where $b_i \in_R \{0,1\}$ (i.e (pad is chosen in $\{0,1\}^n$ with uniform probability). This is the common secret key. To encrypt a message $m = m_1 m_2 \dots m_n$ where $m_i \in \{0,1\}, A$ computes $\mathrm{Enc}(pad, m) = m \oplus pad$ (bitwise exclusive or). To decrypt cyphertext $c \in \{0,1\}^n, B$ computes $\mathrm{Dec}(pad, c) = pad \oplus c = pad \oplus (m \oplus pad) = m$. It is easy to verify that $\forall m, c$ the $\mathbf{Pr}_{pad}[\mathrm{Enc}(pad, m) = c] = \frac{1}{2^n}$. From this, it can be argued that seeing c gives "no information" about what has been sent. (In the sense that the adversary's a posteriori probability of predicting m given c is no better than her a priori probability of predicting m without being given c.)

Now, suppose A wants to send B an additional message m'. If A were to send $c = \mathrm{Enc}\,(pad, m')$, then the sum of the lengths of messages m and m' will exceed the length of the secret keypad, and thus by Shannon's theory, the system cannot be secure. Indeed, the adversary can compute $\mathrm{Enc}(pad, m) \oplus \mathrm{Enc}\,(pad, m') = m \oplus m'$ which gives information about m and m' (e.g. can tell which bits of m and m' are equal and which are different). To fix this, the length of the agreed pad should be the total length of all messages ever to be exchanged over the insecure communication line.

Modern cryptography abandons the assumption that the adversary has available infinite computing resources. Moreover, it assumes instead that the adversary's computation is resource-bounded in some reasonable way. It is based on a gap between efficient algorithms for encryption for the legitimate users versus the computational infeasibility of decryption for the adversary, it requires that one have available primitives with certain special kinds of computational hardness properties. Of these, perhaps the most basic is a *one-way function* and *trapdoor functions*. Informally, a function is one-way if it is easy to compute but hard to invert. We will discuss there two primitives in this chapter. Other primitives include *pseudo-random number generators*, and *pseudorandom function families*, please see [KL14, BR05, GB01] for more details on them.

However, a central issue is where these primitives come from. Although one-way functions are widely believed to exist, and several conjectured candidate one-way functions are widely used, we currently do not know how to prove that they exist mathematically.

2.2 Preliminaries

To formally describe our assumptions (one-way functions and trapdoor function), we first need to recall some complexity theory definitions.

2.2.1 Complexity classes and standard definitions

Complexity class P

A language L is in P if and only if there exists a Turing machine $M(x)$ and a polynomial function $Q(y)$ such that on input string x

1. $x \in L$ iff M accepts x (denoted by $M(x)$).

2. M terminates after at most $Q(|x|\ )$ steps.

The class of languages P is classically considered to be those languages which are 'easily computable'. We will use this term to refer to these languages and the term 'efficient algorithm' to refer to a polynomial time Turing machine.

Complexity class NP

A language L is in NP if and only if there exists a Turing machine $M(x, y)$ and polynomials p and l such that on input string x

1. $x \in L \Rightarrow \exists y$ with $|y| \leq l(|x|)$ such that $M(x, y)$ accepts and M terminates after at most $p(|x|)$ steps.
2. $x \notin L \Rightarrow \forall y$ with $|y| \leq l(|x|), M(x, y)$ rejects.

Note that this is equivalent to the (perhaps more familiar) definition of $L \in \mathrm{NP}$ if there exists a non-deterministic polynomial time Turing machine M which accepts x if and only if $x \in L$. The string y above corresponds to the guess of the non-determinstic Turing machine.

Complexity class BPP

A language L is in BPP (Bounded-error Probabilistic Polynomial) if and only if there exists a Turing machine $M(x, y)$ and polynomials p and l such that on input string x

1. $x \in L \Rightarrow \mathrm{Pr}_{|y|<l(|x|)}[M(x, y)$ accepts $] \geq \frac{2}{3}$.
2. $x \notin L \Rightarrow \mathrm{Pr}\,|y| < l(|x|)[M(x, y)$ accepts $] \leq \frac{1}{3}$.
3. $M(x, y)$ always terminates after at most $p(|x|\ )$ steps.

We know that $\mathrm{P} \subseteq \mathrm{NP}$ and $\mathrm{P} \subseteq$ BPP. We do not know if these containments are strict although it is often conjectured to be the case. It is not known whether BPP is a subset of NP.

2.2.2 Probabilistic algorithms

The class BPP could be alternatively defined using probabilistic Turing machines (probabilistic algorithms). A *probabilistic polynomial-time Turing machine* M is a Turing machine which can flip coins as an additional primitive step, and on input string x runs for at most a polynomial in $|x|$ steps. We could have defined BPP by saying that a language L is in BPP if there exists a probabilistic polynomial-time Turing machine $M(x)$ such that when $x \in L$, the probability (over the coin tosses of the machine) that $M(x)$ accepts is greater than $\frac{2}{3}$ and when $x \notin L$ the probability (over the coin tosses of the machine) that $M(x)$ rejects is greater than $\frac{2}{3}$. The string y in the previous definition corresponds to the sequence of coin flips made by the machine M on input x.

From now on, we will consider probabilistic polynomial-time Turing machines as "efficient algorithms" (extending the term previously used for deterministic polynomial-time Turing machines). We also call the class of languages in BPP "easily computable". Note the difference between a non-deterministic Turing machine and a probabilistic Turing machine. A non-deterministic machine is not something we could implement in practice (as there may be only one good guess y which will make us accept). A probabilistic machine is something we could implement in practice by flipping coins to yield the string y (assuming, of course, that there is a source of coin flips in nature). Some notation is useful when talking about probabilistic Turing machines.

Notation for probabilistic Turing machines

Let M denote a probabilistic Turing machine (PTM). $M(x)$ will denote a probability space of the outcome of M during its run on x. The statement $z \in M(x)$ indicates that z was output by M when running on input x. $\Pr[M(x) = z]$ is the probability of z being the output of M on input x (where the probability is taken over the possible internal coin tosses made by M during its execution). $M(x, y)$ will denote the outcome of M on input x when internal coin tosses are y.

Non-uniform polynomial time

An important concept is that of polynomial-time algorithms, which can behave differently for inputs of different size, and may even be polynomial in the size of the input (rather than constant as in the traditional definition of a Turing machine).

Definition 2.2.1 *A non-uniform algorithm A is an infinite sequence of algorithms $\{M_i\}$ (one for each input size i) such that on input $x, M_{|x|}|(x)$ is run. We say that $A(x)$ accepts if and only if $M_{|x|}(x)$ accepts. We say that A is a polynomial time non-uniform algorithm if there exist polynomials P and Q such that $M_{|x|}(x)$ terminates within $P(|x|)$ steps and the size of the description of M_i (according to some standard encoding of all algorithms) is bounded by $Q(|i|$) .*

Definition 2.2.2 *We say that a language L is in $P/$ poly if $\exists$ a polynomial time non-uniform algorithm $A = \{M_i\}$ such that $x \in L$ iff $M_{|x|}(x)$ accepts.*

There are several relationships known about $\mathrm{P}/$ poly. It is clear that $P \subset \mathrm{P}/$ poly and it has been shown by Adleman that BPP $\subset \mathrm{P}/$ poly.

We will use the term 'efficient non-uniform algorithm' to refer to a non-uniform polynomial-time algorithm and the term "efficiently non-uniform computable" to refer to languages in the class $\mathrm{P/poly}$.

2.2.3 Models of adversary

We will model the computational power of the adversary in two ways. The first is the (uniform) adversary. A *uniform adversary* is any polynomial-time probabilistic algorithm. A non-uniform adversary is any non-uniform polynomial-time algorithm. Thus, the adversary can use different algorithms for different sized inputs. The non-uniform adversary is stronger than the uniform one. Thus, proving that "something" is "secure" even in the presence of a non-uniform adversary is a better result than only proving it is secure in the presence of a uniform adversary.

The weakest assumption that must be made for cryptography in the presence of a uniform adversary is that $\mathrm{P} \neq$ NP. Namely, $\exists L \in \mathrm{NP}$ such that $L \notin \mathrm{P}$. Unfortunately, this is not enough as we assumed that our adversaries could use probabilistic polynomial-time algorithms. So we further assume that BPP $\neq \mathrm{NP}$. Is that sufficient? We need that it be hard for an adversary to crack our systems most of the time. It is not sufficient that our adversary can not crack the system once in a while. Assuming that BPP $\neq \mathrm{NP}$ only means that there exists a language in $L \in \mathrm{NP}$ such that every uniform adversary makes (with high probability) the wrong decision about infinitely many inputs x when deciding whether $x \in L$. Although infinite in number, these wrong decisions may occur very infrequently (such as once for each input size).

We thus need yet a stronger assumption that will guarantee the following. There exists a language $L \in \mathrm{NP}$ such that for every sufficiently large input size n, every uniform adversary makes

(with high probability) the wrong decision on many inputs x of length n when deciding whether x is in L. Moreover, we want it to be possible, for every input size n, to generate input x of length n such that with high probability every uniform adversary will make the wrong decision on x.

The assumption that will guarantee the above is the existence of (uniform) one-way functions (2.5). The assumption that would guarantee the above in the presence of non-uniform adversary is the existence of non-uniform one way functions.

2.3 Perfect secrecy and its limitation

2.3.1 Perfect secrecy

Intuitively, we imagine an adversary who knows the probability distribution over $\mathcal{M}$; that is, the adversary knows the likelihood that different messages will be sent (as in the example given above). Then the adversary observes some cyphertext being sent by one party to the other. Ideally, observing this ciphertext should have *no effect* on the knowledge of the adversary; in other words, the *posteriori* likelihood that some message m was sent (even given the cyphertext that was seen) should be no different from the *a priori* probability that m would be sent. This should hold for any $m \in \mathcal{M}$. Furthermore, this should hold even if the adversary has unbounded computational power. This means that a cyphertext reveals nothing about the underlying plaintext, and thus an adversary who intercepts a cyphertext learns absolutely nothing about the plaintext that was encrypted.

Definition 2.3.1 (perfect secrecy) *An encryption scheme* $(\mathrm{Gen}, \mathrm{Enc}, \mathrm{Dec})$ *over a message space* $\mathcal{M}$ *is perfectly secret if for every probability distribution over* $\mathcal{M}$*, every message* $m \in \mathcal{M}$*, and every cyphertext* $c \in \mathcal{C}$ *for which* $\Pr[C = c] > 0$*:*

$$\Pr[M = m | C = c] = \Pr[M = m] \tag{2.1}$$

(The requirement that $\Pr[C = c] > 0$ is a technical one needed to prevent conditioning on a zero-probability event.) Another way of interpreting Definition is that a scheme is perfectly secret if the distributions over messages and cyphertexts are independent.

2.3.2 One-time pad (Vernam's cipher)

In 1917, Vernam patented a cipher that obtains perfect secrecy. There was no proof of this fact at the time (there was not yet a notion of what perfect secrecy was). Instead, approximately 25 years later, Shannon [Sha49] introduced the notion of perfect secrecy and demonstrated that the one-time pad (sometimes known as Vernam's cipher) achieves this level of security.

Let $a \oplus b$ denote the *bitwise exclusive-or* (XOR) of two binary strings a and b (i.e., if $a = a_1, \ldots, a_l$ and $b = b_1, \ldots, b_l$ then $a \oplus b = a_1 \oplus b_1, \ldots, a_l \oplus b_l$). The one-time pad encryption scheme is defined as follows:

1. Fix an integer $l > 0$. Then the message space $\mathcal{M}$, key space $\mathcal{K}$, and cyphertext space $\mathcal{C}$ are all equal to $\{0,1\}^l$ (i.e., the set of all binary strings of length l).

2. The key-generation algorithm Gen works by choosing a string from $\mathcal{K} = \{0,1\}^l$ according to the uniform distribution (i.e., each of the 2^l strings in the space is chosen as the key with probability 2^{-l}.)

3. Encryption Enc works as follows: given a key $k \in \{0,1\}^l$ and a message $m \in \{0,1\}^l$, outputs $c := k \oplus m$.

4. Decryption Dec works as follows: given a key $k \in \{0,1\}^l$ and a cyphertext $c \in \{0,1\}^l$, outputs $m := k \oplus c$.

Before discussing the security of the one-time pad, we note that for every k and every m it holds that $\mathrm{Dec}_k(\mathrm{Enc}_k(m)) = k \oplus k \oplus m = m$ and so the one-time pad constitutes a legal encryption scheme.

Theorem 2.3.2 *The one-time pad is a perfectly-secret encryption scheme.*

Proof: We work directly with the definition of perfect secrecy (Definition 2.3.1), though with our convention that all messages occur with non-zero probability. (For the one-time pad, this implies that all cyphertexts occur with non-zero probability.) Fix some distribution over $\mathcal{M}$ and arbitrary $m_0 \in \mathcal{M}$ and $c \in \mathcal{C}$. The key observation is that, for every $m \in \mathcal{M}$,

$$\Pr[C = c | M = m] = \Pr[M \oplus K = c | M = m] \tag{2.2}$$
$$= \Pr[m \oplus K = c] = \Pr[K = m \oplus c] = 2^{-l} \tag{2.3}$$

A simple calculation (using Bayes' theorem for the first equality) then gives

$$\Pr[M = m_0 | C = c_0] = \frac{\Pr[M = m_0 \wedge C = c_0]}{\Pr[C = c]} \tag{2.4}$$
$$= \frac{\Pr[C = c_0 | M = m_0] \cdot \Pr[M = m_0]}{\sum_m \Pr[C = c | M = m] \cdot \Pr[M = m]} \tag{2.5}$$
$$= \frac{2^{-l} \cdot \Pr[M = m_0]}{\sum_m 2^{-l} \cdot \Pr[M = m]} \tag{2.6}$$
$$= \frac{\Pr[M = m_0]}{\sum_m \Pr[M = m]} = Pr[M = m_0] \tag{2.7}$$

as required by Definition 2.3.1. □

2.3.3 Limitations of perfect secrecy

In the above section, we conclude that perfect secrecy is attainable with a one-time pad. However, the scheme has several drawbacks. Most prominent is that *the key is required to be as long as the message*. This limits the applicability of the scheme if we want to send very long messages (as it may be difficult to store a very long key securely) or if we don't know in advance an upper bound on how long the message will be (since we can't share a key of unbounded length). Moreover, as the name indicates, the one-time pad scheme is only "secure" if used once (with the same key).

Theorem 2.3.3 *Let* $(\mathrm{Gen}; \mathrm{Enc}; \mathrm{Dec})$ *be a perfectly-secret encryption scheme over a message space* $\mathcal{M}$*, and let* $\mathcal{K}$ *be the key space as determined by* Gen*. Then* $|\mathcal{K}| \geq |\mathcal{M}|$.

Proof: We show that if $|\mathcal{K}| < |\mathcal{M}|$ then the scheme is not perfectly secret. Assume $|\mathcal{K}| < |\mathcal{M}|$. Take the uniform distribution over $\mathcal{M}$ and let $m \in \mathcal{M}$ be arbitrary. Let c be a cyphertext that corresponds to a possible encryption of m; i.e., there exists a $k \in \mathcal{K}$ such that $\mathrm{Enc}_k(m) = c$. (If Enc is randomized, this means there is some non-zero probability that $\mathrm{Enc}_k(m)$ outputs c.) By correctness, we know that $\mathrm{Dec}_k(c) = m$.

Consider the set $\mathcal{M}(c)$ of all possible message that corresponds to c; that is

$$\mathcal{M}(c) = \{\hat{m} | \hat{m} = \mathrm{Dec}_{\hat{k}}(c) \text{ for some } \hat{k} \in \mathcal{K}\} \tag{2.8}$$

We know that $m \in \mathcal{M}(c)$. Furthermore, $|\mathcal{M}(c)| \leq |\mathcal{K}|$ since for each message $\hat{m} \in \mathcal{M}(c)$ we can identify at least one key $\hat{k} \in \mathcal{K}$ for which $\hat{m} = \mathrm{Dec}_{\hat{k}}(c)$. This means there is some $m' \in \mathcal{M}$ with $m' \neq m$ such that $m' \notin \mathcal{M}(c)$. But then

$$\Pr[M = m' | C = c] = 0 \neq \Pr[M = m'] \tag{2.9}$$

□

2.4 A computational approach to cryptography

In previous sections, we presented cryptographic schemes that can be mathematically proven secure, even when the adversary has unlimited computational power. Such schemes are called *information-theoretically secure*, or *perfectly secure*, because their security is because the adversary does not have enough "information" to succeed in its attack, regardless of the adversary's computational power. In particular, as we have discussed, the cyphertext in a perfectly-secret encryption scheme does not contain any information about the plaintext (assuming the key is unknown).

Information-theoretic security stands in stark contrast to computational security that is the aim of most modern cryptographic constructions. Modern encryption schemes have the property that they can be broken given enough time and computation, and so they do not satisfy Definition 2.3.1. Nevertheless, under certain assumptions, the amount of computation needed to break these encryption schemes would take over many lifetimes to carry out even using the fastest available supercomputers. For all practical purposes, this level of security suffices.

Computational security is weaker than information-theoretic security. It also currently relies on assumptions ($\mathrm{P} \neq \mathrm{NP}$) whereas no assumptions are needed to achieve the latter (as we have seen in the case of encryption). Even granting the fact that computational security suffices for all practical purposes, why do we give up on the idea of achieving perfect secrecy? The limitations of perfect secrecy give one reason why modern cryptography has taken this route. Thus, despite its mathematical appeal, it is necessary to compromise on perfect secrecy to obtain practical cryptographic schemes.

The basic idea behind computational security is to show that "*a cipher must be practical, if not mathematically, indecipherable*. It is sufficient to use a scheme that cannot be broken in "reasonable time" with any reasonable probability of success. In Kerckhoff's language, a scheme that is "practically indecipherable". Thus a computational approach incorporates two relaxations of the notion of perfect secrecy:

1. Security is only preserved against adversaries running an "*efficient algorithm*" in probabilistic polynomial time. We equate the notion of efficient algorithms" with (probabilistic) algorithms running in time polynomial in n, meaning that for some constants a, c the algorithm runs in

time $a \cdot n^c$ on security parameter n. We require that honest parties run in polynomial time and only be concerned with achieving security against polynomial-time adversaries. We stress that the adversary must run in polynomial time, maybe much more powerful (and run much longer) than the honest parties.

2. Adversaries can potentially succeed with some *very small* probability. We equate the notion of "*small probability of success*" with success probabilities *smaller than any inverse-polynomial in n*, meaning that for every constant c, the adversary's success probability is smaller than n^{-c} for large enough values of n (see Definition 2.4.1). A function that grows slower than any inverse polynomial is called negligible.

Definition 2.4.1 (Negligible function) *A function f is negligible if for every polynomial $p(\cdot)$ there exist an N such that for all integers $n > N$ it holds that $f(n) < \frac{1}{p(n)}$.*

The above definition considers the success probability of an algorithm negligible if, as a function of the input length, the success probability is bounded by any polynomial fraction. It follows that repeating the algorithm polynomially (in the input length) often yields a new algorithm that also has a negligible success probability. In other words, events that occur with negligible (in n) probability remain negligible even if the experiment is repeated or polynomially (in k) many times. Hence, defining negligible success as "occurring with a probability smaller than any polynomial fraction" is naturally coupled with defining feasible as "computed within polynomial time."

We can now define computational security:

Definition 2.4.2 (Computational security) *Let $(\mathrm{Enc}, \mathrm{Dec})$ be an encryption scheme that uses n-bit keys k to encrypt $l(n)$-length message. Then, $(\mathrm{Enc}, \mathrm{Dec})$ is computationally secure if for every probabilistic polynomial time algorithm $A : \{0,1\}^* \to \{0,1\}$, polynomially bounded $\epsilon : \{0,1\}^* \to [0,1]$, n, and $m_0, m_1 \in \{0,1\}^{l(n)}$,*

$$|\Pr[A(\mathrm{Enc}_k(m_0) = 1) - \Pr[A(\mathrm{Enc}_k(m_1) = 1)]| < \epsilon(n) \tag{2.10}$$

2.5 One-way and trapdoor functions

As modern cryptography is based on a gap between efficient algorithms for encryption for the legitimate users versus the computational in-feasibility of decryption for the adversary, it requires that one have available primitives with certain special kinds of computational hardness properties. Of these, perhaps the most basic is a one-way function.

2.5.1 One-way functions

One Way functions, namely functions that are "easy" to compute and "hard" to invert, are an extremely important cryptographic primitive. Probably the best known and simplest use of one-way functions is for passwords. Namely, in a time-shared computer system, instead of storing a table of login passwords, one can store, for each password w, the value $f(w)$. Passwords can easily be checked for correctness at login, but even the system administrator can not deduce any user's password by examining the stored table.

Definition 2.5.1 (One-way function) *A function $f : \{0,1\}^* \to \{0,1\}^*$ is one-way if:*

1. *there exists a probabilistic polynomial time (PPT) that on input x outputs $f(x)$;*
2. *For every PPT algorithm A there is a negligible function ν_A such that for sufficiently large k,*

$$\Pr\left[f(z) = y : x \stackrel{\$}{\leftarrow} \{0,1\}^k; y \leftarrow f(x); z \leftarrow A\left(1^k, y\right)\right] \leq \nu_A(k) \tag{2.11}$$

Few remarks on the definition:

1. The definition suggests that an adversary is not unable to invert the function, but has a low probability of doing so, where the probability distribution is taken over the input x to the one-way function where x if of length k, and the possible coin tosses of the adversary. Namely, x is chosen at random and y is set to $f(x)$.
2. The adversary is not asked to find x; that would be pretty near impossible. It is asked to find some inverse of y. Naturally, if the function is 1-1 then the only inverse is x.
3. Note that the adversary algorithm takes as input $f(x)$ and the security parameter 1^k (expressed in unary notation) which corresponds to the binary length of x. This represents the fact that the adversary can work in time polynomial in $|x|$, even if $f(x)$ happens to be much shorter. This rules out the possibility that a function is considered one-way merely because the inverting algorithm does not have enough time to print the output. Consider for example the function defined as $f(x) = y$ where y is the log k least significant bits of x where $|x| = k$. since the $|f(x)| = \log|x|$ no algorithm can invert f in time polynomial in $|f(x)|$, yet there exists an obvious algorithm which finds an inverse of $f(x)$ in time polynomial in $|x|$. Note that in the special case of length preserving functions f (i.e., $|f(x)| = |x|$ for all x 's), the auxiliary input is redundant.

2.5.2 Trapdoor functions

Informally, a trapdoor function f is a one-way function with an extra property. There also exists a secret inverse function (the trapdoor) that allows its possessor to efficiently invert f at any point in the domain of his choosing. It should be easy to compute f on any point but infeasible to invert f on any point without knowledge of the inverse function. Moreover, it should be easy to generate matched pairs of f 's and corresponding trapdoor. Once a matched pair is generated, the publication of f should not reveal how to compute its inverse on any point.

Definition 2.5.2 (Trapdoor one-way function) *A trapdoor function is a one-way function $f : \{0,1\}^* \to \{0,1\}^*$ such that there exists a polynomial p and a probabilistic polynomial time algorithm I such the for every k there exists an $t_k \in \{0,1\}^*$ such that $|t_k| \leq p(k)$ and for all $x \in \{0,1\}, I\left(f(x), t_k\right) = y$ such that $f(y) = f(x)$.*

An example of a function which may be trapdoor if factoring integers is hard was proposed by Rabin[170]. Let $f(x,n) = x^2$ mod n where $n = pq$ a product of two primes and $x \in Z_n^*$. Rabin[170] has shown that inverting f is easy iff factoring composite numbers product of two primes is easy.

The most famous candidate trapdoor function is the RSA[176] function. Let $N = pq$ be a product of two primes. It is believed that such an N is hard to factor. The function is $f(x) = x^e \text{mod } N$ where e is relatively prime to $(p-1)(q-1)$. The trapdoor is the primes p, q, knowledge, which allows one to invert f efficiently. The function f seems to be one-way. To date, the best attack is to try to factor N, which seems computationally infeasible.

2.5.3 Block ciphers

Block ciphers are the central tool in designing protocols for shared-key cryptography (aka. symmetric) cryptography. They are the leading available "technology" we have at our disposal.

A block cipher is a function $E : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$. This notation means that E takes two inputs: a k-bit string and the other an n-bit string, and returns an n-bit string. The first input is the key. The second might be called the plaintext, and the output might be called a cyphertext. The key-length k and the block-length n are parameters associated with the block cipher. They vary from block cipher to block cipher, as of course does the design of the algorithm itself.

For each key $K \in \{0,1\}^k$ we let $E_K : \{0,1\}^n \to \{0,1\}^n$ be the function defined by $E_K(M) = E(K;M)$. For any block cipher, and any key K, it is required that the function E_K be a permutation on $\{0,1\}^n$. This means that it is a bijection (ie., a one-to-one and onto function) of $\{0,1\}^n$ to $\{0,1\}^n$. (For every $C \in \{0,1\}^n$ there is exactly one $M \in \{0,1\}^n$ such that $E_K(M) = C$.) Accordingly E_K has an inverse, and we denote it E_K^{-1}. This function also maps $\{0,1\}^n \to \{0,1\}^n$, and of course we have $E_K^{-1}(E_K(M)) = M$ and $E_K(E_K^{-1}(C)) = C$ for all $M, C \in \{0,1\}^n$. We let $E^{-1} : \{0,1\}^k \times \{0,1\}^n \to \{0,1\}^n$ be defined by $E^{-1}(K,C) = E_K^{-1}(C)$. This is the inverse block cipher to E.

The block cipher E is a public and fully specified algorithm. Both the cipher E and its inverse E^{-1} should be easily computable, meaning given K, M we can readily compute $E(K,M)$, and given K, C we can readily compute $E^{-1}(K,C)$. By "readily compute," we mean that there are public and relatively efficient programs available for these tasks.

A random key K is chosen in typical usage and kept secret between a pair of users. The function E_K is then used by the two parties to process data in some way before they send it to each other. Typically, we will assume the adversary will be able to obtain some input-output examples for E_K, meaning pairs of the form (M,C) where $C = E_K(M)$. However, ordinarily, the adversary will not be shown the key K. Security relies on the key's secrecy. So, as a first cut, one might think of the adversary's goal as recovering the key K given some input-output examples of E_K. The block cipher should be designed to make this task computationally tricky. (A more refined view is that the adversary's goal is key-recovery, seeing that security against key-recovery is a necessary but not sufficient condition for the security of a block cipher.)

Data encryption standards

The Data Encryption Standard, or DES, is one of the most important examples of a Feistel cryptosystem. DES was the result of a contest set by the U.S. National Bureau of Standards (now called the NIST) in 1973 and adopted as a standard for unclassified applications in 1977. The winning standard was developed at IBM as a modification of the previous system called LUCIFER. The DES is widely used for the encryption of PINs, bank transactions, and the like. DES is also specified as an Australian banking standard. The DES is an example of a Feistel cipher, which operates on blocks of 64 bits at a time, with an input key of 64 bits. Every 8th bit in the input key is a parity check bit, which means that the key size is effectively reduced to 56 bits.

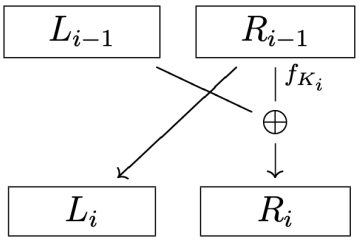
Product ciphers and Feistel ciphers

As a precursor to the description of DES, we make the following definitions, which describe various aspects of the constructions, specific properties, and design components of DES.

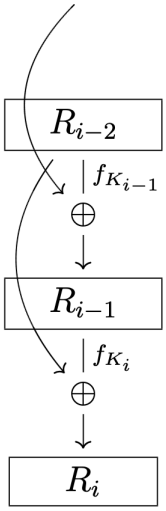
A *product cipher* is a composite of two or more elementary ciphers to produce a more secure cipher than any individual components. A *substitution-permutation network* is a product cipher composed of stages, each involving substitutions and permutations, in which the blocks can be partitioned into smaller blocks for substitutions and recombined with permutations. An *iterated block cipher* is a block cipher involving the repetition of an internal round function, which may involve a key as input. Each of the sequential steps is termed a "round."

We now describe in more detail an example of an iterated block cipher, called a *Feistel cipher*. In a Feistel the input block is of even length $2t$, of the form L_0R_0, and outputs cyphertext of the form R_rL_r. For each i such that $1 \leq i \leq r$, the round map takes $L_{i-1}R_{i-1}$ to L_iR_i, where $L_i = R_{i-1}$ and $R_i = L_{i-1} \oplus f_{K_i}(R_{i-1})$, where f_{Ki} is a cipher which depends only on an input subkey K_i, which is derived from the cipher key K.

The flow of the Feistel cipher therefore looks something like: We can eliminate the L_i by



defining $R_{-1} = L_0$, so that the input is $R_{-1}R_0$, and the round operations are of the form $R_i = R_{i-2} \oplus f_{K_i}(R_{i-1})$, in which case the flow diagram looks like: The final output of the Feistel cipher is



the inverted pair $R_rL_r = R_rR_{r-1}$, which allows the Feistel cipher to be inverted by running through the same algorithm with the key sequence reversed.

The DES is a 16-round Feistel cipher, preceded and followed by an initial permutation IP and its inverse IP^{-1}. That is, we start with a message M, and take $L_0R_0 = IP(M)$ as input to the Feistel cipher, with output $IP^{-1}(R_{16}L_{16})$. The 64-bits of the key are used to generate 16 internal keys, each of 48 bits. The round function's steps f_K is given by the following sequence, taking on 32-bit strings, expanding them to 48-bit strings, and applying a 48-bit block function.

1. Apply a fixed *expansion permutation E*- this function is a permutation of 32 bits with repetition to generate a 48-block $E(R_i)$.

2. Compute the bit sum of $E(R_i)$ with the 48-bit key K_i, and write this as 8 blocks $B_1, \ldots, B_8$ of 6 bits each.

3. Apply to each block $B_j = b_1b_2b_3b_4b_5b_6$ a substitution S_j. These substitutions are specified by $S-boxes$, which describes the substitution as a look-up table. The output of the substitution cipher is 48 bit string C_j, which results in a 32 bit string $C_1 \ldots C_8$.

4. Apply a fixed 32-bit permutation P to $C_1 \ldots C_8$ and output the result $f_{K_i}(R)$.

63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
ca	82	c9	7d	fa	59	47	f0	ad	d4	a2	af	9c	a4	72	c0
b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Figure 2.1: The AES S-box, which is a function $S : \{0,1\}^8 \to \{0,1\}^8$ specified by the following list. All values in hexadecimal. The meaning is: $S(00) = 63, S(01) = 7c, \ldots, S(ff) = 16$

Advance encryption schemes (AES)

In 1997, the NIST called for submissions for a new standard to replace the aging DES. The contest terminated in November 2000 with selecting the Rijndael cryptosystem as the Advanced Encryption Standard (AES).

The Rijndael cryptosystem operates on 128-bit blocks, arranged as 4×4 matrices with 8-bit entries. The algorithm consists of multiple iterations of a round cipher, each of which is the composition of the following four basic steps:

1. *ByteSub* transformation. This step is a nonlinear substitution, given by a S-box (Figure 2.1), designed to resist linear and differential cryptanalysis.

2. *ShiftRow* transformation. Provides a linear mixing for diffusion of plaintext bits.

3. *MixColumn* transformation. Provides a similar as in the ShiftRow step.

4. *AddRoundKey* transformation. Bitwise XOR with the round key.

The Advanced Encryption Standards allows Rhijndael key lengths 128, 192, or 256 bits.

The eight-bit byte blocks which form the matrix entries are interpreted as elements of the finite field $2^8 = 256$ elements. The finite field is represented by the quotient ring

$$\mathbb{F}_{2^8} = \mathbb{F}_2[X]/(X^8 + X^4 + X^3 + X + 1), \tag{2.12}$$

whose elements are polynomials $c_7X^7 + c_6X^6 + c_5X^5 + c_4X^4 + c_3X^3 + c_2X^2 + c_1X + c_0$.

2.5.4 Limitations of computational security

The computational model for security is based on unproven intractability results. Thus it is not possible to state unconditional security results for the most ciphers used in our days. Computers and algorithms improve over time and so does the ability of an adversary to break cryptographic complexity assumptions and protocols. It may be feasible to make a good estimate as to which computational problems are hard today, and which encryption schemes unbroken. But it is very difficult to make more than an educated guess as to which cryptographic schemes will be secure, say, ten years from now. Key length recommendations can only be made based on the assumption that progress continues at a similar rate as today; unexpected algorithmic progress and future technologies like quantum computers can render even the most paranoid choices for the key length obsolete.

This situation is very problematic if we wish to run cryptographic protocols on highly sensitive data such as medical or financial data or government secrets. Such data often has to stay confidential for many decades. But an adversary might intercept messages from a protocol that is secure today, store them, and some decades later, when the underlying cryptosystems have been broken, decrypt them. For highly sensitive data, this would not be an acceptable risk.

Shor's algorithm, exploring the power of quantum computing, enables theoretically to factor integers in a reasonable time that is proportional to their logarithm. It is thus a factorization in a linear time as a function of the number of key bits. This could be detrimental to all public keybased cryptography. In 2019, Google researchers published an algorithm allowing to quickly break an RSA key (of 2048 bits) and with "only" 20 million qubits having an error rate of 0.1% and in a calculation carried out in 8 hours.

Shor's algorithm applied to RSA public key breaking could however have quite a negative impact on most Internet use cases. It is indeed integrated in the TLS and SSL protocols that protect websites and file transfers via HTTPS and FTP, in the IPSEC protocol that protects IP V4 in the IKE sub-protocol, in the SSH protocol for machines remote access and in the PGP protocol that is sometimes used to encrypt emails. RSA and derivatives are also used in many HSM (Hardware Security Modules) such as in cars ECU (Electronic Central Units).

The threat also concerns software electronic signatures and therefore their automatic updates, VPNs used for remote access to protected corporate networks, email security with S/MIME, various online payment systems, DSA (Digital Signature Algorithm, an electronic signature protocol), Diffie-Hellman codes (used for sending symmetrical keys) as well as ECDH, ECDSA and 3-DES elliptic curve cryptography. The Signal protocol used in Whatsapp would also be in the spotlight. So a lot of Internet security is more or less in the line of sight.

2.6 Information-theoretic security

One way out from the limitation of computational security is to use protocols with unconditional (information-theoretical) security. Information-theoretic provides a proper definition of security because nothing is assumed on the computational capacity of the eavesdropper. It also allows for precise security results to be stated. This section presented an overview of Information-Theoretic Security, stating some of the most famous results related to this subject.

2.6.1 Shannon's model for perfect secrecy

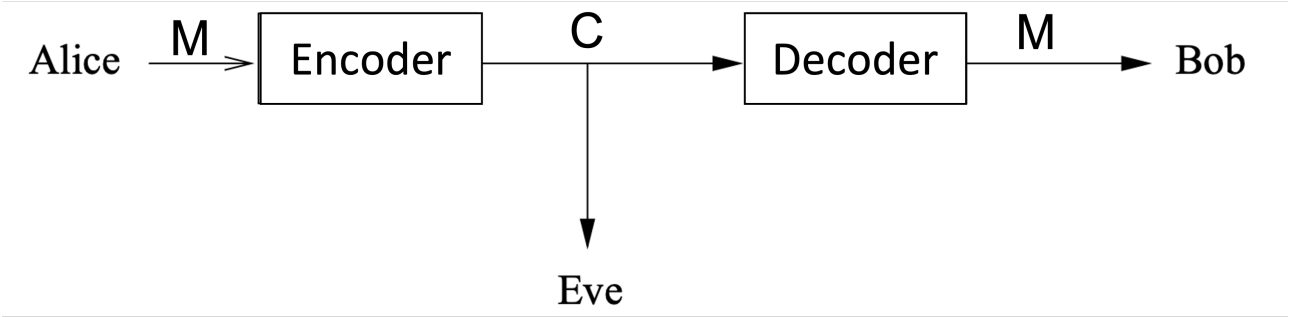


Figure 2.2: Shannon's model for a secrecy system.

Shannon [Sha49] introduced a model of a cryptosystem (see Figure 2.2). Where Eve has perfect access to the insecure channel, i.e., she receives an exact copy of the cryptogram C, where Alice obtains C as a function of the plaintext M and a secret key K, shared by Alice and Bob. According to Shannon's definition, a cipher system is perfect if

$$I(M;C) = 0 \tag{2.13}$$

i.e., Eve gains no knowledge about M by knowing C. Notice that in this definition of a secure cipher system, no assumption about the enemy's computational power is made, making the information-theoretic security more desirable in cryptography than computational security.

Wiretap Channel

One of the features in Shannon's model that leads to his pessimistic result is the fact that he assumes that the enemy Eve has perfect access to the cryptogram C, i.e., it is assumed that the channel from Alice to Eve has the same capacity as the channel from Alice to Bob. Therefore, the key to guaranteeing perfect secrecy is to modify Shannon's model such that the enemy has not the same information as the legitimate receiver. Wyner [Wyn75] and later Csiszár and Körner [CK78a] proposed a new model, called the *wiretap channel*.

In this model, the legitimate users communicate over the main channel, and an eavesdropper has access to the messages received by the legitimate receiver over a wiretap channel. The general setup for this model is shown in Figure 2.3.

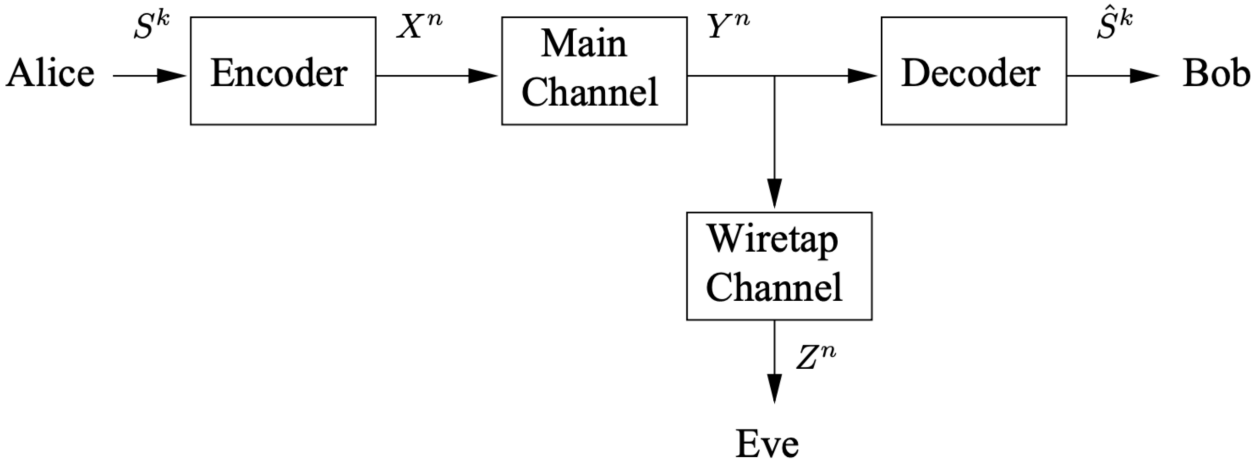


Figure 2.3: Wiretap channel model.

2.6.2 Using public discussion to establish a perfect secret key

More recently, Maurer [Mau93a] made a breakthrough by developing a new model and proving that, for wiretap channel model, a strictly positive secrecy capacity is possible, even if Eve's channel is stronger than the legitimate users' channel. Maurer's model's main feature is that an insecure public channel (yet authenticated) is used to generate a secret key.

First, we define the model without the public channel and state Maurer's definition for secrecy capacity. An illustration of this model is in Figure 2.4.

Definition 2.6.1 *The broadcast channel of interest in the following is defined as:*

- *the source is the sequence* $\{S_i\}_{i=1}^{\infty}$*, where* S_i *is a binary random variable,* $\forall i$*;*
- *the main channel has a finite input alphabet* $\mathcal{X}$ *and a finite output alphabet* $\mathcal{Y}$*;*
- *the wiretap channel has the same input as the main channel, and a finite output alphabet* $\mathcal{Z}$*;*
- *the channel behavior is completely specified by the conditional probability distribution* $P(Y = y, Z = z|X = x)$*, which we refer to as* $P_{YZ|X}$*;*
- *the encoder is a (possibly probabilistic) function* $e : \{0,1\}^k \to \mathcal{X}^n$*, where* R *is the rate and* $k = [nR]$*; the decoder is a function* $d : \mathcal{Y}^n \to \{0,1\}^k$*.*

Definition 2.6.2 *The secrecy capacity of a broadcast channel specified by* $P_{YZ|X}$ *is the maximum rate* R *for which, for every* $\epsilon > 0$*, for all sufficiently large* n*, there exists an encoder-decoder such that for* S *uniformly distributed over* $\{0,1\}^k$ *the following two conditions are satisfied:*

- $\mathcal{P}(d(Y) \neq S) < \epsilon$*, where* $X = e(S)$*;*
- $\frac{1}{k}H(S|Z^n) > 1 - \epsilon$*.*

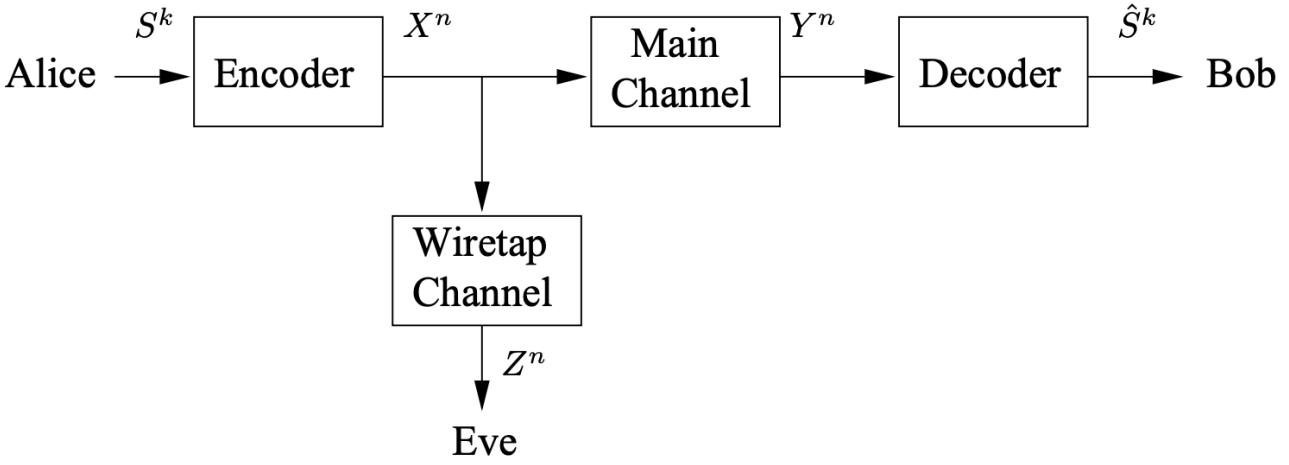


Figure 2.4: Maurer's broadcast channel without a public channel.

Maurer also noticed that, in the previous definition, it would be equivalent the two conditions to hold for all probability distributions.

Now, consider a broadcast channel for which both the main and the wiretap channel are independent binary symmetric channels, i.e.

$$P_{YZ|X} = P_{Y|X} P_{Z|X} \tag{2.14}$$

$$P_{Y|X}(y|x) = \begin{cases} 1-\epsilon, & \text{if } x = y \\ \epsilon, & \text{if } x \neq y \end{cases} \tag{2.15}$$

and

$$P_{Z|X}(z|x) = \begin{cases} 1-\delta, & \text{if } x = z \\ \delta, & \text{if } x \neq z \end{cases} \tag{2.16}$$

Without loss of generality, consider the case $\epsilon \leq 1/2, \delta \leq 1/2$. Denote this channel by $D(\epsilon, \delta)$. The next result characterizes the secrecy capacity for this channel. It shows that, as expected, the secrecy capacity for this channel is only strictly positive if the legitimate user's channel is better than Eve's channel.

Lemma 2.6.1 *The secrecy capacity of the binary broadcast channel $D(\epsilon, \delta)$ is given by:*

$$C_S(D(\epsilon, \delta)) = \begin{cases} h(\delta) - h(\epsilon), & \text{if } \delta > \epsilon \\ 0, & \text{otherwise} \end{cases}, \tag{2.17}$$

where, $h(p)$ is the binary entropy function, i.e., $h(p) = -p\log(p) - (1-p)\log(1-p)$.

To overcome the need for legitimate users over the eavesdropper, Maurer introduced a public channel, insecure but with unconditional secure authentication. Moreover, it is assumed that Eve can listen to the communication over the public channel but cannot perform an identity spoofing attack. For an illustration of this model, see Figure 2.5

Definition 2.6.3 *The secrecy capacity with public discussion denoted $\hat{C}(P_{YZ|Z})$, is the secrecy capacity of the broadcast channel defined in Definition 2.6.1, with the additional feature that Alice and Bob can communicate over an insecure (yet authenticated) public channel.*

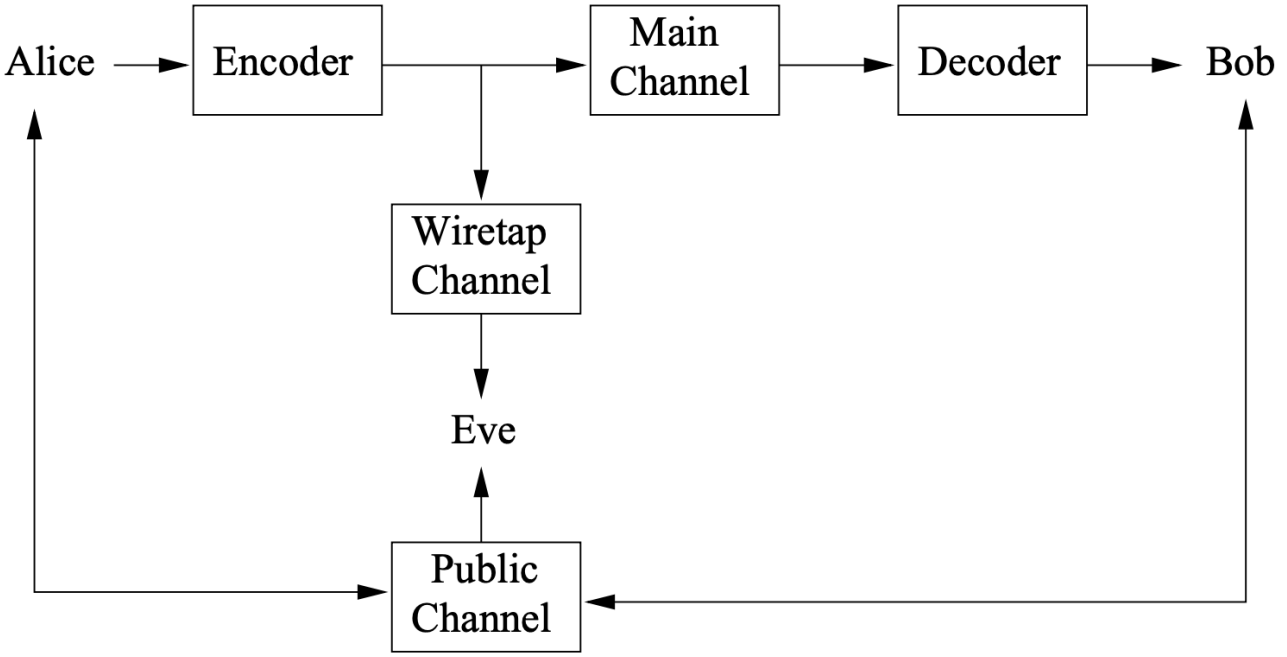


Figure 2.5: Maurer's broadcast channel with a public channel.

The next theorem characterizes the secrecy capacity with public discussion, showing that even if the eavesdropper has a better channel than the legitimate users, perfect secure communication can still be performed.

Theorem 2.6.4 *The secrecy capacity with public discussion of a broadcast channel is given by*

$$\hat{C}(D(\epsilon,\delta)) = h(\epsilon+\delta-2\epsilon\delta) - h(\epsilon) \tag{2.18}$$

Moreover, $\hat{C}(D(\epsilon,\delta))$ is stricly positive unless $\epsilon = 0.5$, $\delta = 0$ or $\delta = 1$, i.e. unless X and Y are statistically independent or Z uniquely determines X

Proof: To sketch the proof of the above theorem , the idea is to construct a conceptual broadcast channel similar to the broadcast channel of Wyner [Wyn75], such that the conceptual main channel is equivalent to the real main channel between Alice and Bob, and the conceptual wiretap channel is a cascade of the real main channel and the real wiretap channel.

Alice sends a random bit X over the real broadcast channel, with $\mathcal{P}(X=0) = \mathcal{P}(X=1) = 1/2$. Let E and D denote the (independent) error bits of the main and of Eve's channel, respectively, i.e. let $Y = X + E$ and $Z = X + D$ where $\mathcal{P}(E=1) = \epsilon$ and $\mathcal{P}(D=1) = \delta$. Bob chooses a bit V and sends $W = Y + V$ over the public channel. Alice computes

$$W + X = V + E,$$

thus Alice receives V with error probability ϵ. Eve knows $Z = X + D$ and $W = X + E + V$, and can compute

$$Z + W = V + E + D.$$

In fact, it is easy to prove that

$$H(V|ZW) = H(V|Z+W),$$

thus Eve can indeed compute $Z + W$ and discard Z and W. Now, it is easy to prove that the conceptual broadcast channel can be seen as $D(\epsilon, \epsilon + \delta - 2\epsilon\delta)$. □

2.6.3 Key establishment from correlated classical data

In this section we study the broadcast channel's use with a public channel to develop unconditional secure secret key agreement protocols. Throughout this thesis, we are interested in the setting where, at the end of any key establishment protocol, interactive parties hold only correlated classical data, i.e., a setting where secret keys can be established from correlated classical information.

The problem of generating a shared secret key using correlated classical data over a public discussion was considered in [Mau93a, MW00, MW99], where two authorized and trusted parties Alice (sender) and Bob (receiver), interact over an insecure communication channel to exchange secret keys S, about which an unauthorized party Eve does not gain any useful information.

General setting

We briefly describe the general setting as considered in [Mau93a]. The setting assumes Alice, Bob, and Eve know random variables $X \in \mathcal{X}$, $Y \in \mathcal{Y}$, and $Z \in \mathcal{Z}$, respectively, distributed according to the joint probability distribution P_{XYZ}, and that Eve has no information about X and Y other than through her knowledge of Z. Alice and Bob share no secret key initially (other than possibly a short key required for authenticating the public classical channel) but are assumed to know P_{XYZ} or at least an upper bound on the quality of Eve's channel.

The protocol and the codes used by Alice and Bob are known to Eve. Every message communicated between Alice and Bob can be intercepted by Eve, i.e., Eve's tapping channel is assumed to have full access to the input of Alice and Bob's main channel, but it is assumed that Eve cannot insert fraudulent messages nor modify messages on this public channel without being detected.

Alice and Bob use a protocol in which at each odd step Alice sends a message $\{C_1, C_3, \ldots, C_{n-1}\}$ to Bob depending on X and at each even step Bob sends a message $\{C_2, C_4, \ldots, C_n\}$ depending on Y. After n steps in the protocol Alice computes a secret key S_A as a function of X and $\boldsymbol{C_n} = [C_1, \ldots, C_n]$ Bob computes a secret key S_B as a function of Y and $\boldsymbol{C_n}$. Their goal is to maximize the $H(S)$ under the conditions that S_A and S_B agree with very high probability and that Eve has very little information about either S_A or S_B.

The goal of an adversary Eve is to gain as much information as possible on the output keys of Alice and Bob without being detected using the classical random variable $\boldsymbol{Z_n}$ and $\boldsymbol{C_n}$.

Security definition

Definition 2.6.5 *A secret key agreement protocol as described above is (ϵ, δ)-secure if, for some specified (small) ϵ and δ, the following conditions hold:*

1. *For odd i, $H(C_i|\boldsymbol{C_{i-1}}X) = 0$;*
2. *For even i, $H(C_i|\boldsymbol{C_{i-1}}Y) = 0$;*
3. *$H(S|C^tX) = 0$;*
4. *$H(S'|C^tY) = 0$;*
5. *$\mathcal{P}(S \neq S') \leq \epsilon$;*

6. $I(S; C^t Z) \leq \delta$.

Conditions 1-4 guarantee that Alice and Bob have no uncertainty regarding the protocol procedures. Condition 5 guarantees that Alice and Bob agree on the same key with probability $1 - \epsilon$. Finally, condition 6 guarantees that, given that Eve knows all the messages exchanged between Alice and Bob over the public channel during the protocol and the output of her channel, the key that Eve has is upper bounded by δ.

The next theorem provides an upper bound on the key's size that Alice and Bob agree via a (ϵ, δ)-secure key agreement protocol.

Theorem 2.6.6 *For every (ϵ, δ)-secure key agreement protocol, we have that*

$$H(S) \leq \min[I(X;Y), I(X;Y|Z)] + \delta|h(\epsilon) + \epsilon \log(|S| - 1) \tag{2.19}$$

To be able to provide a lower bound on the key size we need to make further assumptions. Consider the case when Alice, Bob and Eve receive $X^N = [X_1, \ldots, X_N]$, $Y^N = [Y_1, \ldots, Y^N]$ and $Z^N = [Z_1, \ldots, Z_N]$, where $P_{X^N Y^N Z^N} = \Pi_{i=1}^n P_{X_i Y_i Z_i}$. Next, we define the secret key rate, a quantity of interest in the rest of this section.

Definition 2.6.7 *The secret key rate of X and Y with respect to Z, denoted $S(X;Y||Z)$, is the maximum rate R such that, for every $\epsilon > 0$, there exists a protocol, for sufficiently large n, satisfying conditions 1-5 in Definition 2.6.5 (with X and Y replaced by X^n and Y^n, respectively) and also the two following conditions:*

- $\frac{1}{n} I(S; C^t Z^n) \leq \epsilon$
- $\frac{1}{n} H(S) \geq R - \epsilon$

The next result provides an upper and a lower bound for the secret key rate.

Theorem 2.6.8 *The secret key rate $S(X;Y||Z)$ verifies*

- $S(X;Y||Z) \leq \min[I(X;Y), I(X;Y|Z)]$;
- $S(X;Y||Z) \geq \max[I(Y;X) - I(Z;X), I(X;Y) - I(Z;Y)]$.

The upper bound for the secret key rate in the previous theorem shows that if Eve has less information about Y than Alice or less information about X than Bob, then such a difference of information can be exploited.

The next theorem provides bounds on the secrecy capacity with public discussion of a general broadcast channel.

Theorem 2.6.9 *The secret capacity with public discussion, $\hat{C}_S(P_{YZ|X})$, of a broadcast channel specified by $P_{YZ|X}$ verifies*

$$\hat{C}_S(P_{YZ|X}) \leq \min[\max_{P_X} I(X;Y), \max_{P_X} I(X;Y|Z)] \tag{2.20}$$

The lower bounds on the secret key rate for key establishment using classical correlated data, in the asymptotic limit ($n \to \infty$) is defined by Csiszár and Körner [CK78a] as

$$R \geq I(X;Y) - I(X;Z) \tag{2.21}$$

Which, from the relation $I(X;Y) = H(X) - H(X|Y)$, $I(X;Z) = H(X) - H(X|Z)$, and $H(\cdot) \geq H_{\min}(\cdot)$ is,

$$R \geq H_{\min}(X|Z) - H(X|Y) \tag{2.22}$$

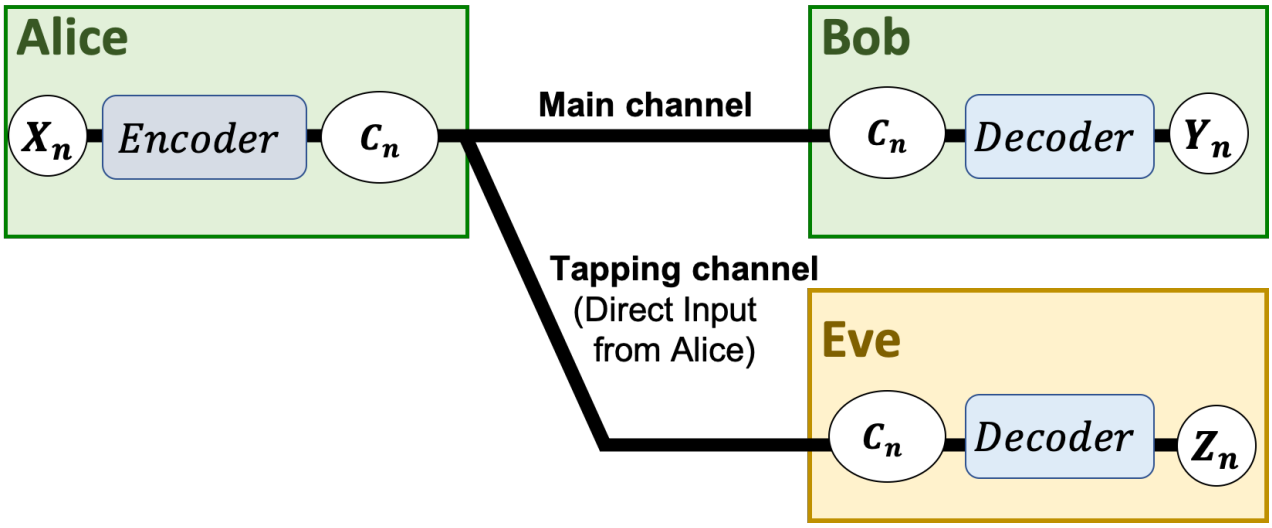


Figure 2.6: A general setting for key establishment protocol between two authorized parties Alice and Bob, and an unauthorized party Eve.

Chapter 3

Quantum Cryptography

The present chapter aims to provide an overview of the most important and most recent advances in quantum cryptography, both theoretically and experimentally. After a brief introduction of the general notions, we will review the main QKD protocols based on discrete- and continuous-variable systems. We will consider standard QKD, device-independent, and measurement-device independent QKD. We will then discuss the ultimate limits of point-to-point private communications and how quantum repeaters and networks may overcome these restrictions. Finally, we will treat topics beyond QKD, including Twin-Field QKD, Flood Light QKD, and Quantum Data Locking.

There a number of reviews and books on QKD (e.g., see Refs.[NCC00, Hol12, BZ07, Hay16, Wat18, WPGP+12, PAB+20b]). Some of the concepts are repeated in this review, but we generally assume basic knowledge of these systems.

3.1 Generic aspects of a QKD protocol

Any QKD protocol, be it based on discrete or continuous variables, can be divided into two-step: quantum communication followed by classical post-processing. During quantum communication, the sender (Alice) encodes a random classical variable X into non-orthogonal quantum states. These states are sent over a quantum channel (optical fiber, free-space link) controlled by the eavesdropper (Eve), trying to steal the encoded information. Leveraging on the fundamentals like uncertainty principle [NCC00] and no-cloning theorem [WZ82], quantum mechanics forbids perfect cloning Eve can only get partial information while disturbing the quantum signals. At the communication channel's output, the receiver (Bob) measures the incoming signals and obtains a random classical variable Y. After several channels, Alice and Bob share raw data described by two correlated variables X and Y.

The raw data generated at the end of the quantum communication step is then post-processed to transform into a pair of the secret key. First, the remote parties use part of the raw data to estimate the parameters of the channel, such as its transmissivity and noise. This stage of parameter estimation is essential to evaluate the amount of post-processing to extract a private shared key from the remaining data. Depending on this information, they perform a stage of error correction, which allows them to detect and eliminate errors, followed by a privacy amplification stage that allows them to reduce Eve's stolen information to a negligible amount. The final result is the secret key.

Sometimes QKD protocols are formulated in entanglement-based representation. This means that Alice' preparation of the input ensemble of states is replaced by an entangled state Ψ_{AB} part

of which is measured by Alice. The measurement on part A affects to prepare a state on part B conditionally. The outcome of the measurement is one-to-one with the classical variable encoded in the prepared states. This representation is beneficial for the study of QKD protocols so that their prepare and measure formulation is replaced by an entanglement-based formulation for assessing the security and deriving the secret key rate.

3.2 Overview of DV-QKD protocol

3.2.1 BB84

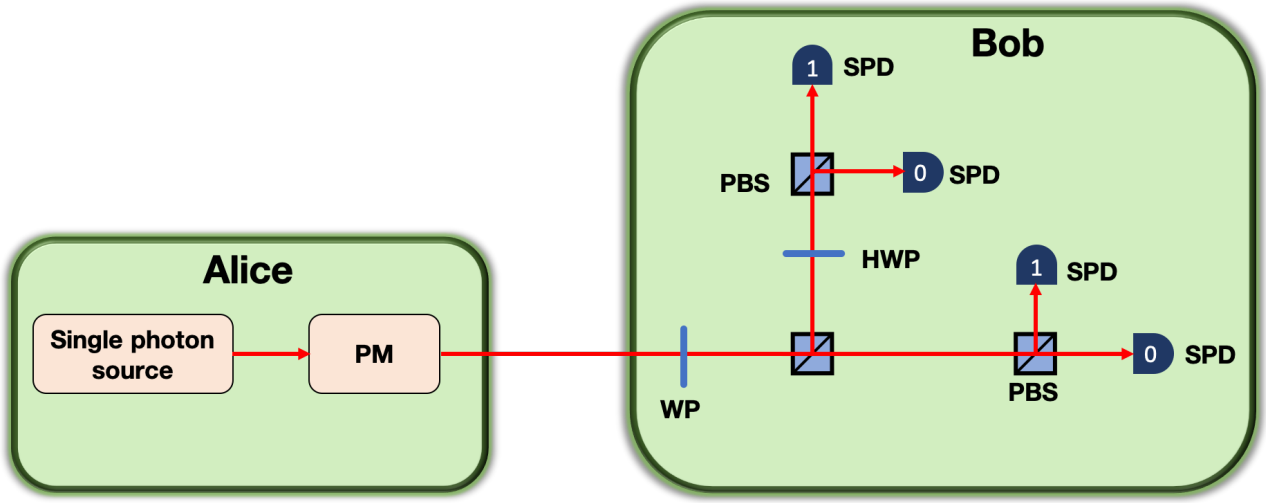


Figure 3.1: Schematic implementation of BB84 using polarization states. Alice's side comprises a photon source (Source) and a polarization modulator (PM), although she could combine the output of four different sources, each with a different polarization. As the photon enters Bob's station, it goes first inside a waveplate (WP), which corrects polarization changes due to the fiber. The beam splitter (BS) passively branches the photon to one of the two possible measurement bases. One of the outputs goes inside a half waveplate (HWP) to rotate the polarization by $45°$. The polarizing beam splitters (PBS) select the photons based on their polarization state. The photon detectors (SPD) are associated with either the value "0" or with the value "1".

In BB84 protocol [BB14] Alice (the transmitter) prepares the qubits, i.e., two-level quantum system, by encoding a classical variable with respect to one of two different orthogonal bases, called the rectilinear ($|0\rangle$, $|1\rangle$: $\mathbb{Z}$ Basis) and the diagonal basis ($|+\rangle$, $|-\rangle$: $\mathbb{X}$ Basis). These two bases are mutually unbiased; that is, a measurement in one of the bases reveals no information on a bit encoded with respect to the other basis. The states prepared by Alice are sent to Bob (the receiver) using the quantum channel, who measures them in one of the two bases $\mathbb{Z}$ or $\mathbb{X}$, selected at random. They repeat this procedure over n quantum channel use and obtain a pair of classical bit strings $X = (X_1, \ldots, X_n)$ at Alice's end, and $Y = (Y_1, \ldots, Y_n)$ at Bob's.

The remaining part of the protocol is purely classical (in particular, Alice and Bob only communicate classically). First, Alice and Bob apply a *sifting* step, where they announce their choices of bases used for the encoding and the measurement, respectively. They discard all bits of their raw key for which the encoding and measurement bases are not compatible. Then Alice and Bob

proceed with a *parameter estimation* step. They compare some (small) randomly chosen set of bits of their raw key in order to get a guess for the *error rate*, i.e., the fraction of positions i in which X_i and Y_i disagree. If the errors detected are above some threshold, this indicates an eavesdropper on the quantum channel, resulting in the abortion of the protocol.

Let X' and Y' be the remaining parts of the raw keys (i.e., the bits of X and Y that have neither been discarded in the sifting step nor used for parameter estimation). These strings are now used for the actual computation of the final key. In an *information reconciliation* step, Alice sends certain error-correcting information on X' to Bob. This, together with Y', allows him to compute a guess for X'. In the final step of the protocol, called *privacy amplification*, Alice and Bob use two-universal hashing to turn the (generally only partially secret) string X' into a shorter but secure key.

The security of the BB84 protocol is based on the fact that an adversary, ignorant of the actual encoding bases used by Alice, cannot gain information about the encoded bits without disturbing the qubits sent over the quantum channel. If the disturbance is too large, Alice and Bob will observe a high error rate and abort the parameter estimation step protocol. On the other hand, if the disturbance is below a certain threshold, then the strings X' and Y' held by Alice and Bob are sufficiently correlated and secret in order to distill a secret key.

In order to prove security, one thus needs to quantify the amount of information that an adversary has on the raw key, given the disturbance measured by Alice and Bob. A general attack strategy an eavesdropper can consider is to attach an ancilla, $|\mathcal{E}\rangle$ (a quantum system possibly higher dimension than a qubit) to Alice's qubit and let them interact in the hope of deriving some information. This interaction can be written as

$$U|a\rangle|\mathcal{E}\rangle = \sqrt{F_a}|a\rangle|\mathcal{E}_{aa}\rangle + \sqrt{D_a}|a^\perp\rangle|\mathcal{E}_{aa^\perp}\rangle \tag{3.1}$$

Where $|a\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle$ and $\langle a|a^\perp\rangle = 0$, with $|\mathcal{E}_{ij}\rangle$ being Eve's possible ancillary states after the interaction. This equation mean that when Alice sends a state $|a\rangle$, Bob has a probability F_a of getting the right result when measuring in the correct basis and D_a otherwise. Unitarity of U ensures

$$\langle\mathcal{E}_{aa}|\mathcal{E}_{aa}\rangle = F_a \tag{3.2}$$
$$\langle\mathcal{E}_{aa^\perp}|\mathcal{E}_{aa^\perp}\rangle = D_a \tag{3.3}$$
$$\langle\mathcal{E}_{aa}|\mathcal{E}_{aa^\perp}\rangle = 0 \tag{3.4}$$

implying the bit error rate

$$e_b = D_a = \frac{1-\cos x}{2-\cos x+\cos y} \tag{3.5}$$

with x and y real numbers. This is the essence of a symmetric attack [86] which can be seen as a contraction of the Bloch sphere by $F_a - D_a$.

Assume that Eve keeps her ancillary system in a quantum memory and waits for Alice and Bob to end all the classical communication related with the reconciliation of the bases (sifting). In this way she can distinguish between her ancillary states given by $|\mathcal{E}_{aa}\rangle$ and $|\mathcal{E}_{a^\perp a^\perp}\rangle$. Then assume that she can also perform a joint measurement on her entire quantum memory, a scenario known as 'collective attack'. In such a case, Eve's amount of information is upper bounded by the Holevo information

$$\chi = S(\rho_E) - \frac{S[\rho_E(a)] + S[\rho_E(a^\perp)]}{2} \tag{3.6}$$

where, $S(\cdot)$ is the von Neumann entropy, and $\rho_E(a)(\rho_E(a^{\perp}))$ is Eve's state for Alice's $|a\rangle(|a^{\perp}\rangle)$. In the presence of the symmetric collective attack, it can be shown that the key rate is then given by,

$$K_{BB84} = 1 - S(\rho_E) = 1 - 2H_2(e_b) \tag{3.7}$$

where the binary Shannon entropy H_2 is computed over bit error rate e_b. As a result, a key can be extracted for an error rate with a value no greater than approximately 11%. This security threshold value of 11% is exactly the same as the one that is found by assuming the most general 'coherent attack' against the protocol, where all the signal states undergo a joint unitary interaction together with Eve's ancillae, and the latter are jointly measured at the end of protocol.

3.2.2 Six state protocol

The BB84 protocol has also been extended to use six states on three bases to enhance the key generation rate, and the tolerance to noise [Bru98]. 6-state BB84 is identical to BB84 except, as its name implies, rather than using two or four states, it uses six states on three bases X, Y, and Z. This creates an obstacle to the eavesdropper who has to guess the right basis from among three possibilities rather than just two of the BB84. This extra choice causes the eavesdropper to produce a higher rate of error, for example, $1/3$ when attacking all qubits with a simple IR strategy, thus becoming more comfortable to detect.

One can extend the analysis of Eve's symmetric collective attack to the 6-state BB84 by considering a third basis, which immediately sets a further constraint on Eve's ancillary state. the new error rate is then

$$e_b = \frac{1 - \cos x}{2 - \cos x} \tag{3.8}$$

with x a real number, as noted in [BP06]. Assuming a symmetric collective attack, a similar calculation to the one for BB84 gives the following secret key rate for the 6-state protocol as

$$K_{6-state} = 1 + \frac{3e_b}{2}\log_2\frac{e_b}{2} + \left(1 - \frac{3e_b}{2}\right)\log_2\left(1 - \frac{3e_b}{2}\right) = 1 - H_2\left(\frac{3}{2}e_b\right) - \frac{3}{2}e_b\log_2(3) \tag{3.9}$$

This rate exactly coincides with the unconditional key rate, proven against coherent attacks, and gives a security threshold value of about 12.6% slightly improving that of the BB84 protocol.

3.2.3 High-dimensional QKD

Discrete variable (DV) QKD schemes encode quantum states in qubits ($d = 2$). However, there has been considerable interest in developing large-alphabet DV QKD schemes that encode photons into qudits: high-dimensional basis states with $d > 2$. This may be intuitively understood from the fact that the presence of an optimal cloning attack leads to larger signal disturbance in higher-dimensional QKD schemes. The BB84 protocol may be extended here by using qudits. The adoption of high-dimensional quantum system has two distinct benefits: (i) such schemes offer the ability to encode multiple $\log_2(d)$ bits of information in each photon, i.e., an increase of the error-free key rate per sifted photons to a value of $K = \log_2(d)$; (ii) an increase in the maximum tolerable error rate, i.e., the error threshold for $K = 0$. For the simple case of d-dimensional BB84 protocol, the secret key rate is given by [BHE+18],

$$K^{(d)}_{\text{BB84}} = \log_2(d) - 2H^{(d)}(e_b) \tag{3.10}$$

where, $H^{(d)}(x) := -x\log_2(x/(d-1)) - (1-x)\log_2(1-x)$ is the d-dimensional Shannon entropy [SS10]. Furthermore, it is also possible to extend the six-state protocol to higher dimensions by employing all $(d+1)$ mutually unbiased bases, assuming that d is a power of a prime, where the secret key rate is given by,

$$K_{6-state}^{(d)} = \log_2(d) - h^{(d)}\left(e_b\frac{d+1}{d}\right) - \frac{d+1}{d}e_b\log_2(d+1) \tag{3.11}$$

3.2.4 Practical imperfection and countermeasure

PNS attack

DV-QKD protocols are ideally defined on qubits (or qudits), single photons carrying one (or $\log d$) bits of information. However, in practice, perfect single-photon sources are generally not available, and there is some probability for a source to emit multiple photons with identical encodings in a given run of the QKD protocol. This can be a security vulnerability to an eavesdropper who employs the photon number splitting (PNS) attack [HIGM95, LÖ0]. The essential idea behind the attack is that Eve can perform a quantum non-demolition measurement to determine the number of photons in a run, and when it is greater than 1, she could steal one of the excess photons while forwarding the others to Bob. In this way, Bob would not detect her presence while she lies in wait for Alice's basis revelation to make sharp measurements of the stolen photons and obtain perfect information of the multi-photon runs.

Countermeasure: Decoy states, SARG04

The need to counter the PNS attack triggered the invention of the decoy-state protocol [Hwa03, Wan05a, Wan05b, LMC05, MQZL05], which allows efficient distillation of secure keys using weak coherent pulse-based QKD systems that once were vulnerable. In decoy-state-based QKD, the average number of photons transmitted is increased during random timeslots, allowing Alice and Bob to detect if Eve is stealing photons when multiple photons are transmitted.

To mitigate a PNS attack, the SARG04 protocol [SARG04] modifies the sifting process. Instead of directly revealing bases, Alice and Bob publicly announce one of the four pairs of non-orthogonal states consisting of $\{[0\rangle, |+\rangle\}, \{|0\rangle, |-\rangle\}$, $\{|1\rangle, |+\rangle\}$, and $\{|1\rangle, |-\rangle\}$. The protocol works as follows: First, Alice chooses one of the four pairs and one of the two states in the pair and transmits it to Bob. Then, Bob performs a measurement with two bases $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$. After that, sifting is performed for unambiguous discrimination between states in an announced pair. For example, assume Alice transmits $|0\rangle$ state in a set $\{|0\rangle, |+\rangle\}$ and Bob measures it with a basis $\{|1\rangle, |-\rangle\}$. If Bob measures $|+\rangle$ state, then it is discarded since it can be from $|0\rangle$ or $|+\rangle$. If Bob measures $|-\rangle$ state, it is stored for post-processing because it can only be from the $|0\rangle$ state. Since two states in a set are non-orthogonal, the PNS attack cannot provide Eve with perfect information on the encoded bit.

3.3 Overview of CV-QKD

The idea of continuous-variable QKD is to exploit coherent quantum communication. The main consequence of this choice is that CV-QKD and DV-QKD involve different measurement stages: homodyne (or heterodyne) for continuous-variable protocols instead of photon counting techniques

discrete-variable protocols. One of CV-QKD's appealing feature is to rely on components (such as PIN photodiodes), that are identical, or very close to standard telecom components and are much more mature from a technological point of view than single-photon detectors.

A seminal result in QKD using continuous variables was the discovery that coherent states are sufficient to distribute secret keys [GG02a, GG01]. Because coherent states are much easier to generate in the lab than any other Gaussian state, this result opened the door to experimental demonstrations and field implementations [HHL+15]. Here, in this section, we propose a general presentation of continuous-variable protocols.

3.3.1 Continuous variable systems

CV quantum systems are described by an infinite-dimensional Hilbert space. Consider a quantum system made of n bosonic modes of the electromagnetic field with tensor-product Hilbert space $\otimes_{k=1}^{n}\mathcal{H}_k$ and associated n pairs of field operators $\hat{a}_k^\dagger$, $\hat{a}_k$, with $k = 1, \cdots, n$. For each mode k we can define the following field quadratures

$$\hat{q}_k := \hat{a}_k + \hat{a}_k^\dagger, \qquad \hat{p}_k := i(\hat{a}_k^\dagger - \hat{a}_k) \tag{3.12}$$

These operators can be arranged in an N-mode vectors $\hat{\mathbf{x}} := (\hat{q}_1, \hat{p}_1, \cdots, \hat{q}_n, \hat{p}_n)^T$. Using the standard bosonic commutation relations, for the field's creation ($\hat{a}_{kl}^\dagger$) and annihilation ($\hat{a}_k$) operators, one can easily verify that the any pairs of entries of vectors $\mathbf{x}$ satisfy the following commutation relation

$$[\hat{x}_l, \hat{x}_m] = 2i\Omega_{lm}, \qquad \Omega_{lm} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tag{3.13}$$

where Ω_{lm} is the symplectic form [WPGP+12]. From Eqs. (3.12)-(3.13) we can see that the vacuum noise is here set to 1.

An n-mode quantum state can be represented either as a density operator $\hat{\rho}$ acting on $\otimes_{k=1}^{n}\mathcal{H}_k$ or as a Wigner function defined over $2n$-dimensional phase space. In particular, a state is Gaussian if its Wigner function is Gaussian, so that it is completely characterized by the first two statistical moments, i.e., the mean value $\bar{\mathbf{x}} := \langle\hat{\mathbf{x}}\rangle = \mathrm{Tr}(\hat{\mathbf{x}}\hat{\rho})$ and covariance matrix (CM) $\mathbf{V}$, whose arbitrary element is defined by

$$V_{ij} := \frac{1}{2}\langle\{\Delta\hat{x}_i, \Delta\hat{x}_j\}\rangle, \tag{3.14}$$

where $\Delta\hat{x}_i := \hat{x}_i - \langle\hat{x}_i\rangle$ and $\{,\}$ is the anti-commutator.

For a single-mode, one can consider different classes of quantum states, the most known are the coherent states. These are states with minimum (vacuum) noise uncertainty, symmetrically distributed in the two quadratures, and characterized by their complex amplitudes in the phase space. They are denoted as $|\alpha\rangle$, where $\alpha = \bar{q} + i\bar{p}$, where $(\bar{q}, \bar{p})$ are the components of the mean value. Another important class is that of squeezed states, where the noise is less than the vacuum in one of the two quadratures (while greater than in the other) [WPGP+12].

3.3.2 CV-QKD protocol

Realization of a generic CV-QKD protocol includes the following steps: Alice encodes a classical variable X in the amplitudes of Gaussian states, which are randomly displaced in the phase space using a zero-mean Gaussian distribution, whose variance is typically large. If coherent states are used, the modulation is symmetric in the phase space. If squeezed states are used instead, then

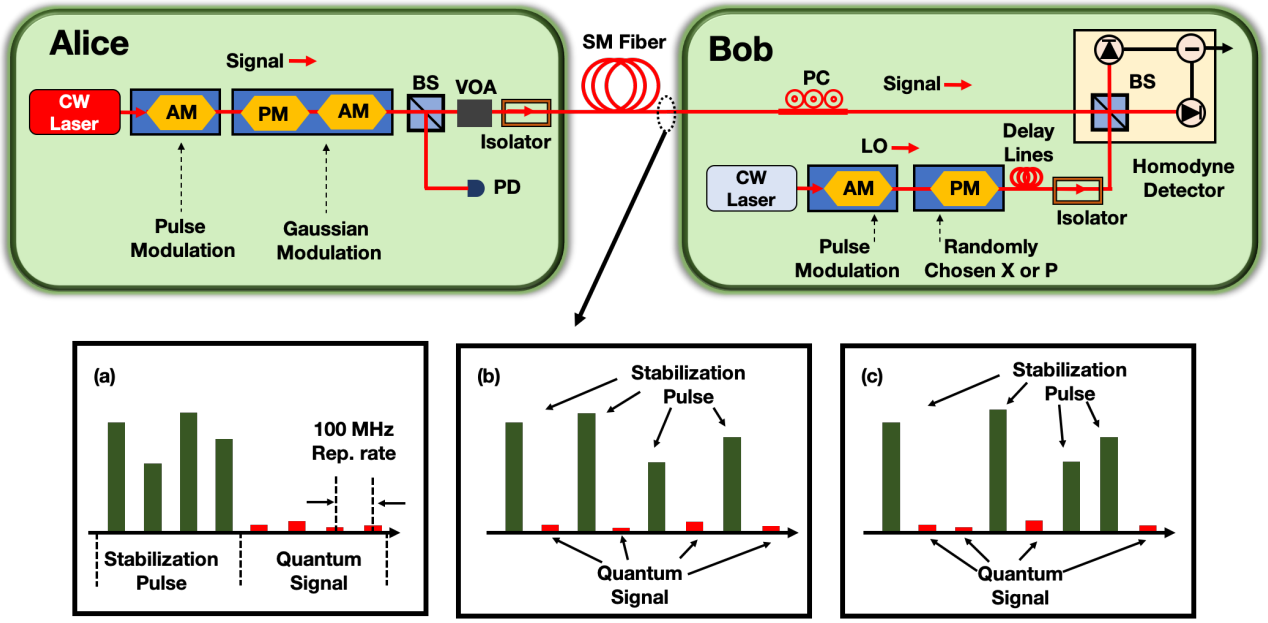


Figure 3.2: Details of experimental setups for CV-QKD based on a Gaussian coherent state alphabet. A CW telecom laser at 1550nm is transformed into 1 nsec pulses with a repetition rate of 100MHz using an amplitude modulator (AM). The Gaussian distributed signal is produced with a pair of modulators (AM and PM), and its brightness is controlled with a variable optical attenuator (VOA). Phase synchronization signals are produced in the modulators that are time-multiplexed with the quantum signal, either regularly as in (a) and (b) or randomly as in (c). The signals are injected into the channel and measured with a locally generated local oscillator at Bob. An AM produces local oscillator pulses while a PM randomly switches their phases by π to allow for a random quadrature measurement. Phase and frequency synchronization between LO and signal is attained through DSP of the data produced by the interference between the LO and the reference pulses. Taken from Ref. [HHL+15].

the displacement is along the squeezing direction, and Alice randomly switches between q- and p-squeezings.

Alice then sends the modulated signal states to Bob through the quantum channel, which is typically a thermal-loss channel with transmissivity T and some thermal noise, quantified by the mean number of thermal photons in the environment $\bar{n}$ or, equivalently, by the excess noise $\epsilon = T^{-1}(1-T)\bar{n}$. Bob performs homodyne or heterodyne detection on the incoming signals at the output of the quantum channel, thus retrieving his classical variable Y. Following this, Alice and Bob perform classical post-processing to extract secret pair of keys.

For CV-QKD, the information reconciliation protocol comprises of two different variations. The first protocol is a *direct-reconciliation* protocol [SRLL02a], in which we allow information reconciliation by forwarding public communication from the sender Alice to the receiver Bob. The second protocol is a *reverse-reconciliation* [GG02b, Fur14] protocol, where we allow information reconciliation by backward public communication from Bob to Alice. It is advantageous to perform a reverse reconciliation in place of a direct reconciliation.

In a Gaussian CV-QKD protocol, where the Gaussian signal states are Gaussian-modulated and the outputs are measured by homodyne or heterodyne detection [SC07], and the optimal attack is a collective Gaussian attack. Here Eve combines each signal state and a vacuum environmental state

via a Gaussian unitary and collects the environment's output in a quantum memory for an optimized and delayed joint quantum measurement.

In a realistic scenario, taking into account imperfect reconciliation with efficiency $\beta \in \{0, 1\}$, the secret key rate against collective attack is given by

$$K_{coll}^{DR} = \beta I(X;Y) - S(X;E) \tag{3.15}$$

$$K_{coll}^{RR} = \beta I(X;Y) - S(Y;E) \tag{3.16}$$

In practice, the first term of the right side hand, $\beta I(X;Y)$ is directly observed in a given implementation of the protocol. Therefore, the real question is to determine the value of $S(Y;E)$ or at least be able to find the upper bound for this quantity to derive a lower bound on the actual secret key rate of a given experiment.

To estimate the lower bound on the key rate, let us consider the prepare and measure version of the GG02 protocol [GG02b], where Alice encodes information in the quadratures X and P of coherent states. The random variables X and P are drawn according to a Gaussian distribution of variance $V_A : X, P \sim \mathcal{N}(0, V_A)$. At the end of the quantum exchange, Alice and Bob perform a parameter estimation, which is done by analyzing m pairs of correlated data $(x_i, y_i)_{1 \leq i \leq m}$ where y_i refers to the quadrature measurement of Bob and x_i refers to the corresponding value of Alice's quadrature. For CV-QKD, it is sufficient to estimate the covariance matrix Γ_{AB} of the state shared by Alice and Bob.

$$\Gamma_{AB} = \begin{pmatrix} V\mathbb{I}_2 & \sqrt{T(V^2-1)}\sigma_z \\ \sqrt{T(V^2-1)}\sigma_z & (1 + T(V-1) + T\mathcal{E})\mathbb{I}_2 \end{pmatrix} \tag{3.17}$$

Where, T is the transmission and $\mathcal{E}$ is the excess noise of the quantum channel. It turns out that only two parameters need to be estimated: (i) the variance on the Bob's side $\langle y^2 \rangle$, (ii) the correlation between Alice and Bob's data $\langle xy \rangle$, as entries in the Γ_{AB} are linked to $\langle x^2 \rangle$, $\langle y^2 \rangle$ and $\langle xy \rangle$ through

$$V = \langle x^2 \rangle + 1, \quad T = \frac{\langle xy \rangle^2}{\langle x^2 \rangle^2}, \quad 1 + T(V-1) + T\mathcal{E} = \langle y^2 \rangle \tag{3.18}$$

Now $S(Y;E) = S(E) - S(E|Y) = S(AB) - S(AB|Y)$, as Eve's system can be considered without loss of generality to be a purification of Alice and Bob's system. The quantity $S(AB)$ and $S(AB|Y)$ can be calculated from the symplectic eigenvalues ν_1, ν_2 of Γ_{AB} and ν_3 of $\Gamma_{AB|Y}$, where $\Gamma_{AB|Y}$ is the covariance matrix of Alice's mode, given Bob's result of the homodyne measurement of say, quadrature x:

$$\Gamma_{AB|Y} = \begin{pmatrix} V - \frac{T(V^2-1)}{1+TV+T\mathcal{E}} & 0 \\ 0 & V \end{pmatrix} \tag{3.19}$$

The symplectic eigenvalues are given by:

$$\nu_1^2 = \frac{1}{2}[\Delta + \sqrt{\Delta^2 - 4D}] \tag{3.20}$$

$$\nu_2^2 = \frac{1}{2}[\Delta - \sqrt{\Delta^2 - 4D}] \tag{3.21}$$

$$\nu_3^2 = V\Big(V - \frac{T(V^2-1)}{1 + T(V-1) + T\mathcal{E}}\Big), \tag{3.22}$$

Where one defines,

$$\Delta = V^2 + (1 + T(V-1) + T\mathcal{E})^2 - 2T(V^2-1) \tag{3.23}$$
$$D = ((1 + T(V-1) + T\mathcal{E})V - T(V^2-1))^2. \tag{3.24}$$

Now, from the expression of the entropy of a Gaussian state as a function of its symplectic eigenvalues, one obtains:

$$S(Y;E) = g\Big(\frac{\nu_1 - 1}{2}\Big) + g\Big(\frac{\nu_2 - 1}{2}\Big) - g\Big(\frac{\nu_3 - 1}{2}\Big) \tag{3.25}$$

where the function g is defined as

$$g(x) = (x+1)\log_2(x+1) - x\log_2 x \tag{3.26}$$

In this finitesize regime the security of CV-QKD was first analyzed against collective attacks [LGG10] by including corrections to the key rate taking into account of the data points used and discarded during parameter estimation and the convergence of the smooth min-entropy towards the von Neumann entropy.

CV-QKD with discrete modulation

In CV-QKD, information is encoded in quantum systems with infinite-dimensional Hilbert spaces. This allows the sender to use bright coherent states and highlyefficient homodyne detections, which naturally boost the communication rate. These features do not come for free. At the error correction stage, one pays a penalty in mapping the continuous output data from the physical Gaussian channel into a binary-input additive white Gaussian-noise channel. This mapping is more accurate by employing discrete modulation [LG09]. The first discrete-modulated CV-QKD protocol was based on a binary encoding of coherent states [SRLL02b] and was designed to overcome the 3 dB limitation of CV-QKD in DR. Later protocols have consider three [BW18] or arbitrary number of phase-encoded coherent states [PLWP18].

The basic idea in Ref. [SRLL02b] is to perform a binary encoding which assigns the bit-value 0 (1) to a coherent state with positive (negative) displacement. Then, the receiver switches the homodyne detection setup, measuring quadrature q or p. After the quantum communication, the parties discard unfavorable data by applying an advantage distillation routine [Mau93b, CM97b], which is a post-selection procedure which extracts a key by using two-way classical communication. The asymptotic security of this protocol was first studied under individual attacks [SRLL02b] and later against collective attacks, with also a proof-of-concept experiment [SAA+07] . In general, the security of CV-QKD with non-Gaussian modulation remains an open question (in finite size regime). In the asymptotic limit, its security has been proven against Gaussian attacks [LG11] and, more recently, general attacks [GDL19].

3.4 Device-Independent QKD (DI-QKD)

Quantum Key distribution protocols are robust against future algorithmic and computational advances, including quantum computers' emergence. This is because its security is information-theoretic, i.e., it can be proven based only on models of the local devices operated by legitimate users and does not require any assumptions on the resources available to an adversary. However,

real-life implementations of QKD rarely conform to the assumptions in idealized models used in security proofs. Any features of the real devices not modeled in the security proof could compromise security, and there are cases where this has happened in actual implementations. Attacks that exploit features not modeled in the security proof are known as *side-channel attacks*. Real systems may still possess side channels, i.e., security vulnerabilities, if their implementation deviates significantly from the security analysis's idealized models.

A way to break out of this loophole that exploits imperfections in the practical realization is to consider device-independent approaches. The security of a device-independent protocol does not depend on the devices' implementation, as no assumptions are made on how devices operate and are used in the protocol. Instead, the security is derived from the input-output behavior, which is tested in the protocol. This has an advantage over standard QKD protocols with trusted devices where a user, in principle, should check the implementation security of their devices regularly to ensure their behavior is still in line with the assumptions of the security proof. This is a technically challenging task and not one that can be expected of an average user. By contrast, in a device-independent protocol, the implementation of the quantum part of Alice and Bob devices can be untrusted which reduces the attack surface to the classical part.

3.4.1 The setup for DI-QKD

The device-independent approach eliminates security flaws due to device imperfections by not making any assumption on devices' implementation. However, many other assumptions are in this scenario, which is also made in the trusted-devices case:

1. Alice and Bob have secure laboratories and control over all channels connecting their laboratory with the outside world. Otherwise, the untrusted devices could broadcast their outputs to the adversary outside the laboratory, or Eve could send a probe into the laboratory to inspect any secret data. Alice and Bob can prevent unwanted information flow between it and any other devices for any devices in their labs.

2. Each party has a trusted way to perform classical information processing.

3. Alice and Bob have access to a perfect random number generator within their laboratories.

4. Alice and Bob are connected by an authenticated classical channel on which an adversary could listen without detection.

5. Alice and Bob are also connected by an insecure quantum channel on which an adversary can intercept and modify signals in any way allowed by quantum mechanics.

3.4.2 Security criterion for DI-QKD

The most essential and necessary ingredient, which forms the basis for DI protocols' security, is a "test for quantumness" based on the violation of a Bell inequality. A Bell inequality can be thought of as a game played by the honest parties using the device they share. Different devices lead to different winning probabilities when playing the game. The game has a unique "feature"- there exists a quantum device that achieves a winning probability ω_q greater than all classical, local devices. Hence, if the honest parties observe that their device wins the game with probability ω_q they conclude that it must be non-local.

DI security relies on the following deep but well-established facts. High winning probability in a Bell game not only implies that the metric system is non-local but, more importantly, that the kind of non-local correlations it exhibits cannot be shared: the higher the winning probability, the less information any eavesdropper can have about the devices' outcomes. The tradeoff between winning probability and secret correlations, can be made quantitative.

3.5 Measurement-Device-Independent QKD (MDI-QKD)

Measurement device Independent approach or QKD is a simple solution to remove all (existing and yet to be discovered) detector side channels, arguably the most critical part of the implementation. In contrast to DI-QKD, in its most straightforward formulation, MDI-QKD requires the additional assumption that Alice and Bob, i.e., the source devices are trusted along with the set of other assumptions, as mentioned in section (3.4.1).

In a simple MDI-QKD setting,

1. Both Alice and Bob prepare phase randomized weak coherent pulses (WCPs) in the four possible BB84 polarization states i.e., single-photon states with either rectilinear $\{|H\rangle, |V\rangle\}$ or diagonal $\{|D\rangle, |A\rangle\}$ polarization.

2. These states are sent to a *untrusted* central relay that is assumed under control of Charlie (or Eve), who performs a Bell state measurement that projects the incoming signals into a Bell state.

3. Once the quantum communication phase is completed, Charlie uses a public channel to announce the events where he has obtained a successful outcome in the relay, including as well his measurement outcome $\alpha = 0, 1, 2, 3$ of the Bell detection.

4. Alice and Bob keep the data that correspond to these instances and discard the rest.

The ideal Bell detection is a measurement with four POVM elements, $\Lambda_\alpha := \sigma_\alpha|\beta\rangle\langle\beta|\sigma_\alpha$, where

$$|\beta\rangle = \frac{1}{\sqrt{2}}(|HH\rangle + |VV\rangle) \tag{3.27}$$

is a maximally entangled state, and σ_α are the Pauli operators (including the identity),

$$\begin{aligned}
\sigma_0 =& |H\rangle\langle H| + |V\rangle\langle V|, \\
\sigma_1 =& |H\rangle\langle V| + |V\rangle\langle H|, \\
\sigma_2 =& i|H\rangle\langle V| - i|V\rangle\langle H|, \\
\sigma_3 =& |H\rangle\langle H| - |V\rangle\langle V|.
\end{aligned} \tag{3.28}$$

Note that, if both Alice and Bob encode information in the rectilinear basis, then they know that their encoded bit values are the same if the outcome is $\alpha = 0$ or $\alpha = 3$, otherwise they know that they are opposite if $\alpha = 1$ or $\alpha = 2$. Therefore, Bob can obtain Alice's bit by flipping (or not flipping) his local bit according to the value of α. Similar is the situation if Alice and Bob use the diagonal basis, as depicted in Table 3.1 . If the parties choose different bases, they simply discard their data.

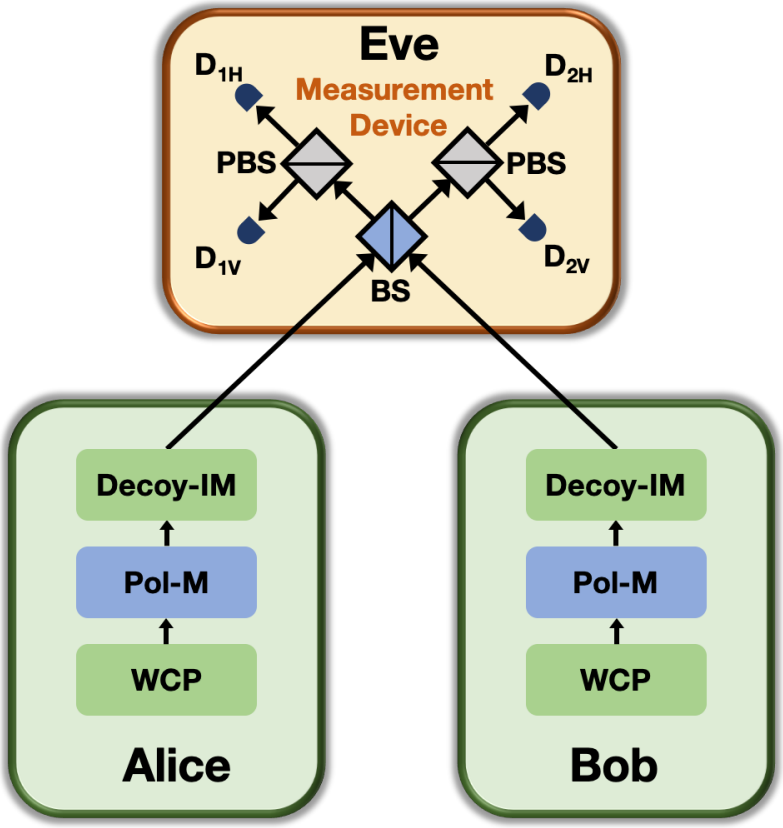


Figure 3.3: Basic setup of a MDI-QKD protocol. Alice and Bob prepare phase randomized weak coherent pulses (WCPs) in a different BB84 polarization state which is selected, independently and at random for each signal, by means of a polarization modulator (Pol-M). Decoy states are generated using an intensity modulator (Decoy-IM). Inside the measurement device, signals from Alice and Bob interfere at a 50:50 beam splitter (BS) that has on each end a polarizing beam splitter (PBS) projecting the input photons into either horizontal (H) or vertical (V) polarization states. Four single-photon detectors are employed to detect the photons and the detection results are publicly announced. A successful Bell state measurement corresponds to the observation of precisely two detectors (associated to orthogonal polarization) being triggered. Alice's and Bob's laboratories are well shielded from the eavesdropper, while the measurement device can be untrusted.

As described in the Figure, Alice and Bob generate weak coherent pulses passing through two distinct polarization modulators, which operate randomly and independently. After this step, the signals are sent through two intensity modulators, which generate the decoy states. The protocol proceeds with the Bell measurement realized by the relay. The signals are mixed in a $50:50$ beam splitter, and the outputs are processed by two polarizing beam splitters (PBS), filtering the input photons into states $|H\rangle$ or $|V\rangle$, and finally detected by two pairs of single-photon detectors. The Bell measurement is successful when two of the four detectors click.

Assuming that the rectilinear basis is used to generate the key, the asymptotic key rate is given by the following expression

$$K_{\text{decoy-MDI}} = P^{11}_{\text{rect}} Y^{11}_{\text{rect}} - P^{11}_{\text{rect}} Y^{11}_{\text{rect}} H_2\left(e^{11}_{\text{diag}}\right) - G_{\text{rect}}\delta\left(Q_{\text{rect}}\right) \tag{3.29}$$

where, $P^{11}_{\text{rect}} = \mu_A \mu_B \exp[-(\mu_A + \mu_B)]$ is the joint probability that both emitters generate single-photon pulses, with μ_A and μ_B describing the intensities (or the mean photon number) of the

	$\{\|H\rangle, \|V\rangle\}$	$\{\|D\rangle, \|A\rangle\}$
$\alpha = 0$	–	–
$\alpha = 1$	bit flip	bit flip
$\alpha = 2$	bit flip	bit flip
$\alpha = 3$	–	bit flip

Table 3.1: The table shows the rules for bit-flipping according to the result $\alpha = 0, 1, 2, 3$ of Bell detection and the sifted basis choice.

photon sources of Alice and Bob. Y_{rect}^{11} gives the gain, while e_{diag}^{11} is the QBER when Alice and Bob correctly send single-photon pulses. The function $H_2(\cdot)$ is the binary Shannon entropy. The gain G_{rect} and the QBER Q_{rect} account for the case where the parties send more than one photon. $\delta(x) = f(x)H_2(x)$ gives the leak of the information from imperfect error correction, with $f \geq 1$ being the efficiency of the classical error correction.

3.6 Limitation of point-to-point QKD

One of the crucial problems in QKD is to achieve long distances at reasonably-high rates. As evident from the Figure.(3.4), which shows a plot for secret-key rate (bits per channel use) versus Alice to Bob distance (km). Theoretical bounds for different QKD protocols are represented in lines, while the experimental result for different QKD schemes is shown as symbols.

Considering the maximum rates that are potentially achievable by current protocols, assuming infinitely long keys and ideal conditions, such as unit detector efficiency, zero dark count rates, zero intrinsic error, unit error correction efficiency, zero excess noise:

- *Secret key capacity:* The blue solid line represent the secret-key capacity of PLOB bound [PLOB17a], which sets the ultimate achievable rate for repeaterless QKD at $K_{\mathsf{SKC}} - \log_2(1-\eta)$, ($\eta = 10^{-\alpha \times \mathsf{distance}/10}$, $\alpha = 0.2$dB/Km), bits per channel use.

- *Single photon QKD:* An ideal implementation of BB84 protocol (based on perfect single-photon sources, ideal detectors and perfect error correction) shows a linear decay of the secret key rate in terms of the loss η in the channel, i.e., $K_{\mathsf{spQKD}} = \eta/2$.

- *Decoy state QKD:* For ideal implementation decoy-state QKD protocol, the secret key rate in terms of loss in the channel is $K_{\mathsf{dsQKD}} = \eta/e$, with e the Euler's number, as shown by green dotted dashed line in Figure 3.4.

- *CV-QKD* At long distances (i.e., small transmissivity η), an ideal implementation of the CV QKD protocols has rate $K_{\mathsf{CVQKD}} \simeq \eta/(2\ln 2) \simeq 0.72\eta$. This rate is r shown by red dashed line in the Figure 3.4.

- Symbol codes for different experimental results as shown in Figure 3.4: red triangles for CV-QKD experiments, brown square for DV-QKD experiments, and orange circle for MDI-QKD experiments.

Extending the communication range of QKD systems is a major objective because of the future network applications. However, the generation rate of the secret key by direct transmission is

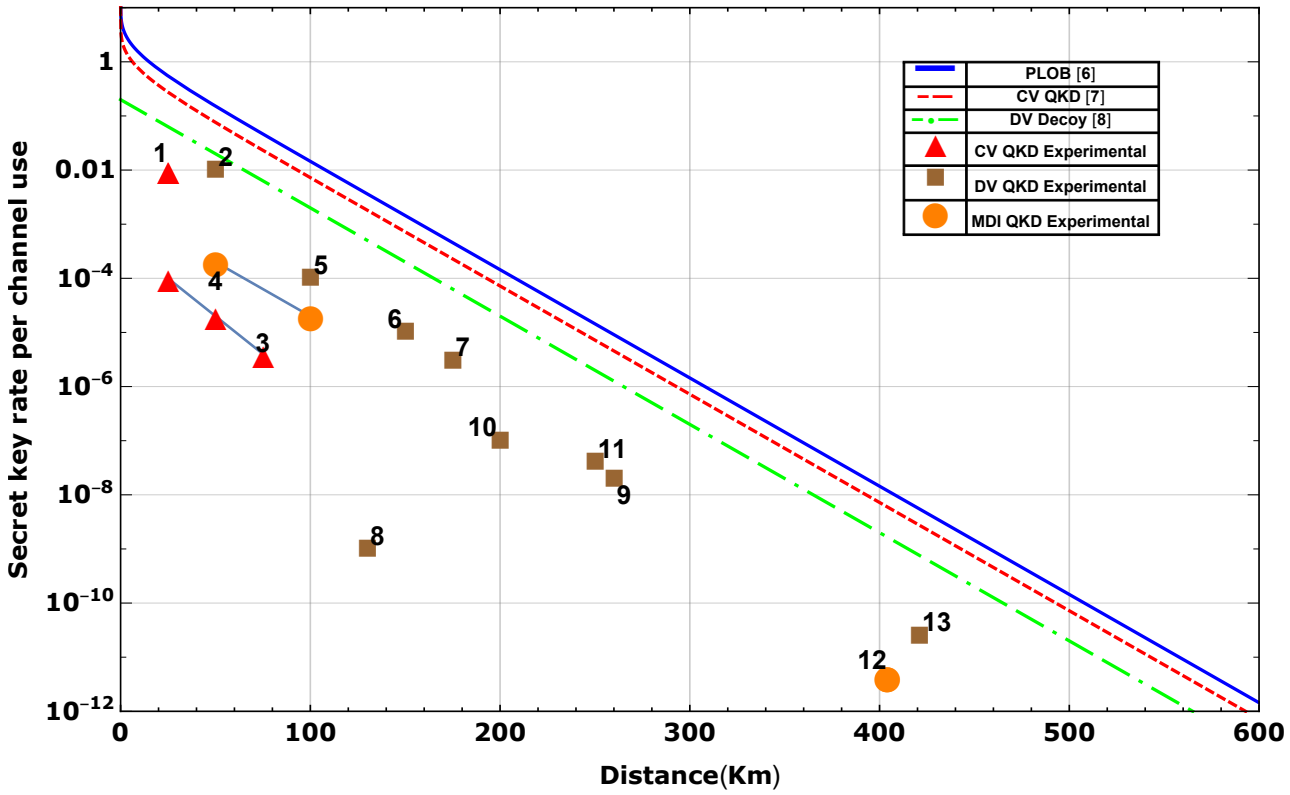


Figure 3.4: Plot showing secret-key rate (bits per channel use) versus Alice–Bob's distance (km). Theoretical bounds (lines) and experimental results (symbols) are shown for different fiber-based quantum schemes. The secret-key capacity of PLOB [PLOB17a] bound: blue line, the ideal implementations of CV protocols: red dashed line, DV-QKD protocol BB84 with single-photon sources: green dotted dashed line. All the experiments represented are numbered in chronological order. The correspondence between numbers and references (following in square brackets) is: 1→ [HLW+15], 2→ [CFL+14], 3→ [JKJL+13], 4→ [CLF+16], 5→ [YDD+09], 6→ [SHF+14], 7 → [NTH+11],8→ [LCW+10],9→ [SWV+09], 10→ [TNZ+07], 11→ [FLD+17], 12→ [YCY+16], 13→ [BBR+18].

fundamentally limited by the distance, as evident from Figure.3.4. Example: For $P_{dark} = 10^{-5}$, $\alpha = 0.2$db/Km, $\eta \approx 0.1$, the maximum distance for repeaters-less QKD is ≤ 250Km and for this limit most of the existing experimental realization of QKD protocol can reach up to 200 Km.

To overcome the fundamental rate-loss scaling of QKD, one may design a multi-hop network that exploits the assistance of quantum repeaters [BDCZ98]. A quantum repeater or quantum relay is any middle node between Alice and Bob which helps their quantum communication by breaking down their original quantum channel into sub-channels. It does not matter what technology the node is employing, e.g., it may or may not have quantum memories. A quantum repeater scheme is said to be "effective" if it can be used to overcome QKD rate-loss performance for a direct transmission, as some distance (and even better a long distance).

The advantage of introducing a quantum repeater can be explained with a simple example. Suppose that an optical fiber connects Alice and Bob with transmissivity η, such that the two-way capacity $\mathcal{C}(\eta)$ is zero. Split the fiber into two identical portions and introduce a middle relay. Since each segment is a lossy channel with transmissivity $\sqrt{\eta}$, both Alice-relay and relay-Bob may be reach the capacity $\mathcal{C}(\sqrt{\eta}) > \mathcal{C}(\eta)$. Combining the outputs, e.g., composing keys or swapping entanglement, $\mathcal{C}(\sqrt{\eta}) > 0$ becomes an achievable rate for the entire repeater-assisted communication

between Alice and Bob.

3.7 Twin-Field QKD

In the MDI-QKD protocol, the idea is to use a middle relay that can be untrusted, i.e., run by Eve. This is the first step towards the end-to-end network principle, which assumes a scenario with unreliable middle nodes. On the other hand, despite MDI-QKD employing a relay, it cannot beat the PLOB bound for point-to-point QKD [PLOB17a]. This limitation has been recently lifted by the introduction of a more efficient protocol called "twin-field" (TF) QKD [LYDS18].

In the TF-QKD protocol, Alice and Bob send two phase-randomized optical fields (faint pulses) to the middle relay (Charlie/Eve) to produce a single-photon interference to be detected by a single-photon detector, whose outcomes are publicly declared. The term twin derives from the fact that the optical fields' electromagnetic phases should be sufficiently close to interfering. More precisely, Alice and Bob send to the relay pulses whose intensity μ_i (for $i = A$ or B) is randomly selected between three possible values. Then, they respectively choose phase ϕ_A and ϕ_B as $\psi_i = (\alpha_i + \beta_i + \delta_i) \oplus 2\pi$, where $\alpha_i \in \{0, \pi\}$ encodes a bit, $\beta_i \in \{0, \pi/2\}$ determines the basis, and the final term δ_i is randomly selected from M slices of the interval $[0, 2\pi)$, so that it takes one of the value $2\pi k/M$ for $k = \{0, 1, \ldots, M-1\}$.

To ensure only phases close enough are selected, after disclosing on an authenticated channel, Alice and Bob only accept the same choices of the slice, i.e., the instances for $\delta_A = \delta_B$. These pulses interfere at the relay constructively (or destructively). Then, Alice announces the basis she used β_A and the intensity μ_A for each instance. The raw key is extracted from the basis $\beta_A = \beta_B = 0$ and for one of the intensities. A bit α_a can be shared between Alice and Bob by considering the absolute difference between α_A and α_B to be equal to 0 or π (depending on the relay's announcement). The rest of the results can be used for other purposes, including estimating error rates and decoy-state parameters.

Note that the twin pulses are in principle set by requiring δ_A to be as close as possible to δ_B the nonzero difference between them introduces an intrinsic QBER. The two become identical provided that M is infinitely large. Realistically, a finite but large value of M can be used though, which decreases the probability of matching two-phase slices. An estimation made in [LYDS18] gives the optimal value of $M = 16$ with QBER of $\approx 1.28\%$.

In [LYDS18], the authors considered a restricted scenario where the 'global phase' does not leak any useful information to Eve, giving a key rate

$$K_{\mathsf{TF}}(\mu, L) = \frac{d}{M} K(\mu, L) \tag{3.30}$$

$K(\cdot)$ is the secret key rate of an efficient BB84 protocol with tagging argument [HL06], and μ, L is the intensity and the distance, respectively. Later [TLWL18], considered a collective attack where Eve uses an identical beam splitter set along each path connecting Alice and Bob to the relay. While this attack considerably increases Eve's gain, the key rate scaling $O(\sqrt{\eta})$ remains unchanged. Using the TF-QKD protocol over a communication line with total Alice-Bob's transmissivity η, not only beats PLOB bound but also the rate performance is also not so far from the single-repeater bound of $-\log_2(1 - \sqrt{\eta})$.

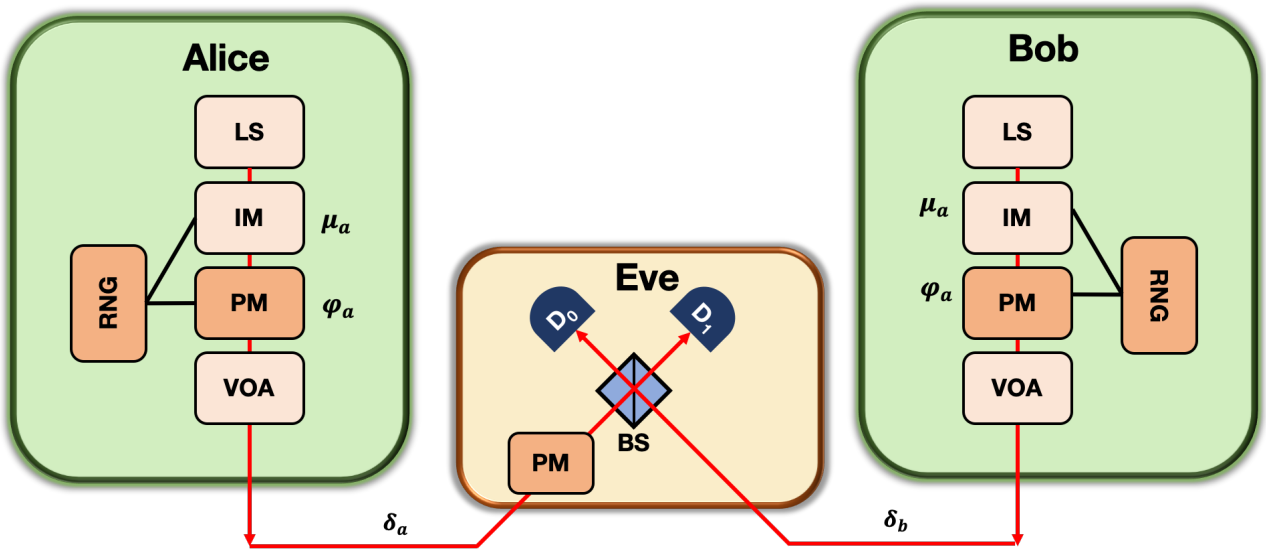


Figure 3.5: Setup to implement TF-QKD. The light sources (LS) generate pulses whose intensities $\mu_{a,b}$ are randomly varied by the intensity modulators (IM) to implement the decoy-state technique. Phase modulators (PM) are combined with random number generators (RNG) to encode each light pulse with phases $\varphi_{a,b}$, which include the random phases $\rho_{a,b}$. The variable optical attenuators (VOA) set the average output intensity of the pulses to bright (classical regime) or dim (quantum regime).

3.8 Floodlight QKD

Floodlight (FL)- QKD represents a two-way CV-QKD protocol that can provide orders-of-magnitude higher SKRs than conventional QKD protocols. The idea behind FL-QKD is to employ multimode encoding. In other words, each message is carried by many optical modes so that the SKR per encoding is substantially increased, even though the SKR per optical mode remains restricted by the PLOB bound. A 55 Mbit/s experimental SKR over a 10-dB-loss channel has been reported [ZZD+16]. More recently, a 1.3 Gbits/s SKR in the presence of a 10-dB attenuation has been demonstrated [ZZWS17].

In FL-QKD, Alice employs broadband amplified spontaneous emission (ASE) source to generate correlated reference and signal light beams. The weak-signal light beam is sent to Bob for phase modulation followed by the optical amplification, while the strong ASE portion of the beam is retained at the Alice side as the local oscillator (LO) reference beam. Bob performs phase modulation on the weak-signal light beam, followed by an amplification using an EDFA. The EDFA compensates for the channel loss and adds bright noise to mask his phase-modulated signal into noise, and such prevents Eve's passive eavesdropping, given that Eve does not have the right reference signal. Additionally, Alice does not need a shot-noise limited homodyne detector but a commercial homodyne detector instead to detect Bob's sequence. In addition to Broadband ASE classical signal, Alice employs a spontaneous parametric down-conversion (SPDC) photon-pair source to generate the time-correlated signal and idler photon, with idler photon being detected by the SPD, and the signal photon being sent towards the Bob with the weak classical ASE signal. Alice ensures that her signal photon has the same polarization as the weak classical ASE signal. After combining the SPDC's signal photons with the weak ASE-noise signal, Alice taps the combined signal portion and applies the second SPD. These two SPDs comprise Alice's channel monitoring circuit. Bob taps the portion of the received signal and passes it to the SPD. Alice and Bob then perform the coincidence measurement

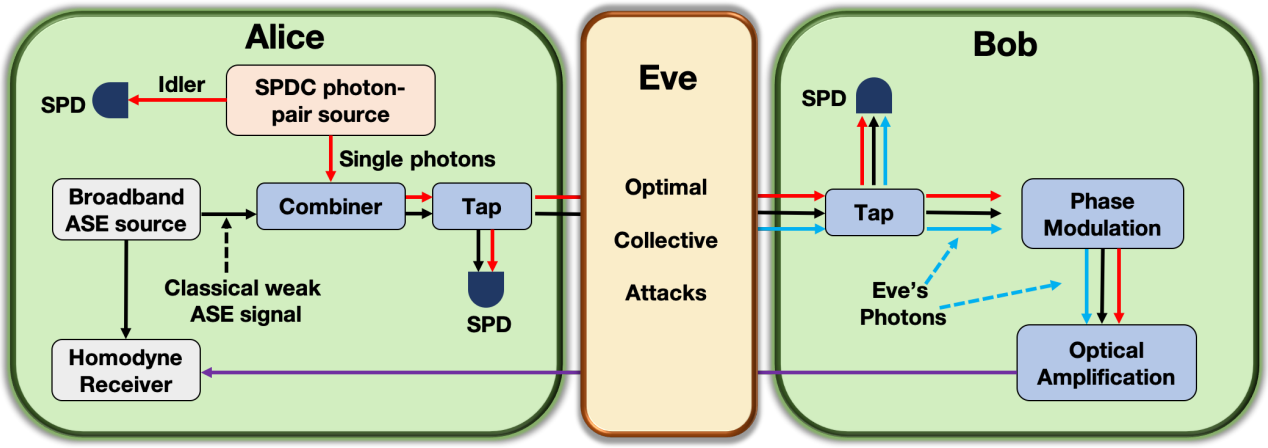


Figure 3.6: Schematic of FL-QKD under Eve's optimum collective attack. Photons generated by Alice's broadband source are marked in black color line; photons generated by Alice's photon-pair source are marked by red color line; photons emitted by Eve's entanglement source are marked as a blue color line, and the thick purple line marks photons emitted by Bob's amplifier.

to estimate the extent of Eve's activity. The authors claim that this protocol is secure against passive attacks, in which Eve uses the lost light. However, it is sensitive to the active attacks when Eve injects her light into Bob's terminal and decodes Bob's beam stream using her owns stored reference. To overcome this problem, the authors claim that Eve's photons are uncorrelated with the idler photons and contribute to the coincidence measurement but introduce the noise photons. This increase in noise photons can be used to quantify the level of Eve's intrusion as follows:

$$f_E = 1 - \frac{C_{IB} - \tilde{C}_{IB}}{C_{IA} - \tilde{C}_{IA}} \frac{S_A}{S_B}, \tag{3.31}$$

where C_{IB} (C_{IA}) denotes time-aligned coincidence rate of Bob's (ALice's) tap, while $\tilde{C}_{IB}$ ($\tilde{C}_{IA}$) denoted the corresponding time-shifted coincidence rate. We use S_A (S_B) to denote the singles rate of Bob's (Alice's) tap. The SKR of the FL-QKD scheme can be lower bounded by

$$K_{\text{FL-QKD}} \geq \left[\beta I_{AB}(P_e) - \chi_{BE}^{(UB)}(f_E)\right] R, \tag{3.32}$$

where β is the reconciliation efficiency, I_{AB} is Alice-Bob mutual information determined by

$$I_{AB}(P_e) = 1 + P_e \log_2 P_e + (1 - P_e) \log_2 (1 - P_e), \tag{3.33}$$

where P_e being Alice's bit error probability of phase-modulated channel. We use R to denote the signal rate and $\chi_{BE}^{(UB)}(f_E)$ to denote the upper bound of Bob-Eve Holevo's information.

3.9 Everlasting security

For many cryptographic tasks (be it classical or quantum) information-theoretic secure protocols simply do not exist (in particular if we cannot assume an majority of honest participants). A compromise is the concept of everlasting security. In a nutshell, a protocol is everlastingly secure if it cannot be broken by an adversary that becomes computationally unlimited after the protocol

execution. This guarantees that all assumptions need only to hold during the protocol execution, sensitive data is not threatened by possible future attacks on today's schemes. We only need to reliably judge the current state of the art, not future technologies

Definition 3.9.1 (Everlasting secure key establishment protocol) *Any key establishment protocol is everlasting secure if it is secure against an adversary who:*

1. *throughout the execution of the protocol is a computationally limited algorithm.*
2. *after the protocol is over, may run any (unbounded in space or time) algorithm.*

Everlasting [Unr13] or *long-term* [SML10] security implies that information-theoretic security is guaranteed *except* during the short period of time during which we assume a computational (or memory) assumption holds. This also implies that assumptions on an adversary's computational power only need to hold during the protocol execution. For example, the assumption of an initial short shared secret (for authenticating the classical channel) in the implementation of QKD can be replaced with a computational assumption [BS15] or an assumption about the quantum storage capabilities of the eavesdropper [HN06]. Sensitive data is not threatened by possible future attacks on today's schemes. Moreover, we only need to reliably judge the current state of the art, not future technologies.

3.9.1 Rationale for everlasting security

Development of quantum cryptography, in particular quantum key distribution has been driven by the desire to achieve unconditional security. However, the usefulness of QKD has been challenged by [Ber09]. To run a QKD protocol, an authenticated channel is needed. But how to implement such a channel? If we use a public key infrastructure for signing messages, we lose unconditional security and thus the main advantage of QKD. If we use shared key authentication, a key needs to be exchanged beforehand. (And, if we exchange an authentication key in a personal meeting, why not just exchange enough key material for one-time pad encryption – storage is cheap.)

A simple change of focus resolves the problems described in the previous paragraph. Instead of seeing the goal of quantum cryptography in achieving unconditional security, we can see it as achieving everlasting security. For example, if we run a QKD protocol and authenticate all messages using signatures and a public key infrastructure, then we do not get an unconditionally secure protocol, but we do get everlasting security: only the signatures are vulnerable to unlimited adversaries, but breaking the security of the signatures after the protocol execution does not help the adversary to recover the key.

Chapter 4

QKD Against Bounded Adversary

QKD commonly offers security against an unbounded adversary, i.e., the adversary can have access to unlimited technology. For example, the eavesdropper (Eve) may have a universal quantum computer with unlimited computational power, as well as a perfect quantum memory of unbounded capacity and ideal detectors. Such a high level of security puts QKD at the forefront on theoretical ground of what is achievable in theory, in terms of security. While these strong assumptions put QKD on a solid theoretical ground, they may be considered unrealistic given the present stage of development of quantum technologies. Such strong assumptions create a disproportion between the technology that will be deployed in a foreseeable future and what is assumed that is already available to Eve. Thus, assessing the usefulness of QKD to serve real-world use cases *in practice* remains a complex and disputed question.

One way to overcome this gap is to consider a different security scenario where a potential eavesdropper has some technological limitations. We review a few such examples of security models, where certain assumptions are made on Eve's technological capabilities. First, we review the *Bounded Quantum Storage Model* (BQSM), where Eve is assumed to be able to store only a limited number of qubits. Moreover, this number is assumed to grow sub-linearly with the number of bits exchanged between Alice and Bob. Second, we consider the *Noisy Storage Model*, where the adversary's quantum storage is bounded and noisy, respectively. The assumption of bounded quantum storage deals with the noiseless case (but assumes a small amount of storage), whereas the noisy-storage model deals with the case of noise (but possibly a large amount of storage). Finally we study the assumption that Eve can store unlimited qubits in quantum memory, however, only for a finite time, and its application to *Quantum Data Locking*.

Before we proceed to review the different scenarios, we briefly review the entropic uncertainty relations, which will play a significant role in proving the security against Eve with constrained quantum memory.

4.1 Entropic uncertainty relations

Consider a collection of k-measurements $\Pi = \{\Pi_j\}_{j=1,\dots,k}$. On a given state ρ, the $j-$th measurement produces a random variable $\Pi_j(\rho)$ with output x_j and associated probability $p_{\Pi_j(\rho)}(x_j)$. An entropic uncertainty relation is expressed by an inequality of the form

$$\inf_{\rho} \frac{1}{k} \sum_{j=1}^{k} H[\Pi_j(\rho)] \geq c_{\Pi} \tag{4.1}$$

where $H[\Pi_j(\rho)] = -\sum_{x_j} p_{\Pi_j(\rho)}(x_j) \log_2 p_{\Pi_j(\rho)}(x_j)$ is the Shannon entropy of $\Pi_j(\rho)$ and $c_{\mathcal{M}}$ is a constant that only depends on the set of measurements $\mathcal{M}$. By convexity, it is sufficient to restrict on pure states.

For example, consider the case of a d-dimensional Hilbert space and a pair of projective measurements $\mathcal{A}$ and $\mathcal{B}$. Each measurement is defined by a corresponding collection of d-orthogonormal vectors $\mathcal{A} \equiv \{|a_1\rangle, \ldots, |a_d\rangle\}$ and $\mathcal{B} \equiv \{|b_1\rangle, \ldots, |b_d\rangle\}$. Then Maassen-Uffink entropic uncertainty relation [MU88] states that

$$\inf_{\rho} \frac{H[\mathcal{A}(\rho)] + H[\mathcal{B}(\rho)]}{2} \geq c_{\mathcal{A},\mathcal{B}} \tag{4.2}$$

where $c_{\mathcal{A},\mathcal{B}} = \log_2 \max_{k,h} |\langle a_k|b_h\rangle|$ and

$$H[\mathcal{A}(\rho)] = -\sum_{k=1}^{d} \langle a_k|\rho|a_k\rangle \log_2 \langle a_k|\rho|a_k\rangle, \tag{4.3}$$

$$H[\mathcal{B}(\rho)] = -\sum_{h=1}^{d} \langle b_h|\rho|b_h\rangle \log_2 \langle b_k|\rho|b_k\rangle. \tag{4.4}$$

In particular, if the two observables are mutually unbiased, then $\max_{k,h} |\langle a_k|b_h\rangle| = 1/\sqrt{d}$ and we obtain

$$\inf_{\rho} \frac{H[\mathcal{A}(\rho)] + H[\mathcal{B}(\rho)]}{2} \geq \frac{1}{2} \log_2 d. \tag{4.5}$$

Given a collection of k observables, one can always find a state ρ such that $H\left[\mathcal{M}_j(\rho)\right] = 0$ for a given j. Therefore the constant $c_{\mathcal{M}}$ in Equation (4.1) is at least larger than $\left(1 - \frac{1}{k}\right) \log_2 d$. An entropic uncertainty relation that saturates this bound is said to be maximally strong. An almost maximally strong entropic uncertainty relation is obtained for a maximal choice of $k = d+1$ mutually unbiased observables, in which case the constant $c_{\mathcal{M}}$ in Equation (4.1) equals $\log_2 \frac{d+1}{2}$ [Sá93].

4.2 QKD in the bounded quantum storage model

4.2.1 Bounded Storage Model

In information, theoretic cryptography physical assumptions appear, which do not rely on any hardness assumptions but merely assume a limit on some other resource. In classical cryptography, the bounded-storage model introduced in [Mau93a] assumes that the adversary can only store a certain number of classical bits. Protocols are known that do (in principle) allow the secure implementation of any cryptographic task as long as the adversary's storage is small. However, It was later discovered that any classical protocol which requires the honest parties to store n bits in order to execute it successfully could be broken by an adversary that can store more than about $\mathcal{O}(n^2)$bits.

This gap changes dramatically when using quantum communication. Likewise, one now assumes that the adversary's quantum storage is limited to a certain number of qubits. There is no restriction on how many classical bits the adversary can store. This is known as the bounded-quantum-storage model. [FGS+18a] (see also Ref. [DFSS05]). The advantages over the classical bounded-storage model are two-fold: First, given current day technology, it is tough to store quantum states. Secondly, the honest player does not require any quantum storage, making the protocol implementable using present-day technology.

4.2.2 Key distribution in bounded quantum storage model

We consider a one-way protocol in which the sender Alice encodes a variable X into a d-dimensional Hilbert space, with $|X| = d$, i.e., $\log d$ bits on a d-dimensional Hilbert space. Let $\mathcal{S}$ be a set of orthonormal bases of a d -dimensional Hilbert space $\mathcal{H}_d$. For each basis $\vartheta \in \mathcal{S}$, we assume that the d basis vectors are parametrized by the elements of the fixed set $\mathcal{X}$ of size $|\mathcal{X}| = d$. We then consider QKD protocols consisting of the steps described as

- **One-Way QKD:** Let $N \in \mathbb{N}$ be arbitrary.

  1. *Preparation*: For $i = 1 \ldots N$, Alice chooses at random a basis $\vartheta_i \in \mathcal{S}$ and a random element $X_i \in \mathcal{X}$. She encodes X_i into the state of a quantum system according to the basis ϑ_i and sends this system to Bob. Bob measures each of the states he receives according to a randomly chosen basis ϑ'_i and stores the outcome $Y_i \in \mathcal{X}$ of this measurement.
  2. *Sifting:* Alice and Bob publicly announce their choices of bases and keep their data at position i only if $\vartheta_i = \vartheta'_i$. In the following, we denote by X and Y the concatenation of the remaining data X_i and Y_i, respectively. X and Y are sometimes called the sifted raw key.
  3. *Error correction:* Alice computes some error correction information C depending on X and sends C to Bob. Bob computes a guess $\hat{X}$ for Alice's string X, using C and Y.
  4. *Privacy amplification:* Alice chooses at random a function f from a two-universal family of hash functions and announces f to Bob. Alice and Bob then compute the final key by applying f to their strings X and $\hat{X}$, respectively.

Note that the quantum channel is only used in the preparation step. Afterward, the communication between Alice and Bob is only classical (over an authentic channel).

The protocol is specified by collecting k different orthogonal bases where Alice randomly selects one of the bases and then encodes the classical random variable X by using the d mutually orthogonal vectors in the chosen basis. Bob independently selects one of the k bases at random and applies the corresponding projective measurement on the receiver side. The protocol is analogous to a d -dimensional version of BB84 with k different bases. After the quantum part of the protocol, in which n states are prepared, transmitted, and measured, the users proceed with the sifting phase, in which they select only the signal transmissions for which they have made the same choice of bases. The protocol then concludes with error reconciliation and privacy amplification.

The difference with standard QKD is that in the BQSM, the eavesdropper Eve is assumed to be only capable of storing a finite amount of quantum information. More specifically, it is assumed that Eve has kept no more than q qubits in her quantum memory after n quantum signal transmissions and before sifting. Therefore, all remaining quantum states intercepted by Eve have already been measured before the sifting phase occurs.

A fundamental estimate of the number of secret bits (excluding sifting) that can be extracted from such a protocol is given by (for direct reconciliation):

$$\ell^{\epsilon} \simeq H^{\epsilon}_{\mathsf{min}}(X^n|ZE) - H_{\mathsf{max}}(C) \tag{4.6}$$

where ϵ is a security parameter, $H^{\epsilon}_{\min}(X^n|ZE)$ is the smooth min-entropy [74,438] conditioned on Eve's side information for n signal transmissions, and $H_{\max}(C)$ is the number of bits publicly exchanged for error reconciliation. Under the assumptions of the BQSM, here Eve's side information

comprises a quantum part E and a classical part Z. Furthermore, since Eve's quantum memory has capacity below q qubits, we have

$$\ell^{\epsilon} \gtrsim H_{\min}^{\epsilon}\left(X^n|Z\right) - q - H_{\max}(C) \tag{4.7}$$

It remains to bound the (classical) conditional smooth min-entropy $H_{\min}^{\epsilon}\left(X^n|Z\right)$. It has been shown in the reference [FGS+18a] that if the set of k bases employed in the protocol satisfies an entropic uncertainty relation as in Equation (4.1) , then for any $\lambda \in (0, 1/2)$

$$H_{\min}^{\epsilon}\left(X^n|Z\right) \geq \left(c_{\Pi} - 2\lambda\right) n, \tag{4.8}$$

with

$$\epsilon = \exp\left[-\frac{\lambda^2 n}{32\left(\log_2(kd/\lambda)\right)^2}\right]. \tag{4.9}$$

For example, using two mutually unbiased bases we can apply the Maassen-Uffink entropic uncertainty relation in Equation (4.5) and obtain for sufficiently small λ

$$H_{\min}^{\epsilon}(X^n|Z) \gtrsim \frac{n}{2}\log_2 d \tag{4.10}$$

In general, the assumptions of BQSM allow us to increase the resilience to noise of a QKD protocol, but the rate is not expected to improve dramatically compared to an unbounded quantum-capable eavesdropper. We conclude by noting that the number of secret bits in Eq. (4.6) must be multiplied by a factor $1/k$ to account for the probability that Alice and Bob chose the same basis.

4.3 Noisy storage model

The noisy storage model [WST08a, STW09, Sch10] can best be understood by thinking about what a dishonest attacker - the adversary - can or cannot do. The adversary is computationally all-powerful and may have a quantum computer that operates flawlessly and instantaneously. The adversary can also have an arbitrary quantum storage device before and after the protocol. The only restriction assumed is that the adversary cannot store qubits perfectly as they undergo decoherence.

We will now have a closer look at the noisy-storage model. A noisy quantum memory as is defined as a device whose input states are in some Hilbert space $\mathcal{H}_{in}$. A state ρ stored in the device decoheres over time. That is, the content of the memory after some time t is a state $\mathcal{F}_t(\rho)$, where $\mathcal{F}_t : \mathcal{B}\left(\mathcal{H}_{in}\right) \to \mathcal{B}\left(\mathcal{H}_{\text{out}}\right)$ is a completely positive trace-preserving map corresponding to the noise in the memory. Since the amount of noise may of course depend on the storage time, the behaviour of the storage is completely described by the family of maps $\{\mathcal{F}_t\}_{t>0}$. We will make the minimal assumption that the noise is Markovian, that is, the family $\{\mathcal{F}_t\}_{t>0}$ is a continuous one-parameter semigroup

$$\mathcal{F}_0 = \mathbb{I} \quad \text{and} \quad \mathcal{F}_{t_1+t_2} = \mathcal{F}_{t_1} \circ \mathcal{F}_{t_2} \tag{4.11}$$

This tells us that the noise in storage only increases with time, and is essential to ensure that the adversary cannot gain any information by delaying the readout. This is the only restriction imposed on the adversary who may otherwise be all-powerful. In particular, we allow that all his actions are instantaneous, including computation, communication, measurement and state preparation.

In a nutshell, the noisy-storage model assumes that it is challenging to store many qubits without making any errors. Given that no experimental implementation can reliably store more than a handful

of qubits right now, this is a technologically well-motivated assumption. However, it is possible to achieve security even if the adversary could store thousands of qubits - we need to send more qubits during the protocol.

The secuirty of cryptographic protocols in the noisy storage model are proved by introducing certain time delays Δt which force any adversary to use the storage device for a time at least Δt. The assumptions imply that the best an adversary can do is to read out the information from the device immediately after time Δt, as any further delay will only degrade his information further.Thus, to analyze the security, $\mathcal{F} = \mathcal{F}_{\Delta t}$ can be considered, instead of the family $\{\mathcal{F}_t\}_{t\geq 0}$. Note that since the adversary's actions are assumed to be instantaneous, he can use any error-correcting code even if the best encoding and decoding procedure may be difficult to perform. Summarizing, the noisy storage model assumes that

1. The adversary has unlimited classical storage, and (quantum) computational resources.

2. Whenever the protocol requires the adversary to wait for a time Δt, he has to measure/discard all his quantum information except what he can encode (arbitrarily) into $\mathcal{H}_{in}$. This information then undergoes noise described by $\mathcal{F}$.

Noisy Storage Model allows achieving security, in principle, for any cryptographic problem in which Alice and Bob do not trust each other. Two-party cryptographic primitives [WCSL10a] such as oblivious transfer and bit commitment are proven to be unconditionally secure [WCSL10b, KWW12a] for realistic noise levels, against the most general attack. Experimental Implementation of these protocols was demonstrated with present-day hardware used for quantum key distribution was demonstrated [ENG+14, NJCM+12]. A quantum protocol for oblivious transfer was experimentally demonstrated for optical continuous-variable systems, and the security was proved in the noisy-storage model [FGS+18b].

4.4 Quantum data locking

The phenomenon of *Quantum Data Locking* (QDL) can be exploited to obtain efficient high-dimensional QKD protocols within the assumption that Eve has access to a quantum memory of unlimited capacity, but that can store quantum information only for a finite time. This assumption implies that she is forced to measure her share of the quantum system within a given time after having obtained it. When the memory time goes to zero, we obtain as a limiting case the setting of personal attacks, where Eve is forced to measure the signals as soon as she receives them. We first briefly review the security criterion against an eavesdropper with time-limited quantum storage, and then we review the methodology behind the Quantum Data Locking.

4.4.1 Security against eavesdropper with time-limited storage

Suppose Alice wishes to use a memoryless quantum channel $\mathcal{N}_{A\to B}$ to send private information to Bob. Upon n uses of the channel, she encodes M messages $x = 1, \ldots, M$, each with probability $p_X(x)$, into the input states $\rho_A(x)$'s. Then Bob will receive the output states $\rho_B(x) = \mathcal{N}_{A\to B}^{\otimes n}(\rho_A(x))$. Let us recall that a quantum channel $N_{A\to B}$ can always be represented as the reduced dynamics induced by a unitary transformation on a larger space, that is,

$$\mathcal{N}_{A\to B}(\rho_A) = \mathrm{Tr}_E\left[U(\rho_A \otimes \omega_E)U^\dagger\right] \tag{4.12}$$

where ω_E is a pure state for a quantum system associated with the environment of the channel, and U is a unitary transformation coupling the system with its environment. In the worst-case scenario the eavesdroper Eve might collect all the information leaking into the channel environment, in which case the state obtained by Eve reads $\rho_E(x) = \tilde{\mathcal{N}}^{\otimes n}_{A\to E}(\rho_A(x))$, where $\tilde{\mathcal{N}}_{A\to E}$ is the complementary channel, defined as

$$\tilde{\mathcal{N}}_{A\to E}(\rho_A) = \mathrm{Tr}_B\left[U(\rho_A \otimes \omega_E)U^\dagger\right] \tag{4.13}$$

Let us consider the state

$$\sigma_{XE} = \sum_{x=1}^{M} p_X(x)|x\rangle\langle x| \bigotimes \rho_E(x) \tag{4.14}$$

This state describes the correlations between the classical input x and Eve's quantum system. To quantify the security of the channel one usually considers the trace distance,

$$\Delta := \frac{1}{2}\|\sigma_{XE} - \sigma_X \otimes \sigma_E\|_1 \tag{4.15}$$

where $\sigma_X = \sum_{x=1}^{M} p_X(x)|x\rangle\langle x|, \sigma_E = \sum_{x=1}^{M} p_X(x)\rho_E(x)$ are the reduced states of σ_{XE} and $||\cdot||_1 = \mathrm{Tr}|\cdot|$. If the trace distance is small, this implies that the state σ_{XE} is close to the uncorrelated state $\sigma_X \otimes \sigma_E$. Recall that, from an operational point of view, the trace distance is the bias in distinguishing the states by a measurement. The trace norm is indeed the standard security quantifier used in quantum key distribution: if $\Delta \leq \epsilon$, the communication protocol is secure up to a probability ϵ.

The trace norm is the proper security quantifier in a generic setting. However, under certain assumptions on the technological capabilities of the eavesdropper, we can adopt a weaker security criterion. If we know that the eavesdropper cannot store quantum information for longer than a given time τ, then we know that she is forced to make a measurement within a time τ after she received the quantum state. This leads us to consider a post-measurement security quantifier. A measurement Λ on Eve's system defines a classical random variable Y with conditional probability distribution

$$p^\Lambda_{Y|x}(y) = \mathrm{Tr}\left(\rho_E(x)\Lambda(y)\right) \tag{4.16}$$

where $\{\Lambda_y\}$ are POVM elements, satisfying $\Lambda_y \geq 0$ and the completeness relation $\sum_y \Lambda_y = \mathbb{I}$. A post-measurement security criterion requires that the joint probability distribution $p^\Lambda_{XY}(x,y) = p_X(x)p^\Lambda_{Y|x}(y)$ is close to the product of its marginals $p_X(x)p^A_Y(y)$, where $p^\Lambda_Y(y) = \sum_x p_X(x)p^\Lambda_{Y|x}(y)$, for all measurements Λ. Here we consider the distance

$$\Delta_{\mathrm{acc}} := \max_\Lambda \frac{1}{2}\left\|p^\Lambda_{XY} - p_X p^\Lambda_Y\right\|_1 \tag{4.17}$$

(the meaning of the subscript "acc" will be clear in the next paragraph) where $\frac{1}{2}\left\|p^\Lambda_{XY} - p_X p^\Lambda_Y\right\|_1 = \frac{1}{2}\sum_{x,y}\left|p_X(x)p^\Lambda_{Y|x}(y) - p_X(x)p^\Lambda_Y(y)\right|$ is the total variation distance. The operational meaning of Δ_{acc} is the bias in distinguishing between the classical distributions p^Λ_{XY} and $p_X p^\Lambda_Y$. In other words, Δ_{acc} is the bias in distinguishing between the states σ_{XE} and $\sigma_X \otimes \sigma_E$ by a local measurement.

The accessible information is an entropic quantity naturally associated with the distance Δ_{acc}. Let us recall that the accessible information is defined as the maximum classical mutual information that Eve can obtain about the input variable by local measurements on her subsystem, that is,

$$I_{\mathrm{acc}}(X;E) = \max_\Lambda I(X;Y) \tag{4.18}$$

where $I(X;Y) = H(X) + H(Y) - H(XY)$ is the classical mutual information of the variables X and Y. From Alicki-Fannes' inequality [AF04] :

$$I_{\text{acc}}\,(X;E) \leq 2\Delta_{\text{acc}}\,\log d^n + \eta\,(2\Delta_{\text{acc}}\,) \tag{4.19}$$

where $\eta(\cdot) = -(\cdot)\log(\cdot)$. On the other hand, Pinsker's inequality yields [FHT03]

$$\Delta_{\text{acc}} \leq \sqrt{\frac{1}{2} I_{\text{acc}}(X;E)} \tag{4.20}$$

These two inequalities imply the effective equivalence of Δ_{acc} and $I_{\text{acc}}\,(X;E)$ as security quantifiers. If the accessible information is small, Pinsker's inequality implies that the Δ_{acc} is also small. Viceversa, if Δ_{acc} is small, then the accessible information is small provided $\Delta_{\text{acc}} << (\log d^n)^{-1} = n^{-1}/\log d$.

4.4.2 Comparison with BB84

The first QDL protocol was discussed in Ref. [DHL+04, HLSW04]. Such a protocol is analogous to BB84, with the fundamental difference that Alice and Bob share one secret bit at the protocol's beginning. While in BB84, Alice and Bob randomly select their local basis and only later reconcile their choice in the sifting phase, in QDL, they use the 1 bit of information they secretly share to agree on the choice of the basis on which to encode (and decode) information. Therefore, according to this secret bit, Alice encodes n bits into n qubits, using either the computational or the diagonal basis, and Bob measures the received qubits on the same basis. We follow the original presentation of Ref. [DHL+04] and assume a noiseless channel from Alice and Bob. Suppose that Eve intercepts the n signal qubits. As she is forced to measure them (either instantaneously or after a given time), the amount of information she can obtain about the message can be quantified by the accessible information.

While it is clear that Eve has to measure her share of the quantum state at a certain point, the accessible information criterion is sensitive to the time at which such a measurement takes place. If Eve obtains a small amount of side information before she measures her share, she could use it to increase her accessible information by a disproportionate amount. Consequently, accessible information security is not, in general, composable [KRBM07]; that is, a secure protocol according to the accessible information criterion may not remain so when used as a subroutine of another communication protocol. On the other hand, if Eve obtains K bits of side information after the measurement, then (since the classical mutual information obeys total proportionality) her accessible information cannot increase by more than K bits, and composable security will be granted.

As is customary in quantum key distribution, the secret key generation protocol using quantum data locking is divided into two parts. The first part is a QDL protocol in which Alice encodes her share of the raw key into quantum states and sends them to Bob via an insecure quantum channel. After Bob measures the channel's output, he obtains his share of the raw key to be reconciled with Alice's one. The security of this part is offered by the QDL effect and is quantified by the accessible information. Alice sends error-correcting information to Bob through a public channel (in our case, there is no need for privacy amplification since the raw key is already secure due to QDL. Hence, we are in a situation where the QDL protocol is used as a subroutine of the key distribution protocol. This implies that the latter will be secure only if the former is secure in the composable sense. As discussed above, this is, in general, true only under the assumption that Eve has already measured

her share of the quantum state when the second part of the protocol takes place. If Alice knows that Eve's quantum memory has a coherence time not more extensive than τ, she can wait for a sufficiently long time before sending error-correcting information to Bob through the public channel.

4.4.3 QDL under noiseless channel setting

In a quantum data locking protocol [DHL+04, HLSW04] the legitimate parties Alice and Bob initially share a secret key of $\log K$ bits. They use the key to agree on a code to send classical information through a quantum channel. If they publicly declare a list of K codes, they can secretly use the shared key to agree on one of them. On the other hand, if an eavesdropper, who does not know the secret key, intercepts, and measures the quantum codewords, we require that her accessible information about the input messages must be negligibly small.

Let us first consider the case in which the channel from Alice to Bob is noiseless. In this case, Alice can encode classical information using a set of orthogonal n -qudit states belonging to a given basis. If Bob knows Alice's basis, he can reliably decode by measuring on the same basis. Suppose that Eve intercepts the whole set of n qudits. To ensure security, K must be chosen large enough to make Eve's mutual information negligibly small. It was shown in [FHS13] that for n large enough, there exist choices of

$$\log K = 4 \log 1/\epsilon + O(\log \log 1/\epsilon) \tag{4.21}$$

bases such that

$$I_{\text{acc}}(X;E) \leq \epsilon \log d^n \tag{4.22}$$

Notice that for any given (small) ϵ and n large enough, this implies that a relatively small secret key is sufficient to lock an arbitrarily long message. It is worth stressing that this result represents a strong violation of classical information theory in the quantum framework. Indeed, it is well known that in the classical framework, the secure encryption of a message of m bits requires at least m bits of the secret key (this result is based on the security of the one-time pad). The results of [FHS13] imply that one can lock information through a noiseless qudit channel at a rate of $\log d$ bits per channel use by consuming secret key at a rate (in bits per channel use) of

$$k = \frac{1}{n} \log K \sim \frac{1}{n} \log 1/\epsilon \tag{4.23}$$

Such a secret-key consumption rate is asymptotically zero if ϵ is constant or decreases sub-exponentially in n.

4.4.4 QDL under noisy channel setting

While the phenomenon of quantum data locking has been known for more than ten years, the problem of locking information through noisy channels has been considered only recently in [GHK+14a], where the notion of locking capacity of a noisy channel was introduced. The latter is defined as the maximum number of bits per channel use that can be reliably sent through a given channel in such a way that the eavesdropper's accessible information is negligibly small.

Two notions of locking capacities have been defined. The *weak-locking capacity* is defined by requiring security against an eavesdropper who measures the channel's output from Alice to Bob. The *strong-locking capacity* instead requires security against an eavesdropper having direct access to the input states prepared by Alice. In an optical setting, a cipher based on the quantum data locking

effect is dubbed a *quantum enigma machine* [GHK+14a]. While the twentieth century's Enigma machine relied on computational security (the presumed difficulty of inverting the intricate pattern of electromechanical elements that was used to scramble the inputs of a typing machine), a quantum enigma machine would ensure provable information-theoretical security against an eavesdropper who cannot store quantum information for an arbitrarily long time.

Alice and Bob publicly agree on a set of K codes $\mathcal{C}_1, \ldots \mathcal{C}_K$, where each code contains M equiprobable codewords $\mathcal{C}_k = \{|\psi_k(x)\rangle\}_{x=1,\ldots,M}$, with $|\psi_k(x)\rangle \in \mathbb{C}^{d^n}$. In a strong-locking scenario Eve intercepts the input states $|\psi_k(x)\rangle$'s. since she does not know the code, the state (4.14) reads:

$$\sigma_{XE} = \frac{1}{M}\sum_{x=1}^{M} |x\rangle\langle x| \otimes \frac{1}{K}\sum_{k=1}^{K} |\psi_k(x)\rangle\langle\psi_k(x)| \tag{4.24}$$

Putting $\rho(x) = K^{-1}\sum_{k=1}^{K} |\psi_k(x)\rangle \langle\psi_k(x)|$ and $\rho = M^{-1}\sum_{x=1}^{M}\rho(x)$, the accessible information of σ_{XE} reads

$$I_{\mathrm{acc}}(X;E) = \max_{\Pi}\left\{\log M - \sum_y \mathrm{Tr}\left(\rho\Pi_y\right)\log \mathrm{Tr}\left(\rho\Pi_y\right) + \sum_{xy} M^{-1}\,\mathrm{Tr}\left(\rho(x)\Pi_y\right)\log\left[M^{-1}\,\mathrm{Tr}\left(\rho(x)\Pi_y\right)\right]\right\} \tag{4.25}$$

where the maximum is over POVM's Π.

By convexity of mutual information, the maximum is achieved for a rank-one measurement with POVM elements of the form $\Pi_y = \mu_y |\phi_y\rangle \langle\phi_y|$ where the $|\phi_y\rangle$'s are unit vectors and $\mu_y > 0$. The condition $\sum_y \mu_y |\phi_y\rangle \langle\phi_y| = \mathbb{I}$ implies $\sum_y \mu_y/d^n = 1$. Putting $Q_x(\phi_y) = \langle\phi_y|\rho(x)|\phi_y\rangle$, we then obtain

$$I_{\mathrm{acc}}(X;E) = \log M - \min_{\{\mu_y|\phi_y\rangle\langle\phi_y|\}} \sum_y \frac{\mu_y}{M}\left\{H\left[Q\left(\phi_y\right)\right] - \eta\left[\sum_x Q_x\left(\phi_y\right)\right]\right\} \tag{4.26}$$

where $H\left[Q\left(\phi_y\right)\right] = -\sum_x Q_x\left(\phi_y\right)\log Q_x\left(\phi_y\right)$. Finally, we notice that the positive quantities μ_y/d^n can be interpreted as probability weights. An upper bound on the accessible information is then obtained by the fact that the average cannot exceed the maximum, which yields

$$I_{\mathrm{acc}}(X;E) = \log M - \frac{d^n}{M}\min_{\{\mu_y|\phi_y\rangle\langle\phi_y|\}} \sum_y \frac{\mu_y}{d^n}\left\{H\left[Q\left(\phi_y\right)\right] - \eta\left[\sum_x Q_x\left(\phi_y\right)\right]\right\} \tag{4.27}$$

$$\leq \log M - \frac{d^n}{M}\min_{|\phi\rangle}\left\{H[Q(\phi)] - \eta\left[\sum_x Q_x(\phi)\right]\right\} \tag{4.28}$$

where the minimum is over all unit vectors $|\phi\rangle \in \mathbb{C}^{d^n}$.

We now show that for certain choices of the codes $\mathcal{C}_k$'s, the accessible information is smaller than $\epsilon \log d^n$ for n and K large enough. Consider the case of random codes, where the codewords in $\mathcal{C}_k$ are chosen i.i.d. from a certain ensemble of states. Then for any given x and $|\phi\rangle$ the quantity

$$Q_x(\phi) = \frac{1}{K}\sum_{k=1}^{K} |\langle\psi_k(x) \mid \phi\rangle|^2 \tag{4.29}$$

is the sum of random variables which, for K large enough, will converge to its average $\mathbb{E}\left[Q_x(\phi)\right]$. If the random codewords are chosen from an isotropic ensemble, that is, one satisfying $\mathbb{E}_\psi[|\psi\rangle\langle\psi|] =$

$\mathbb{I}/d^n$, then $\mathbb{E}\left[Q_x(\phi)\right] = 1/d^n$. In turn, if $Q_x(\phi) \sim (1 \pm \epsilon)/d^n$, then $H[Q(\phi)] \gtrsim (1-\epsilon)M/d^n \log d^n$, and $\eta\left[\sum_x Q_x(\phi)\right] \sim \eta\left[M/d^n\right] = -M/d^n \log M/d^n$, which finally implies $I_{\text{acc}}(X;E) \lesssim \epsilon \log d^n$

The minimum value of K for which $Q_x(\phi)$ is close enough to its average for all x and $|\phi\rangle$ can be obtained by applying suitable concentration inequalities [AW02, PGPBL09]. For n large enough and if ϵ decreases sublinearly with n, we have obtained the following condition on K [LL15c],

$$\frac{1}{n} \log K \gtrsim \max\{\log \gamma, \log d - \chi\} \tag{4.30}$$

where $\chi = \frac{1}{n} \log M$ is the communication rate, and

$$\gamma^n = \frac{\mathbb{E}\left[Q_x(\phi)^2\right]}{\mathbb{E}\left[Q_x(\phi)\right]^2} = \mathbb{E}\left[Q_x(\phi)^2\right] d^{2n} \tag{4.31}$$

Notice that the factor γ depends on the ensemble from which the random codewords are drawn.

If the codewords are drawn from the uniform distribution on the unit sphere in $\mathbb{C}^{d^n}$, one obtains $\mathbb{E}\left[Q_x(\phi)^2\right] = \frac{2}{d^n(d^n+1)}$, which yields $\gamma^n = \frac{2d^n}{d^n+1}$. If the channel from Alice to Bob is noiseless, we have $\chi = \log d$ and thus obtain an asymptotically vanishing secret-key consumption rate, $\lim_{n\to\infty} \frac{1}{n} \log K = 0$. This result corresponds to the findings of [HLSW04, FHS13] which considered random codewords in a high-dimensional Hilbert space and obtained quantum data locking protocols with zero asymptotic secret-key consumption rate through a noiseless channel.

Suppose instead that the codewords are of the form $|\psi_k(x)\rangle = \otimes_{j=1}^n |\psi_{k,j}(x)\rangle$, where for any $j = 1, \ldots, n$, the vectors $|\psi_{k,j}(x)\rangle$'s are drawn i.i.d. from the uniform distribution on the unit sphere in $\mathbb{C}^d$. For these separable codewords we obtain $\mathbb{E}\left[Q_x(\phi)^2\right] = \left[\frac{2}{d(d+1)}\right]^n$, which yields $\gamma^n = \left(\frac{2d}{d+1}\right)^n$. This result corresponds to the quantum data locking protocols discussed in [LL15c]. Given a noisy channel allowing a classical communication rate χ, we obtain a secret-key consumption rate of $k = \max\{1 - \log(1+1/d), \log d - \chi\}$ bits per channel use.

4.4.5 Application

The results reviewed in the previous section can be applied to achieve secure communication against an eavesdropper with time-limited quantum storage. Suppose Alice and Bob initially share nk bits of the secret key. They can use this secret key to lock n uses of the quantum channel. If the channel allows a classical communication rate of χ bits per channel use, they will be able to communicate about $n\chi$ bit of locked information.

After a waiting time sufficiently longer than the coherence time of Eve's quantum memory, Alice and Bob can run a second quantum data locking protocol. If $\chi > k$, they can recycle nk bits of the previous message as a secret key for the new round of quantum data locking. Many times, by repeating this procedure, they will achieve a net rate of locked communication of $r = \chi - k$ bits per channel use.

Discrete variable QDL

A simple non-trivial example of noisy communication is the d -dimensional erasure channel. Upon n uses of the erasure channel, Alice prepares quantum data locking codewords of the form $|\psi_k(x)\rangle = \otimes_{j=1}^n |\psi_{k,j}(x)\rangle$, where $|\psi_{k,j}(x)\rangle$ are random codewords drawn from the uniform distribution on the unit sphere in $\mathbb{C}^d$. Given that the channel from Alice to Bob is a memoryless qudit erasure channel

with erasure probability p, they can achieve a classical communication rate (in bits per channel use) of

$$\chi = (1-p)\log d \tag{4.32}$$

The complementary channel from Alice to Eve is also a qudit erasure channel, with erasure probability $(1-p)$. As discussed in the previous section, a secret-key consumption rate of $k = \max\{1-\log(1+1/d), \log d - \chi\}$ bits is needed for quantum data locking. In our example, the erasure channel from Alice to Eve will erase all but a fraction p of the qudits sent by Alice. This implies that the secret-key consumption rate will be also reduced by a factor p, leading to $k = \max\{p - p\log(1+1/d), p\log d - \chi\}$. For an 8 -bit channel $(d = 256)$, the net rate of weak locking for the erasure channel,

$$r = \chi - k = (1-p)\log d - \max\{p - p\log(1+1/d), (2p-1)\log d\} \tag{4.33}$$

compared with its classical capacity $C = (1-p)\log d$ and the private capacity $P = (1-2p)\log d$. Similar results are obtained for other channels of the form $\tilde{\mathcal{N}}_{A\to E}(\rho) = (1-p)\rho + p\rho_0$, where ρ_0 is a given density operator [LL15c].

Continuous variable QDL

We now see the application of quantum data locking to a continuous-variable quantum system. In [LL15a] authors have considered the case of a lossy bosonic channel with transmissivity η, where the input codewords are multimode coherent states drawn from a Gaussian distribution with N mean photons per mode. Although the quantum system has infinite dimensions, it is sufficient to consider the typical subspace spanned by these random codewords. For n -mode coherent states, such a typical subspace has dimension $d^n \sim 2^{ng(N)}$, with $g(N) = (N+1)\log(N+1) - N\log N$. Here we consider a weak-locking scenario where Eve measures the complementary channel, which in this case is also a lossy bosonic channel with transmissivity $(1-\eta)$. Inspired by [PGPBL09] we have introduced a reverse-reconciliation protocol for secret-key generation by quantum data locking. In this protocol, Alice and Bob publicly agree on a collection of measurements Π_k, for $k = 1, \ldots, K$. Then Alice locally prepares an entangled bipartite state and sends one subsystem to Bob through the quantum channel. According to the pre-shared secret key's value, Bob makes the measurement Π_k. This induces a virtual backward quantum channel from Bob to Alice. As shown in [6], this protocol may achieve an asymptotic classical communication rate of $\chi = g(N) - g\left[(1-\eta)N'\right]$ bits per mode, with $N' = N/(1+\eta N)$. On the other hand, weak locking can be obtained with a secret-key consumption rate of $k = 2g[(1-\eta)N] - g\left[(1-\eta)N'\right] - g\left[(1-\eta)N''\right]$ with $N'' = (1+2\eta N)N'$. In this way, we achieve a net weak-locking rate of $r = \chi - k$ bits per mode which, in the limit of $N \to \infty$ yields, for any $\eta > 0$

$$r = \log\left(\frac{1}{1-\eta}\right) + 1 \tag{4.34}$$

This yields a rate larger than 1 bit per mode for any non-zero transmissivity, i.e., a constant rate of secret-key generation across arbitrarily long communication distances.

The obtained rate of weak-locking can be compared with the secret-key rate achievable assuming the standard security criterion quantified by the trace distance. For the lossy channel a lower and an upper bound on this rate are respectively given by $r_{lb} = \log\left(\frac{1}{1-\eta}\right)$ and $r_{ub} = \log\left(\frac{1+\eta}{1-\eta}\right)$.

Part II

Quantum Computational Hybrid Cryptography

Chapter 5

Quantum Computational Time-lock security model

5.1 Introduction

As presented in Chapter 3 the use of quantum resources enables cryptographic primitives that are not achievable with classical means such as QKD or QRNG. Theoretical quantum cryptography has largely developed around the central challenge of proposing explicit quantum and information-theoretically-secure versions of the core cryptographic services used in our digital world. This ambitious plan has been extremely fruitful, driving the quantum cryptographic field from a small community of pioneers in the 1980s, to an established field today, exemplified by the IACR conference QCrypt and the development of a quantum industry, in which quantum cryptography is playing a prominent role.

However, current QKD systems have now reached levels of performance essentially comparable to the fundamental limits on the secret capacity [PLOB17a, TGW14]. This indicates the impressive technological maturity that quantum communications engineering has reached. Conversely, this also fundamentally limits our hope to experience large performance gains for QKD in the future. A fundamental challenge for theoretical quantum cryptography therefore consists in understanding the relations and trade-off between security models and achievable cryptographic primitives and secure functionalities.

Extending the functionality and overcoming the performance limitations of quantum-based secure communications hence requires to consider a broader picture. This can consist of pushing further the entanglement frontier, by developing our ability to send, store and process large entangled states. Such fundamental efforts will be crucial for developing large-scale quantum information processing, however, it requires some complex technological challenges to be overcome.

The approach we consider in this chapter explores a complementary space: consider security models weaker than unconditional security and characterize the gain in practicality (i.e. performance and functionality, over cost). This approach requires a clear bench-marking of the security gain, with respect to classical cryptography, and the "security cost" related to the assumptions that have been introduced.

In this chapter, we propose to explore the benefits that can be taken from assuming short-term computational security of one-way function (say AES for short). This assumption positions our work in a space outside of unconditional security. However, we want to recall here that such an assumption is more conservative than assuming the *long-term security* of AES.

This latter option is however implicitly made in the context of many QKD practical deployments [PLL+09, SFI+11, DLQY16, ZXC+18], when QKD is used to renew AES encryption keys, leading to a secure communication construction that is only as secure as AES, and in which the added value of QKD is highly questionable. [PPS04, ABB+14, Ber]

We want to claim that the direction we consider here might be a rational way out of the real-world quantum cryptography conundrum: namely to explore a space of assumptions where quantum cryptography can offer a clear security advantage over classical cryptography, namely a world in which one-way-functions would not be long-term-secure, but could still be used at short-term, to boost the performance of quantum cryptography beyond the fundamental performance bounds [PLOB17a, TGW14], that might be too restrictive for real-world use [Sas17].

5.2 Time-lock

A *time-lock* is a part of a locking mechanism commonly found in bank vaults and other high-security containers, designed to prevent the opening of the safe or vault until it reaches the preset time. An authorized employee of the bank can open the vault, however, any unauthorized thief or attacker trying to break in the vault cannot open it before this preset time. Combined with an extra security mechanism, such as an alarm alerting the Sheriff, the time-lock forms a very effective security mechanism. Quantum Computational Time-lock construction will essentially follow the same principle, however, in that case, a computational one-way function will play the role of the time-lock mechanism, while the decoherence (of quantum storage), plays the role of the Sheriff.

5.3 Short term secure encryption

Definition 5.3.1 (Computationally secure encryption scheme) *The encryption scheme* $(\mathrm{Gen}; \mathrm{Enc}; \mathrm{Dec})$ *is computationally secure, if for all sequential polynomial-time adversaries* $A : \{0,1\}^* \to \{0,1\}$ *there exists a negligible function* negl *such that for all* $m_0, m_1 \in \{0,1\}^*$,

$$\left| \Pr[A(\mathrm{Enc}_k(m_0) = 1) - \Pr[A(\mathrm{Enc}_k(m_1) = 1)] \right| \leq \mathrm{negl}(n) \tag{5.1}$$

In the above definition we have used the notion of sequential polynomial time. This is the notion of polynomial time usually employed in cryptography [Unr15a] that counts all executions steps, no matter whether they are in parallel or sequential. Thus sequential polynomial time is more or less independent of the machine model, but for concreteness we specify that an algorithm is sequential-polynomial-time if it can be implemented by a quantum circuit that is output by a probabilistic polynomial-time Turing machine (the Turing machine may run in polynomial-time in the size of both the classical and the quantum input).

Definition 5.3.2 (T-secure encryption) *An encryption scheme is T-secure if it can provide computational security against an adversary accessing the encrypted message during a time, at most T.*

We refer to Alice and Bob as authorized parties who have access to T-secure encryption and Eve as an unauthorized party who does not have access to T-secure encryption.

An example of T-secure encryption is the time-release encryption [Unr15a] (also-known-as time-lock puzzle). Timed-release encryption (TRE) is a two-factor encryption scheme combining public key encryption and time-dependent encryption – decryption requires a trapdoor which is kept confidential by a time-server until at an appointed time. A T-timed-release encryption algorithm takes a message m and "encrypts" it in such a way that the message cannot be decrypted within time T by an "untrusted party", but can be decrypted after time $T' > T$. TRE constructions based on iterated hashing are secure against a quantum adversary [Unr].

Uncloneable encryption is a very similar notion to that of short term secure encryption. It is an encryption scheme where without the key, one cannot make a copy of the cyphertext. Unknown Recipient Encryption (URE) guarantees that if the cyphertext arrives at a recipient, he can verify that no one else got the plaintext. (The "unknown" in "unknown recipient encryption" means that it is not necessary to know the recipient beforehand, not that the recipient will be kept secret.)

Proposition 5.3.1 *If an encryption scheme is computationally secure, then it is also a T-secure encryption provided the adversary is sequential polynomial time limited during a time at least T.*

.

Proof: The proof of the proposition follows from Definition 5.3.1, according to which an encryption is computationally secure against sequential polynomial-time adversaries. Thus, if an adversary is assumed to be sequential polynomial-time limited for time a at least T, then the encryption scheme is computationally secure until time T. As a result, following Definition 5.3.2, the encryption scheme $(\mathrm{Gen}; \mathrm{Enc}; \mathrm{Dec})$ is T-secure. □

Everlasting security based on shot-term computational security assumption A cryptographic protocol has everlasting security if it is secure against adversaries that are computationally unlimited after the protocol execution. As underlined in [Unr10], such model is well suited to scenario requiring long-term security, but where we cannot predict which cryptographic schemes will be broken, say, several decades after the protocol execution. Everlasting secure communication cannot be obtained solely with classical means and computational techniques, since a classical communication can always be copied, stored, and attacked later. In [Unr10] Unruh established in a variant of the Universal Composability framework, that everlasting secure communications and general secure multi-party computation is achievable with quantum resources and using signature cards as a trusted setup.

Another recent work illustrates how the relaxation from unconditional to everlasting security can be used to strongly boost the practicality of Device-Independent QKD [MDCAF20]. As a matter of fact, the short-term security (during protocol execution) of post-quantum cryptographic assumptions can be leveraged to relax the extremely stringent requirement for loophole-free Bell tests.

5.4 Time-limited quantum storage

Definition 5.4.1 (t_{coh}-decohering quantum memory) *A quantum memory is t_{coh}-decohering if it's evolution can be described by a complete positive trace-preserving map $\mathcal{N}_{t_{coh}} : \rho \to \mathcal{N}_{t_{coh}}(\rho)$, such that*

$$\left|\left|\mathcal{N}_{t_{coh}}(\rho) - \frac{\mathbb{I}_d}{d}\right|\right|_1 = \mathcal{O}\left(\frac{1}{d}\right) \tag{5.2}$$

Where, the evolution $\mathcal{N}_{t_{coh}}$ is Markovian and d is the dimension of the memory.

In the above definition, we considered the evolution of the quantum storage to be Markovian, i.e., the family $\{\mathcal{N}_T\}_{T>0}$ is a continuous one-parameter semi-group

$$\mathcal{N}_0 = \mathbb{I} \text{ and } \mathcal{N}_{T_1+T_2} = \mathcal{N}_{T_1} \circ \mathcal{N}_{T_2}. \tag{5.3}$$

This assumption tells that the noise in the quantum memory increases over time, and is essential to ensure that the adversary cannot gain any information by delaying the readout.

Given the technological challenges associated with quantum storage [SAA+10], a reasonable assumption consists in assuming that the adversary is generically limited in its capacity to store quantum information. This is in contrast with QKD, which is defined under the assumption that an adversary have unlimited quantum storage and computational resources. While this assumption have laid a ground for high level of theoretical security guarantee, the former may be considered unrealistic given the current developments in quantum technologies.

The *bounded-quantum storage model*, introduced by Damgard, Fehr, Salvail and Schaffner [DFSS08] is one different security model which assumes that the potential adversary can only store a limited amount of qubits. Furthermore, this number is assumed to grow only sublinearly with the number of bits exchanged between Alice and Bob. Thus, the security is generally proved by overflowing adversary's quantum memory. In general the assumptions of bounded quantum storage allow us to increase the resilience to noise of a QKD protocol, but the rate is not expected to improve dramatically compared to an unbounded quantum-capable eavesdropper.

This model is inspired by the classical bounded storage model, [CM97a], for which a cryptographic advantage can only provided, for key establishment, against an attacker whose memory size is less than quadratic with respect to the one of legitimate users [DM04], thereby limiting the impact of such model in practice, in an era where cheap classical storage has become abundant. The bounded-quantum storage model allows to significantly widen the scope of cryptographic primitives that can be constructed with quantum resources, in particular Oblivious Transfer (OT), Bit Commitment (BC) and password-based identification [DFSS08].

The *noisy storage model*, introduced by Wehner, Schaffner and Terhal [WST08b] provides a more realistic way to account for the difficulty of storing quantum information. It assumes that the attacker has an arbitrary amount of quantum storage, whose quality, in particular, degrades with time. Assuming time-degradation of the classical capacity of the storage enables to prove the unconditional security of OT and BC [KWW12b], while entanglement sampling technique allows to extend the validity of the noisy storage to the case where the time-limited bound applies to the quantum capacity [DFW14]. The notion of time-limited quantum memory is similar to the noisy-storage model [WST08a]. The assumption of bounded quantum storage deals with the noiseless case (but assumes a small amount of storage), whereas the noisy-storage model deals with the case of noise (but possibly a large amount of storage). New protocols for bit commitment and oblivious transfer based on weak string erasure have been constructed in this security model, and the security is proved against arbitrary attacks [WST08a].

Another recent line of work, called *Quantum data locking* (QDL), is based on the even stronger assumption that quantum storage fully decoheres after some time limit. Relying on a pre-shared secret, legitimate users can then leverage the information locking property to design secure communication schemes, that rely on the time-limited quantum storage assumption to impose that the attacker is limited to accessible information. This assumption is in general not composable with the plain quantum security model of QKD. Different QDL constructions can then be used to upper

bound this accessible information. A first category relies on to single-photon encoding [GHK+14b] and has been experimentally demonstrated [LHA+16], with however standard (QKD-like) limitations in terms of loss-tolerance while requiring greater experimental complexity. A second category relies on continuous-variable encoding, and could in principle be used to reach quantum data locking secure rates close to the classical capacity [LL15d]. However such constructions resort to random coding arguments for which practical implementation with structured measurement is not possible.

5.5 QCT security model

Model Assumptions As proposed in 2015 [All15] a novel security model that we later coined as **Quantum Computational Timelock** (QCT) security model. It is depicted on Figure 5.1 and consists of two nested assumptions:

Definition 5.5.1 (QCT security model) *It consist of two assumptions,*

1. *Alice and Bob are assumed to have access to a public authenticated classical channel and to an encryption scheme that is computationally secure with respect to any unauthorized attacker Eve for a time at least t_{comp} after a cyphertext is exchanged on the classical channel.*

2. *Eve's d-dimensional quantum memory is t_{coh}-decohering with $t_{coh} << t_{comp}$. Seeing the quantum memory as a channel, it can be written as as a time-dependent and complete positive trace-preserving map $\mathcal{N}_t : \rho \to \mathcal{N}_t(\rho)$, as defined in Equation 5.2.*

It is interesting to note that these two categories of assumptions, namely short-term computational security [Unr15b] and noisy quantum storage [KWW12b], have so far already been considered in quantum cryptography, yet only disjointly.

In the QCT Security Model we need some initial authentication between Alice and Bob, (See the Section 6.2 where the key establishment protocol based on QCT security model is described). This initial authentication can be based on an authenticated channel (which is an assumption then). Another alternative requires distributing a shared secret (with correct authentication) for authenticating communications over a public channel. In the latter case, the assumption is then about the ability to share an initial secret, with authentication.

Definitely we want the encryption scheme to be short term secure against a quantum computer. However, we did not specify on the kind of encryption schemes that can be considered under the QCT model assumptions. We can refine this QCT model assumption by considering that the short-term secure encryption (be it based on a symmetric or asymmetric scheme) is quantum secure, i.e. secure against a quantum computer.

The QCT security model explores a space of assumptions, namely, a world in which encryption schemes would not be long-term-secure but could still be used in short-term. Secondly, the optical quantum memories are technologically bound to decohere within a timescale shorter than when the encryption scheme is secure. The objective of this security model is to construct cryptographic protocols that can boost quantum cryptography's performance beyond the fundamental performance bounds [PLOB17a, TGW14], that might be too restrictive for real-world use [Sas17].

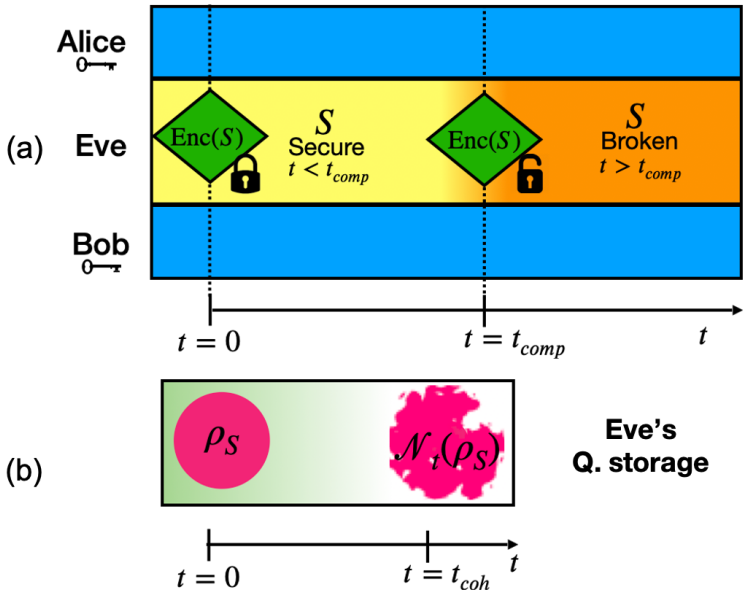


Figure 5.1: QCT security model: Assumption (a): Short-term secure encryption during time t_{comp}, during which Alice and Bob can exchange an ephemeral classical secret S. Assumption (b): Time-limited quantum memory, with coherence time $t_{coh} << t_{comp}$

.

5.6 Rationale of the QCT security model

The Quantum Computational Timelock (QCT) approach intends to reduce the divergence between practical and theoretical quantum cryptography and address the associated dilemma described in the previous subsection by devising a *hybrid security model*.

This QCT security model is positioned between the "absolute security model" used in QKD, where no assumptions limit the power of the attacker concerning the quantum channel (where some trust assumptions[1] must be fulfilled to guarantee the security of endpoints), and classical cryptographic security models based on computational hardness assumptions, that also require trusted classical hardware at the endpoints.

The rationale for the QCT security model is also rooted on a central observation: quantum cryptographic *functionalities* can in the broad sense be guaranteed assuming the existence of computational long-term-secure one-way-function [Gol09, ANS20]. This conversely implies that a *quantum cryptographic advantage* can only arise in stronger models, i.e. in security models where long-term computational security of one-way function (and therefore encryption) does not hold.

5.7 Validity of QCT security model

5.7.1 Validity of short term secure encryption assumption

The first assumption is reasonable to make as it only requires computational encryption to be secure for a short time, unlike classical cryptographic protocols, which assume that encryptions are difficult to break even after a very long time. The assumption is more conservative in assuming the *long-term*

[1] devices in Alice and Bob's lad are assumed to work exactly according to their specifications, and are shielded, i.e., they do not leak any information from leaking out of the lab.

security of encryption schemes like AES, which for instance, is assumed to be secured for the time of the order of 10^9 sec i.e., ≈ 30 years [Hat03]. This latter option is however implicitly made in the context of many QKD practical deployments [PLL+09, SFI+11, DLQY16, ZXC+18], when QKD is used to renew AES encryption keys, leading to a secure communication construction that is only as secure as AES, and in which the added value of QKD is highly questionable. [PPS04, ABB+14, Ber].

Definitely we want the encryption scheme to be short term secure against a quantum computer. However, We did not specify on the kind of encryption schemes that can be considered to be t_{comp}-secure. We can refine this QCT assumption by considering either public-key encryption scheme or secret-key encryption scheme to be short-term secure (against a quantum computer).

Advantages of considering public-key encryption schemes for short term secure computational assumption is that no shared initial secret key is required to start the key establishment protocol. Authentication of the classical channel and secret information sharing between authenticated parties can be done using the same public keys. Moreover, public-key encryption schemes are specifically beneficial when multiparty key distribution is desired. Unfortunately, there are no known constructions for public-key encryption schemes that are secure (even short-term secure) against a quantum computer.

Advantages of using symmetric-key encryption schemes for short term secure computational assumption is that there are no publicly known quantum attacks on classical symmetric-key cryptographic schemes and the cryptanalysis of symmetric-key classical cryptography on a quantum computer reduces to exhaustive search. Performing exhaustive key search given a known plaintext–cyphertext pair corresponds to the problem of finding an element in an unsorted database of N elements. The complexity of this problem is of $\mathcal{O}(N)$ on a classical computer but only of $\mathcal{O}(\sqrt{N})$ on a quantum computer.

5.7.2 Validity of time-limited quantum storage assumption

The practical implementation of an attack by an adversary on the time-limited quantum storage assumption will require efficient quantum storage with coherence time greater than the computational time ($t_{coh} > t_{comp}$), i.e., an adversary needs to be able to store quantum information for a time greater than the time for which encryption is assumed to be secure, and retrieve it on-demand later. A natural question to be asked is how plausible it is to achieve this requirement?

To provide the answer, in this section, we discuss today's quantum storage capabilities, by analyzing different experimental demonstrations of state of the art quantum memories. For the comparison, we only consider those experimentally demonstrated quantum memories,

- Which have shown storage of optically interfaced quantum light
- Storing light at a single photon level (quantum regime).

Based on the approach to light-matter coupling, we categorize quantum memories into two categories.

Single-atom-based quantum memories:

The first is a *single-atom-based quantum memory*, where a single atom is placed in a highly reflective optical cavity. Light shining into the cavity repeatedly reflects from its mirrors which can dramatically increase the absorption of an incoming photon. Based on different approach to design the quantum memory we briefly discuss following quantum memories:

Type of Quantum Memory	Approaches	Platform	Storage & retrieval Efficiency	Coherence Time
Single atom based quantum memories	Trapped ions [LMR+11]	Cold atoms	16%	139μs
	Nuclear spin	SiV centre [LLTG18]	NA	115ns
	Nuclear spin	NV centre (*proposed*) [PJH+17]	25%	40ns
	Cavity QED [KRRR15]	Cold atoms	39%	3μs
Ensemble based quantum memories	AFC [HEK+20]	Solid state	0.5%	0.53s
	EIT [CLW+13]	Cold gas	56%	54μs
	Raman scheme [VGTE+18]	Cold atoms	65%	60μs
	Cavity [EVGC+18]	Cavity	72%	110μs
	DLCZ[BBV+14]	Cold gas	82%	0.9μs
	GEM [CCE+16a]	Cold gas	87%	1ms

Table 5.1: Quantum storage time of different state of the art quantum memory systems. For the comparison, we considered experimentally demonstrated quantum memories which have shown storage of optically encoded quantum light, and are at single-photon level.

- **Trapped ions:** Memories such as *trapped ions:* have been shown to exhibit long coherence times on the order of 10 min [WUZ+17] though, not optically interfaced. Nevertheless, these memories can be optically interfaced by tuning the optical resonator's frequency near an atomic transition to create a dipole coupling between the atoms and the cavity field. For storage of photonic qubit in a single atom, the overall storage and retrieval efficiency of 16% for coherence time of 139μs was recorded [LMR+11].

- **Nuclear spin:** Quantum memory based on solid-state nuclear spin systems, such as *Silicon–vacancy centres* (SiVC) in diamonds have shown a coherence time of 115ns [PJH+17]. For *Nitrogen-vacancy centers* (NVC) in diamonds an experiment was proposed [LLTG18], which offers to achieve a coherence time of 40ns with an overall efficiency of 25%. A detailed review of optically interfaced solid-state quantum memories can be found here, [ACB+18].

- **Cavity QED:** *Superconducting circuit QED* are hybrid systems that have shown to exhibit a coherence time up to 100s [DS13]. However, since microwave photons are not well suited for long-distance communication, an optical-to-microwave interface is needed which introduces noise due to optical interactions. Heralded transfer of a polarization qubit from a photon onto a single atom with 39% efficiency and storage time of 3μs was realized [KRRR15].

Ensemble-based quantum memories:

Another approach is the *ensemble-based quantum memories* or the collective coupling. An ensemble of atoms is prepared in the ground state which is in a large superposition. The incoming photon is absorbed by the ensemble such that the state of the photon is delocalized over all the atoms in the ensemble. The collective state is then efficiently converted back into a single photon with a well-defined direction. We also report the storage and retrieval efficiency of these memories.

These memories have preferential importance due to their strong light-matter coupling and high bandwidths. The collective state in an ensemble of atoms is more robust to environmental dephasing. A large ensemble facilitates storing multiple photons in a single memory. A list of techniques has been deployed to develop such quantum memories.

- **Raman Schemes:** Warm vapor *Raman memory schemes* have been used to efficiently store GHz-bandwidth photons for up to nanoseconds with an efficiency of 30%[RNL+10, CCE+16b] and with cold atoms, the efficiency is of 65% with coherence time 60 μs [VGTE+18].

- **Electromagnetically Induced Transparency (EIT):** Electromagnetically Induced Transparency (EIT) is an optical phenomenon in atoms that uses quantum interference to induce transparency into an otherwise resonant and opaque medium. For quantum memory application using EIT, the coherence time was recorded up to 54 μs with an efficiency of 56%[CLW+13].

Both EIT and Raman memory schemes are optically controlled quantum memories, where a strong optical pulse is used to induce the absorption of photons into the storage medium. The main challenge of optically controlled quantum memories is the noise, in particular, as the single-photon level signal is emitted with a strong control beam, due to which the residual control beam becomes a serious source of noise in the single-photon signal band.

Another important scheme of quantum memory is called engineered absorption, which is based on the photon echo effect. There are two important approaches in this scheme:

- **Gradient Echo Memories GEM:** Memories designed using the GEM method have shown very high efficiency up to 90% with coherence time-limited to 100 μs. Laser-cold atoms used for GEM have produced an efficiency of 87% with a coherence time of 0.6 ms[CCE+16a].

- **Atomic Frequency Combs (AFC):** Solid-state AFC has shown lifetime storage up to few hundreds of ms, however, the efficiency is very low [OTW+18, HEK+20].

- **Optical Cavity:** An *optical cavity* is an effective method to enhance atom-light coupling strength. The cavity retains the photon and releases it when needed. The main advantages of a cavity-based quantum memory are its simple and inexpensive configuration and the very broad working wavelength range. However, due to the loss of the cavity, it cannot provide a long storage time. It has shown the efficiency of 72% with the coherence time of 110 μs [EVGC+18].

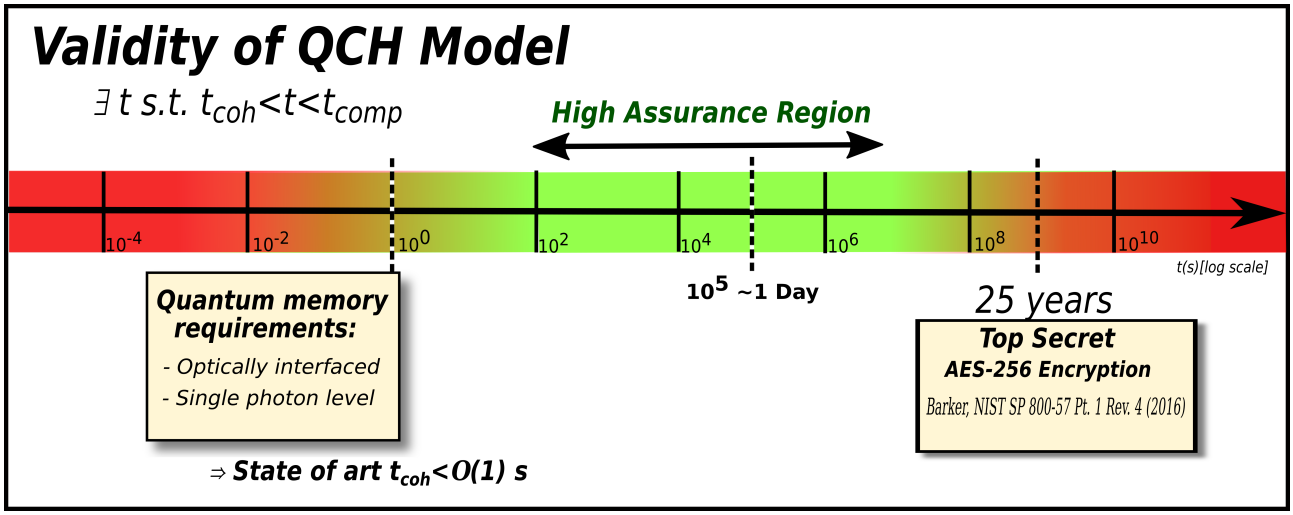


Figure 5.2: Validity of QCT security model with respect to existing computational hardness assumption for AES and demonstrated quantum storage coherence time at single photon level. For example, assuming $t_{comp} >\geq 10^5$ sec, seems safe.

5.7.3 Analysis

A practical lower bound on the value of t_{comp} can be inferred from assumed long-term security of the AES256 encryption scheme, that is considered to meet the requirements for long-term (30 years) confidentiality of Top Secret data [Hat03].

Regarding the coherence time of optically addressable quantum memory, as reviewed in above section, experimental demonstrations of storage and then retrieval of optically encoded quantum information, at single photon level. This indicates that the value of t_{coh} ranges from a few nanoseconds to microseconds [SAA+10].

Given the large gap between the upper bound on t_{coh} and lower bound on t_{comp}, the validity of the QCT security model can be assumed with a very high confidence today. This also leaves a considerable margin for its validity in the future. Finally, it has to be noted that aim here to build a key distribution protocol with everlasting security, which means in particular that the validity of the QCT security model only needs to hold at the time of protocol execution to provide information-theoretic security in the future. A comparison of efficiency and coherence time of different optical quantum memory systems is shown in Table [5.1]. Thus, assuming, for example, $t_{comp} = 10^5\, s \sim 1\,\mathrm{day}$, leaves a reasonable security margin with respect to the state of art in quantum storage capabilities, as shown in Figure 5.2.

5.8 Objectives of the QCT security model

The objective of the QCT security model is to enable performance and functionality improvements in quantum cryptography, while maintaining a clear advantage with respect to both classical cryptography (based on computational assumptions) and with respect to QKD.

- Security gain over classical cryptography. As we shall use the QCT approach to build a key establishment scheme, called MUB-QCT (presented in the next Chapter) the resulting protocol cannot be unconditionally secure due to the nature of the QCT assumptions. However, the

model is crafted to enable *everlasting security*. This means that the established keys can be provably secure against a computationally unbounded adversary, provided that the initial ephemeral encrypted communication is not broken by an adversary within a time shorter than the decoherence time of its available quantum storage (at protocol execution time). Such security level is impossible to reach only with classical means[2].

- Improvement of the performance envelope, with respect to QKD and more broadly to repeaterless quantum secret capacity fundamental bounds [PLOB17b]. This improvement will be sought by considering constructions where security can be proved in the regime where Alice sends multiple copies of the same quantum state to Bob, thereby increasing rates and loss tolerance with respect to discrete-variable QKD, whose security fundamentally relies on no-cloning and therefore forbids the emission of multiple copies. We will also target improvements in terms of practical security, stemming from reduced trust requirements associated with constructions in the QCT paradigm.

[2]The reason this lies in the definition of the everlasting security itself, where the unconditional security is guaranteed against an (passive) adversary who is computationally bounded during the execution of the protocol and computationally unbounded after the execution of the protocol. While following a classical cryptographic protocol a passive adversary can make copies of the classical information and stores them. After the execution of the protocol, the adversary can perform parallel computations using unlimited computational power and resource, and thus, in principle can break the security.

Chapter 6

From QCT to a Key Establishment Protocol

6.1 Introduction

In this chapter we discuss key-establishment in Quantum Computational Timelock (QCT) security model. The newly proposed key-establishment protocol is called as "**MUB-QCT**", where we use Mutually Unbiased Bases as the important ingredient to construct the key-distribution protocol.

We first present a general structure of constructing a cryptographic construction in the QCT security model in the Section 6.2. We also discuss the eavesdropping model in the QCT security model and define the security parameters to prove the security of a key distribution in the QCT security model. In Section 6.3.1 and Section 6.3.2, we describe the explicit MUB-QCT key distribution protocols.

6.2 Key establishment from QCT security model

Using the QCT security model we propose a generic cryptographic construction for key establishment. We refer to Alice and Bob as authorized parties who have access to t_{comp}-secure encryption and Eve as an unauthorized party who does not have access to T-secure encryption.

In a generic key-establishment framework, authorized parties, Alice and Bob, want to exchange a bit(s) $x \in \mathcal{X}$ reliably while guaranteeing that an unauthorized Eve can only learn a negligible amount of information about x. Alice and Bob are assumed to have access to an authenticated classical communication channel or the ability to exchange a small secret in an authenticated way. In this setting, to establish the secure keys, Alice and Bob perform following steps

- **Setting a computational time-lock:** Alice and Bob, that are assumed to have access to the t_{comp}-secure encryption scheme $(\mathrm{Enc}; \mathrm{Dec})$, use it to time-lock the classical secret $s \in \mathcal{S}$
- **Quantum communication:** The second step consists of an encrypted quantum communication phase, where Alice encodes the random bit x using the secret s as

$$|\psi_x^s\rangle = U_s|x\rangle \tag{6.1}$$

and sends the state to Bob via an insecure quantum channel. Bob performs the projective measurement on the quantum state $|\psi_x^s\rangle$, using s, and obtains $y \in \mathcal{Y}$, which with high probability reconciles with x, as shown in Fig (6.1a).

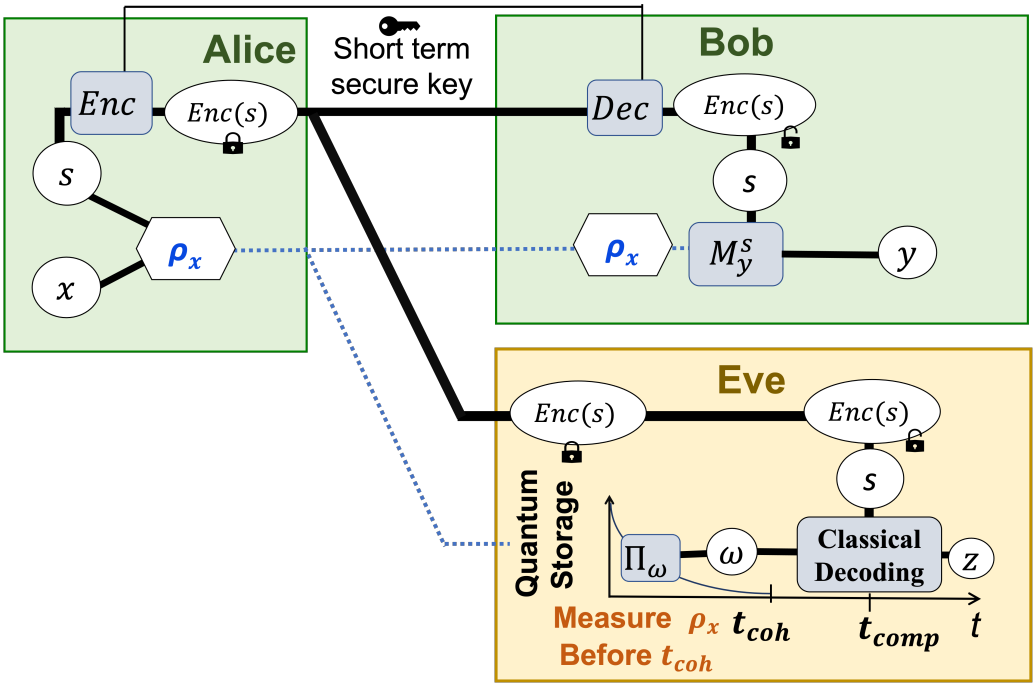


Figure 6.1: A general protocol describing QCT construction in QCT security model. Protocol is defined between authorized parties Alice and Bob, and an unauthorized party Eve. Alice encodes the classical message x on a quantum state ρ_x, using the secret s, and send it over the quantum channel. Objective for both Bob and Eve is to guess x given ρ_x and $\mathrm{Enc}(s)$. Bob measure it immediately using the measurement operator M_y^s, obtaining the outcome y. However, assumptions of QCT security model forces Eve to measure the quantum state ρ_x before t_{coh} using the POVM Π_ω to obtain classical outcome ω and perform post-measurement classical decoding at time $t \geq t_{comp}$ to guess z.

6.2.1 Key establishment protocol in QCT security model

We now consider a simple protocol describing a key establishment in the QCT security model. The protocol is defined for a single quantum channel use as,

Protocol 1 Quantum Computational Time-lock Key Establishment

Input: Alice: $(\mathrm{Enc}, \mathrm{Dec}, x \in \mathcal{X}, s \in \mathcal{S})$, **Bob:** $(\mathrm{Enc}, \mathrm{Dec}, s, |\psi_x^s\rangle)$, **Eve:** $(\mathrm{Enc}, \mathrm{Dec}, \rho_x)$.
Output: Alice: $x \in \mathcal{X}$, **Bob:** $y \in \mathcal{Y}$, **Eve:** $z \in \mathcal{Z}$

- **Alice:**
  1. *Input: bit* $x \in \mathcal{X}$, *a secret* $s \in \mathcal{S}$.
  2. *Set a computational time-lock* $\mathrm{Enc}(s)$ *and sends it to Bob.*
  3. *Encodes the bit* x *on a* d*-dimensional quantum state as* $\rho_{xs} = |\psi_x^s\rangle\langle\psi_x^s|$, *using the secret* s, *and sends it to Bob.*
- **Bob:**
  1. *Decrypts* $\mathrm{Enc}(s)$ *using* Dec, *to obtain* s.
  2. *Performs projective measurement on* ρ_{xs} *using* s, *and outputs a bit* $y \in \mathcal{Y}$.

6.2.2 Eavesdropping model: reduction to wiretap channel setting

In the QCT construction, authorized parties, Alice and Bob, are connected via a authentic classical channel and an insecure quantum channel. As mentioned before, Alice and Bob use the computational assumptions to exchange the key for the authentication of classical 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.

As a consequence of this setting, Alice and Bob have access to a realization of correlated classical random variables X and Y, respectively, whereas an adversary, Eve, obtains a random variable Z. Moreover, Eve has no information about X and Y other than through her knowledge of Z. Under this setting, Alice and Bob can distill a secret key from their shared correlation by performing classical post-processing using a suitable universal$_2$ hasg function [CW79a, BBCM95a]. With this setting for Eve's channel, we are in a similar set-up as strong data locking [LL15b], whereas an adversary Eve receives direct inputs from Alice.

However, for an unauthorized adversary Eve, the classical secret s is time-locked until time t_{comp}. The input state received by the Eve is

$$\rho_x = \frac{1}{|s|} \sum_s \rho_{xs}. \tag{6.2}$$

As a worst-case scenario, Eve can mount her attack using a copy of the input state ρ_x. However, she cannot store quantum information during time longer that $t_{coh} < t_{comp}$ and hence must measure state without knowing s as depicted in Figure 6.1(b). Her measurement Π_ω on ρ_x gives classical outcome ω. Later at time t_{comp}, when the time-locked encryption

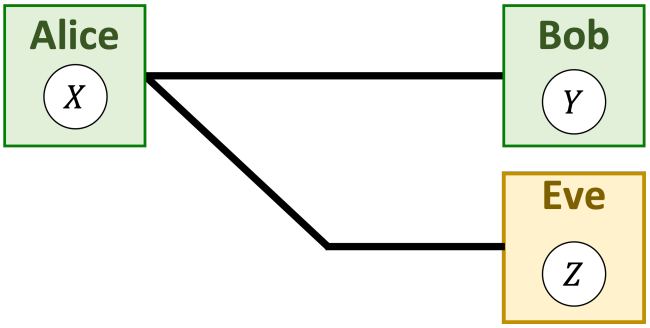


Figure 6.2: Reduction to wiretap channel setting: Eve has full access to the classical and quantum channel, and as at the end of the MUB-QCT protocol Alice and Bob hold classical random variables X and Y, while Eve holds a classical random variable Z. Moreover, Eve has no knowledge of the random variable X other than her knowledge of Z, thus, following I. Csiszár, J. Körner [CK78a] the setting reduces that of a classical wiretap channel. As a result, a positive key rate can be obtained as $R \geq I(X;Y) - I(X;Z)$

6.3 MUB-QCT protocol

In this section we study key agreement protocol that we called **MUB-Quantum Computational Timelock** (MUB-QCT), where a classical bit x is encoded on a d-dimensional quantum state (qudit). The protocol leverages the QCT security model to transmit an ephemeral secret S between Alice and Bob. This secret S is then used to unitarily randomize the qudit state (twirling operation) using a full set mutually unbiased bases (MUBs).

Notations: We make use of the following notation: for an integer d, we denote a set of d elements $\{0, \ldots, d-1\}$ as $[d]$. Any random variable is denoted by a capital letter, for example X, with probability distribution P_X over a finite alphabet $\mathcal{X}$. The realization of X is denoted by the lower-case letters x, for $x \in \mathcal{X}$. We denote vectors in superscript face: for example $x^n := (x_1, \ldots, x_n)$, $x^n \in \mathcal{X}^n$.

Parameters: The m-MUB-QCT-(b, c) key distribution protocol is parametrized by the following parameters

- b : number of bits encoded on a d-dimensional quantum state.
- c : the classical capacity of the encoding.
- m : number of copies of the qudit state sent per channel use.

Ingredients: An essential element of the MUB-QCT protocol will consist in randomizing one of the basis states of a d-dimensional Hilbert space using set of unitaries:

- A complete set of $d+1$ mutually unbiased bases (MUB), in dimension d. We index this set by $\theta \in [d+1]$ and will denote $\{U_\theta\}$ the unitary operations that transforms the computational basis into the different MUB basis indexed by θ.
- A full set of pair-wise independent permutations $\{P_\sigma\}$, $\sigma \in [|\mathcal{P}|]$. A family $\mathcal{P}$ of permutations of a set of d elements $[d]$, is pair-wise independent if for all $i_1 \neq i_2$ and $j_1 \neq j_2$, and for σ chosen uniformly over $\mathcal{P}$ one has, $\Pr\{\sigma(i_1) = j_1, \sigma(i_2) = j_2\} = \frac{1}{d(d-1)}$. The total number of pair-wise independent permutations for a set of d-elements is $|\mathcal{P}| = \frac{\binom{d}{d/2}}{2} \sim 2^{d-1}$ for large d.

Different Protocols: Based on the number of bits encoded on a d-dimensional quantum state and the number of copies of the qudit state sent per channel use, we propose different versions of MUB-QCT protocol.

- In section 6.3.1, we propose 1-MUB-QCT-$(\log d, \log d)$ protocol, where for a single copy of quantum state sent per channel use $\log d$ bits are encoded on a qudit, using a full set of MUBS.
- In section 6.3.2 we propose 1-MUB-QCT-$(1, \log d)$ protocol, where for a single copy of quantum state sent per channel use a bit is encoded on a qudit, using a full set of MUBS and a full set of pair-wise independent permutations.

- In section 6.3.3, we propose MUB-QCT protocol with multiple copies per channel use, namely m-MUB-QCT-$(\log d, \log d)$ and m-MUB-QCT-$(1, \log d)$ protocol.

We consider a noisy and lossless quantum channel setting. However, the generalization to the case of a lossy quantum channel could be addressed relatively simply, by adding a sifting phase,.

6.3.1 1-MUB-QCT-(log d, log d) protocol

Encoding at Alice

- *Setting a computational timelock:* Alice picks θ at random in $[d+1]$. The information $S = \theta$ is sent from Alice to Bob using a short-term-secure encryption scheme. S constitutes a computational timelock, i.e. a classical secret shared between Alice and Bob, but not available to Eve during time at least t_{comp}.

- *Quantum communication* Given an input bit $x \in [d]$, Alice generates the state $U_\theta|x\rangle$ and sends it to Bob

We will denote the state encoded by Alice and inputted on the quantum channel as

$$|\psi_x^\theta\rangle = U_\theta|x\rangle \tag{6.3}$$

Decoding at Bob

Bob's decoding strategy is fixed in order to offer perfect correctness over a ideal quantum channel. It corresponds to the following operations:

- Knowing $S = (\theta)$, Bob unitarily transforms the received state back into the standard basis, by applying $U_\theta)^\dagger$ to his received state

- Bob implements a d-outcome projective measurement in the standard basis, corresponding to POVM $\{M_y\}_{y\in[d]}$ with $M_y = |y\rangle\langle y|$

Bob's global decoding strategy can thus be represented by a d-outcome projective measurement $\{M_y\}^\theta_{y\in[d]}$ with

$$M_y^\theta = \sum_\theta (U_\theta)(|y\rangle\langle y|)(U_\theta)^\dagger) \tag{6.4}$$

Protocol 2 1-MUB-QCT-$(\log d, \log d)$ Protocol

Input: Alice: $(x^n \in [d]^n, \theta^n \in [d+1]^n$
Bob: $(\mathrm{Enc}(\theta^n), \mathrm{Dec}, \rho_{x\theta})$.

Output: Alice: $(S_A = x^\ell \in [d]^l)$,
Bob: $(S_B = y^\ell \in [d]^l)$

The protocol:

1. **Data generation:**

   - *Alice chooses* $x^n \in [d]^n$ *and* $\theta^n \in [d+1]^n$*, uniformly at random.*

2. **Time lock:**

   - *Alice time locks θ^n using a time-lock encryption scheme* Enc*, and sends it to Bob.*
   - *Bob decrypts it immediately using the decryption function* Dec*, to obtain θ^n.*

3. **Quantum communication:**

   - *For ($i = 1; i \leq n; i++$)*
     - *State preparation: Alice prepare a qudit state $\rho_{x\theta} = |\psi_x^\theta\rangle\langle\psi_x^\theta|$, Equation (6.3).*
     - *Distribution: Alice sends the quantum state $\rho_{x\theta}$, to Bob.*
     - *Measurement: Bob measures each quantum state using a POVM, M_y^θ, and outputs the result $y_i \in [d]$.*
   - *After n iterations (channel use) Alice and Bob obtains a string $(x^n; y^n)$*

4. **Parameter estimation:**

   - *Alice chooses a sub-string, of length $\tilde{n} < n$ from x_n and sends to Bob the corresponding positions and values of the string.*
   - *Bob compares this substring to the corresponding one in his output y_n and announces the result.*
   - *Alice and Bob use the result to estimate the error probability np_e (where p_e is the estimated error probability per channel use, as calculated in Appendix B). They abort the protocol if the estimated error exceeds a threshold value ε_{PE} (predefined by Alice and Bob), otherwise they accept the protocol and outputs $(x_{\tilde{n}}; y_{\tilde{n}})$, for $\tilde{n} < n$.*

5. **Information Reconciliation and Privacy Amplification:**

   - *Error correction: To correct the errors, Alice and Bob use an error correcting code [CW79b] that minimizes the leak to the Eve, given the parameters of code and the estimated error ε_{PE}. The error correction outputs error corrected keys $(\hat{x}^{n'}; \hat{y}^{n'})$. Alice and Bob then verify whether their keys are identical, using universal hashing on a small subset of the error-corrected strings. The over all error correction procedure succeeds except with a small probability ε_{EC}.*
   - *Privacy amplification: Finally Alice and Bob uses a privacy amplification protocol based on universal hashing [BBCM95b] to transform the error-corrected keys into the final secret keys $S_A = S_B = S$.*

6.3.2 1-MUB-QCT-(1, log d) protocol

We shall call $A = A_1A_2$ be the d dimensional Hilbert space used in the protocol, with d a power of 2. We also denote $\{|x\rangle\} : x \in \{0, 1\}$ and $\{|r\rangle\} : r \in [d/2]$ the (standard) orthonormal bases of A_1 and A_2 respectively. The encoding vector basis on A is defined as $i_{xr} \equiv \frac{d}{2} \times x + r$ and noted $\{|i_{xr}\rangle\}_{x\in\{0,1\},r\in[d/2]}$.

Encoding at Alice

- *Setting a computational timelock:* In order to construct the cryptographic primitive, Alice picks θ and σ at random in $[d+1] \times [|\mathcal{P}|]$. The information $S = (\theta, \sigma)$ is sent from Alice to Bob using a using a t_{comp}-secure encryption scheme. S constitutes a computational timelock, i.e. a classical secret shared between Alice and Bob, but not available to Eve during time at least t_{comp}.

- *Quantum communication* Given an input bit $x \in \{0,1\}$, Alice generates (locally at random) r in $[d/2]$ and sends the state $P_\sigma U_\theta |i_{xr}\rangle$ to Bob

We will denote the state encoded by Alice and inputted on the quantum channel as

$$|\psi_{i_{x,r}}^{\theta,\sigma}\rangle = P_\sigma U_\theta |i_{x,r}\rangle \tag{6.5}$$

Decoding at Bob

Bob's decoding strategy is fixed in order to offer perfect correctness over a ideal quantum channel. It corresponds to the following operations:

- Knowing $S = (\theta, \sigma)$, Bob unitarily transforms the received state back into the standard basis, by applying $(P_\sigma U_\theta)^\dagger$ to his received state

- Bob implements a two-outcome projective measurement in the standard basis, corresponding to POVM $\{M_y\}_{y=0,1}$ with $M_y = \sum_{r=1}^{d/2} |i_{y,r}\rangle\langle i_{y,r}|$

Bob's global decoding strategy can thus be represented by a two-outcome projective measurement $\{M_y\}_{y=0,1}^{\theta\sigma}$ with

$$M_y^{\theta\sigma} = \sum_{\theta,\sigma} (P_\sigma U_\theta)(\sum_{r=1}^{d/2} |i_{y,r}\rangle\langle i_{y,r}|)(P_\sigma U_\theta)^\dagger) \tag{6.6}$$

Protocol 3 1-MUB-QCT (1,$\log d$) Protocol

Input: Alice: $(x \in \{0,1\}^n, \theta \in [d+1]^n, \sigma \in [|\mathcal{P}|]^n,$
$r \in [d/2]^n)$, **Bob:** $(\mathrm{Enc}(\theta^n, \sigma^n), \mathrm{Dec}, \rho_x)$.

Output: Alice: $x^\ell \in \{0,1\}^\ell$, **Bob:** $y^\ell \in \{0,1\}^\ell$.

The protocol:

1. **Data generation:** *Alice chooses* $(x^n, \theta^n, \sigma^n, r^n)$, *uniformly at random in* $\{0,1\}^n \times [d+1]^n \times [|\mathcal{P}| \times [d/2]^n$

2. **Timelock:** *Alice and Bob exchange timelocked information* (θ^n, σ^n) *using short-term secure encryption scheme* $(\mathrm{Enc}, \mathrm{Dec})$.

3. **Quantum communication:** *For* $(k = 1;\ k \leq n;\ k++)$

   - *Encode and send* x *over a qudit: Alice sends a single copy of the qudit state* $|\psi_{x_k,r_k}^{\theta,\sigma}\rangle$ *to Bob over the quantum channel.*

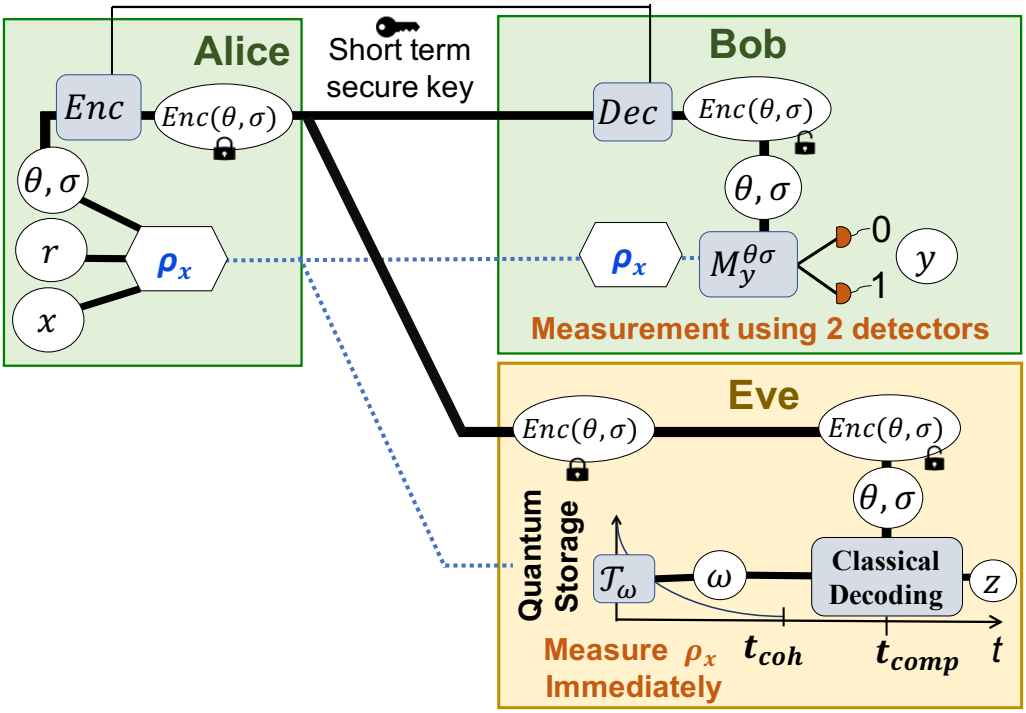


Figure 6.3: A general overview of MUB-QCT protocol. Communication between authorized Alice and Bob (in green). Technologically limited Eve (in yellow) cannot break timelocked encryption before t_{comp} and can only store quantum state in quantum memory during time $t_{coh} < t_{comp}$. As a result, forcing Eve to measure ρ_x immediately. At a later at time, after t_{comp}, time-locked encryption elapses, and Eve learns (θ, σ) and performs classical decoding to obtain z.

- *Receive qudit and decode y: Upon reception of the qudit state at the quantum channel output and knowing (θ_k, σ_k) Bob performs the measurement $\{M_y\}^{\theta_k \sigma_k}$ and obtains outcome y_k.*

4. **Classical post-processing:**

- *Parameter estimation: Based on a random sampling of (x^n, y^n) Alice and Bob estimate the bit error rate $n.p_e$ (Where, p_e is the error rate per channel use). If $n.p_e$ is below some set threshold ε_{th}, they abort.*
- *Finally Alice and Bob run an error correction algorithm followed by privacy amplification (PA) to obtain the final keys $(S_A; S_B)$, of length ℓ.*

6.3.3 MUB-QCT with multiple quantum state copies

In this section, we explore the MUB-QCT protocol with multiple copies of the quantum state per channel use. The motivation is to explore if the MUB-QCT protocol offers high tolerance to the channel loss incurred at long-distance by transmitting multiple photons per channel use i.e., more than one copy of quantum state per channel use.

We propose MUB-QCT protocol with multiple copies per channel use, namely m-MUB-QCT-$(\log d, \log d)$ and m-MUB-QCT-$(1, \log d)$ protocols.

m-MUB-QCT-(log d, log d) Protocol

Alice prepares m copies of the qudit state, $|\psi_x^\theta\rangle$, using same basis θ . She send the state $\rho_x^{(m)}$ to Bob over a quantum channel, where,

$$\rho_x^{(m)} = \frac{1}{|\theta|}\sum_\theta \left(|\psi_x^\theta\rangle\langle\psi_x^\theta|\right)^{\otimes m}. = \frac{1}{|\theta|}\sum_\theta \left(U_\theta|i_x\rangle\langle i_x|U_\theta)^\dagger\right)^{\otimes m}. \tag{6.7}$$

Alice and Bob then follow the rest of the protocol as defined in Protocol 2.

m-MUB-QCT-(1, log d) protocol

Alice prepares m copies of the qudit state, $P_\sigma U_\theta|i_{xr}\rangle\langle i_{xr}|(P_\sigma U_\theta)^\dagger$, using same basis θ, permutation σ, and local randomness r. She send the state $\rho_x^{(m)}$ to Bob over a quantum channel, where,

$$\rho_x^{(m)} = \frac{1}{|r||\theta||\sigma|}\sum_{r,\theta,\sigma} \left(P_\sigma U_\theta|i_{xr}\rangle\langle i_{xr}|(P_\sigma U_\theta)^\dagger\right)^{\otimes m}. \tag{6.8}$$

Alice and Bob then follow the rest of the protocol as defined in Protocol 3.

Security against photon number splitting attack

This section presents how, unlike QKD protocol [HIGM95, L00], the MUB-QCT protocol in the QCT security model offers security against the photon number splitting attack (Section 3.2.4). As a result, we can understand why multiple copies per channel use of the same quantum state can be sent in the MUB-QCT protocol.

One way to overcome the channel losses at large distance is by sending multiple copies of single photons per channel use. However, the situation completely changes when sending multiple copies of single photon. For a source to emit multiple copies with identical encodings in a given run of the key distribution protocol, an eavesdropper who employs the photon number splitting (PNS) attack can be a security vulnerability. The essential idea behind the attack is that Eve can perform a quantum non-demolition measurement to determine the number of photons in a run. If the pulse contains more than one photon, then Eve can split off the extra photons and transmit the remaining single photon to Bob. Eve can store these extra photons in a perfect quantum memory until Alice reveals the encoding basis. Eve can then measure her photons in the correct basis and can obtain information of the key without introducing detectable errors. In this way Bob would not be able to detect her presence while she lies in wait for Alice's basis revelation to make sharp measurements of the stolen photons and obtain perfect information of the multi-photon runs.

In order to protect against a PNS attack and maximize both the key generation rates and the possible distance over which QKD can be used, '*decoy states*' (Section 3.2.4) have been introduced. The decoy states are weak coherent pulses with different mean number of photons. Since Eve cannot distinguish between decoy pulses and real QKD pulses, she attacks all pulses; Alice and Bob can then identify a PNS attack by comparing the gain and quantum bit error rate (QBER) for the different decoy states. However, the maximum achievable key rate for QKD with decoy state is limited to η/e, which is even less than single photon QKD:BB84 .

We derive our motivation from this limitation and aim to construct the MUB-QCT protocol, which embraces sending multiple copies of a single-photon, in the QCT security model (Chapter 5). In this situation, the security of any key distribution protocol against PNS attack follows intrinsically

from the QCT security model: If an adversary Eve chooses to store the extra photons in her quantum storage, then she cannot store them for the time more than t_{coh}. At the time t_{comp}, encoding basis information is revealed for Eve to measure her stored quantum states. However, according to the QCT security model $t_{coh} < t_{comp}$ i.e., quantum storage decoheres before the basis information is revealed. Moreover, as proved in Section 7.2.1 the optimal measurement for the Eve is to measure the quantum state immediately upon receiving instead of storing the state in the quantum storage and measure at t_{comp}. Thus, it is impossible to implement a successful PNS attack in the QCT security model. Implying multiple copies with identical encoding can be sent in the MUB-QCT protocol.

Chapter 7

Security of MUB-QCT protocol

In this chapter we present the security of the MUB-QCT protocols. The security of the protocols is proved by demonstrating that under the QCT assumptions, the optimal attack strategy for non-authorized party Eve consists in an immediate measurement followed by classical post-processing on measurement data. This strategy is known as state discrimination with post measurement information as described in [GW10]. For this state discrimination problem, we determine the maximum success probability or the guessing probability for Eve to retrieve the key, to calculate a bound on Eve's information.

7.1 Security definition

The security of the MUB-QCT protocol is offered by the QCT security model effects, and requires to prove two things: *correctness* and *secretness*.

- The protocol is correct if Alice and Bob's output bits differs with negligible probability.

As described in Section 6.2.2, at the end of the MUB-QCT primitive, Eve learns a classical random variable Z. She does not know the random variable X, other than her knowledge of Z. This setting is similar to the one for classical secret key agreement by a public discussion on a broadcasting channel [Mau93a]. Eve's input channel can then be considered a wiretap channel, where wire-tapper Eve's received message is direct input from Alice's source and is thus not necessarily a degraded version of the message. Moreover, if Eve's mutual information $I(X;Z)$ is less than Alice and Bob's mutual information $I(X;Y)$ [CK78a], then the security of such a setting is guaranteed.

- To complete the secrecy proof of QCT construction, the principle idea is to bind Eve's mutual information $I(X;Z)$ and to show that $I(X;Z) < I(X;Y)$.

It hence differs QKD, where Eve has access to a perfect quantum memory and security definition uses trace distance.

Following the security definition 2.6.5, for the key agreement from a correlated classical data, as defined in the Section 2.6.3, the over all security criterion of the MUB-QCT protocol is defined as

Definition 7.1.1 (Security definition) *A cryptographic protocol for key distribution in the QCT security model is secure if it satisfies following properties:*

1. **Correctness:** *The protocol is ε_{cor}-correct if, for S_A, S_B, and $\varepsilon_{cor} > 0$,*

$$Pr[X \neq Y] \leq \varepsilon_{cor} \tag{7.1}$$

2. **Secrecy:** *The protocol is ε_{sec}-secret if for $\varepsilon_{sec} > 0$*

$$I(X;Z) \leq \varepsilon_{sec} \tag{7.2}$$

7.2 Security of 1-MUB-QCT-(log d, log d) protocol

Recall from section 6.3.1, in the 1-MUB-QCT-(log d, log d) protocol, to generate a secure key with Bob, Alice encodes $\log d$ bits on a d-dimensional quantum system using a full set of $(d+1)$ Mutually Unbiased Bases (Definition 1.33). She chooses a mutually unbiased base U_θ for $\theta \in [d+1]$ from a full set of $d+1$ MUBs. Using a short-term secure encryption scheme she exchange $\mathrm{Enc}(\theta)$ with Bob. She then encodes $\log d$ bits i.e., $x \in [d]$ onto a d-dimensional qudit as

$$\rho_x = \frac{1}{|\theta|} \sum_{\theta} U_\theta |x\rangle\langle x| U_\theta^\dagger \tag{7.3}$$

Alice sends this state to Bob, who on receiving this state performs a measurement using operators M_y^θ defined by the time-locked information θ as

$$M_y^\theta = \sum_i U_\theta |y\rangle\langle y| U_\theta^\dagger \tag{7.4}$$

and obtains an outcome $y \in [d]$.

7.2.1 Optimal attack strategy for Eve

For an unauthorized Eve, the secret θ is time-locked until t_{comp}, while her quantum storage fully decoheres within $t_{coh} < t_{comp}$. Thus on receiving the state ρ_x Eve could perform following strategies:

I Eve performs an immediate measurement at time $t = 0$, using a POVM Π_ω, obtain a classical outcome ω. At t_{comp} when time-lock encryption elapses, she obtains the secret θ and perform post-measurement classical decoding using θ and ω to obtain $z \in \mathcal{Z}$.

II Eve stores the quantum state ρ_x in her quantum storage and wait for time-locked encryption to elapse. At t_{comp}, when she receives the secret θ, she decodes the key bit by performing the measurement on $\mathcal{N}_{t_{comp}}(\rho_x)$ using the secret θ to obtain $z \in \mathcal{Z}$.

Proposition 7.2.1 *In MUB-QCT, under the assumptions of the QCT security model, the optimal attack strategy of an adversary Eve is to perform immediate measurement on all incoming quantum states followed by post-measurement decoding.*

Proof: If Eve follows strategy I, and opts to measure the state $\mathcal{N}_{t_{comp}}(\rho_x)$ at t_{comp}, then following the assumption of the QCT security model the quantum state left in her memory at time t_{comp} is

$$\frac{1}{2}\left|\left|\mathcal{N}_{t_{coh}}(\rho_x) - \frac{\mathbb{I}_d}{d}\right|\right|_1 \leq o\left(\frac{1}{d}\right) \tag{7.5}$$

As a result following [Ren08], the best success probability to guess the value of $x \in [d]$ correctly follows as

$$P_{\mathrm{I}} \leq \frac{1}{d} + o\left(\frac{1}{d}\right) \tag{7.6}$$

However, If Eve chooses to follow the strategy II, then the optimal immediate measurement strategy followed by a post-measurement decoding for Eve is the "state discrimination with post-measurement information" as described in [GW10]. For this strategy the best measurement corresponds to a POVM $(\hat{\Pi}_\Omega)$, with $|\mathcal{X}|^{|\theta|}$ outcomes, each labeled by the $|\theta|$ long binary strings $\Omega = \omega_0, \ldots, \omega_{|\theta|}$, for $\omega_\theta \in \mathcal{X} = [d]$. Such that, when the time-locked encryption elapses and the information about the pair θ is revealed, Eve applies the following map f_θ on the string Ω, which corresponds to an output $z = f_\theta(\Omega)$ i.e., the assignment is done by selecting the value ω_θ corresponding to θ. Finally, Eve guesses the value of x from the output z. Following Equation (1.52), is calculated as

$$\begin{aligned}
P_{guess} &= \max_{\hat{\Pi}_\Omega} \frac{1}{|x||\theta|} \sum_{\Omega} \mathsf{Tr}\left(\hat{\Pi}_\Omega \sum_{\theta} \rho_{\omega_\theta \theta}\right) \quad \text{Where,} \quad \rho_{\omega_\theta\theta} = |e^\theta_{\omega_\theta}\rangle\langle e^\theta_{\omega_\theta}| \\
&= \max_{\hat{\Pi}_\Omega} \frac{1}{|x||\theta|} \sum_{\Omega} \mathsf{Tr}\left(\hat{\Pi}_\Omega \mathcal{F}(\Omega)\right) \quad \text{Where,} \quad \mathcal{F}(\Omega) = \sum_{\theta} \rho_{\omega_\theta\theta} \\
&\leq \max_{\hat{\Pi}_\Omega} \frac{1}{|x||\theta|} \sum_{\Omega} \lambda_\Omega \mathsf{Tr}\left(\hat{\Pi}_\Omega\right) \\
&\leq \frac{\lambda}{|x||\theta|} \max_{\hat{\Pi}_\Omega} \sum_{\Omega} \mathsf{Tr}\left(\hat{\Pi}_\Omega\right) = \frac{d\lambda}{|x||\theta|} = \frac{\lambda}{d+1}.
\end{aligned} \tag{7.7}$$

Where, λ_Ω is the maximum eigenvalue of $\mathcal{F}(\Omega)$ and λ is the maximum of all $\{\lambda_\Omega\}$ for an ensemble of $\{\mathcal{F}(\Omega)\}$. The last two inequalities follow from [Proposition 2, [CHT18]]. Now the calculation for guessing probability is translated to the problem of finding the maximum eigenvalue λ.

We calculate the maximum eigenvalue λ using different methods:

- **Numerical simulation**

We first calculated the P_{guess} numerically using an SDP calculation in MATLAB. We obtain following value of P_{guess} for different values of d, as shown in Table [7.1].

Plotting P_{guess} as a function for d, from Equation (8.13) and Table 7.1, in Figure 7.1, shows that our numerical calculations matches the analytic result and for large value of d, $P_{guess} \propto \mathcal{O}\left(\frac{1}{\sqrt{d}}\right)$.

- **By calculating the λ analytically**

d	P_{guess}
2	0.789
3	0.65
4	0.57
5	0.53
8	0.39
16	0.27

Table 7.1: P_{guess} for different values of d as calculated numerically by SDP

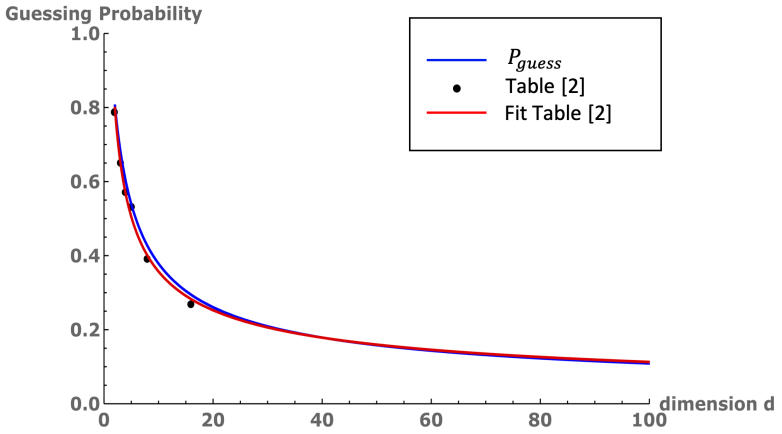


Figure 7.1: Plot of P_{guess} as a function for d for from Equation (7.19) and Table [7.1]. The fitted curve satisfies $P_{guess} = \frac{1.129}{\sqrt{d}}$. This shows that our numerical calculations match the analytic result and for large value of d $P_{guess} \propto \mathcal{O}\left(\frac{1}{\sqrt{d}}\right)$.

Assuming that the λ corresponds to $\Omega = \{0, \ldots, 0\}$. This implies that the problem of finding λ corresponds to finding the maximum eigenvalue λ_{max} of the state $\mathcal{F}(\{0, \ldots, 0\})$,

$$\lambda \geq \lambda_{max}(\mathcal{F}(\{0, \ldots, 0\})) \tag{7.8}$$

It is interesting to observe that the operator $\mathcal{F}(\{0, \ldots, 0\})$ leaves the linear space $\mathcal{H}_0 = \text{span}(\{\theta_0\}|\theta \in [d+1])$ invariant i.e., for each vector α in $\mathcal{H}_0$, $\mathcal{F}\alpha \in \mathcal{H}_0$. Here, $\mathcal{H}_0$ is a $d+1$ dimensional vector space with $d+1$ non-orthogonal basis $(\{\theta_0\}|\theta \in [d+1])$. Let $\mathcal{A}$ be a restriction of $\mathcal{F}(\{0, \ldots, 0\})$ onto the space $\mathcal{H}_0$ i.e., $\mathcal{A}$ is a $d+1$ dimensional matrix which linearly transform $\mathcal{F}(\{0, \ldots, 0\})$ with respect to the non-orthogonal basis $(\{\theta_0\}|\theta \in [d+1])$. Let $\{\alpha_1, \ldots, \alpha_{d+1}\} = (\{\theta_0\}|\theta \in [d+1])$, then

$$\mathcal{F}_{\alpha_j} = \sum_{i=1}^{d+1} A_{ij}\alpha_i \tag{7.9}$$

These equations can be written in the equivalent form as

$$\sum_{j=1}^{d+1} (\delta_{ij}\mathcal{F} - A_{ji}I)\alpha_j = 0 \tag{7.10}$$

Let $Z_{ij} = \delta_{ij}\mathcal{F} - A_{ji}I$, then

$$\sum_{j=1}^{d+1} Z_{ij}\alpha_j = 0 \tag{7.11}$$

This equation translates to

$$\begin{bmatrix} \mathcal{F}-A_{11}I & -A_{12}I & -A_{13}I & \dots & -A_{1r}I \\ -A_{21}I & \mathcal{F}-A_{11}I & -A_{23}I & \dots & -A_{2r}I \\ -A_{31}I & -A_{32}I & \mathcal{F}-A_{33}I & \dots & -A_{2r}I \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -A_{r1}I & -A_{r2}I & -A_{r3}I & \dots & \mathcal{F}-A_{rr}I \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \vdots \\ \alpha_r \end{bmatrix} = 0 \tag{7.12}$$

Solving this for $\mathcal{F}(\{0,\dots,0\})$ we can find

$$\mathcal{A} = \begin{pmatrix} 1 & \frac{1}{\sqrt{d}} & \dots & \frac{1}{\sqrt{d}} \\ \frac{1}{\sqrt{d}} & 1 & \dots & \frac{1}{\sqrt{d}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{\sqrt{d}} & \frac{1}{\sqrt{d}} & \dots & 1 \end{pmatrix} \tag{7.13}$$

Now using the fact that the maximum eigenvalue is invariant under the change of the basis, the λ corresponds to the maximum eigenvalue λ_{max} of matirx $\mathcal{A}$ and is calculated as

$$\lambda = 1 + \sqrt{d} \tag{7.14}$$

Finally, the upper bound on the guessing probability is

$$P_{guess} \leq \frac{1+\sqrt{d}}{d+1} \tag{7.15}$$

- **By bounding sum of l rank one projectors**

To calculate λ, we use the the fact that for any matrix A, its maximum eigenvalue γ is always less than or equal to any matrix norm $|\gamma| \leq ||A||$ [HLW+15]. We consider the infinite matrix norm for our calculations. Following which,

$$\lambda \leq ||\mathcal{F}(\Omega)||_\infty \tag{7.16}$$

As a result, to calculate the maximum eigenvalue λ, it is now required to calculate the sum of the norm of $(d+1)$ projectors. For this we use following theorem

Lemma 7.2.1 *Following inequality holds for the sum of l rank-1 projectors acting on an arbitrary finite dimensional Hilbert space $\mathbb{C}^d$*

$$\begin{aligned} ||\gamma_1 + \dots + \gamma_l||_\infty &\leq 1 + (l-1)\cos\phi \\ \cos\phi &= \max_{i,j>1} ||\gamma_i\gamma_j|| \end{aligned} \tag{7.17}$$

Proof: See Appendix A. □

In our case we have, $\gamma_i = |e^{\theta}_{\omega_\theta}\rangle\langle e^{\theta}_{\omega_\theta}|$, $l = (d+1)$ and $\cos\phi = \frac{1}{\sqrt{d}}$, as $|\langle e^{\theta_1}_i | e^{\theta_2}_j\rangle| = 1/\sqrt{d}$. Following which we have

$$\lambda \leq \Big|\Big|\mathcal{F}(\Omega)\Big|\Big|_\infty \leq 1 + \sqrt{d} \tag{7.18}$$

As a result,

$$P_{guess} \leq \frac{1+\sqrt{d}}{d+1} \tag{7.19}$$

Consequently strategy II. is the optimal eavesdropping strategy. □

7.2.2 Security analysis

Following the security definition 7.1.1 of a cryptographic protocol in QCT security model, to prove the security of MUB-QCT protocol we need to prove two things namely correctness and the secretness. As a result we have following lemmas proving the security of the protocol

Correctness

For a single channel use, In order to decode $\log d$-bits of information, Bob performs a measurement in the basis θ, described by a POVM M^{θ}_y, Equation (7.4). His measurement apparatus consists of d detectors, such that a click in each corresponds to one of the d -bit. Now, let, $p_c = (1-p_e)$ be the probability that there is a correct detection given that there is a click in detector, and let, p_e be the probability that there is a wrong detection given that there is a click in detector. Then, assuming that the correct detection, if there is a click p_c, occurs in one detector and error in detection p_e is uniformly distributed over $d-1$ detectors, we have

$$H(X|Y) = h_d(p_e) = -(1-p_e)\log(1-p_e) - p_e \log\left(\frac{p_e}{d-1}\right). \tag{7.20}$$

For n-channel use, the total probability for error detection is then np_e. For a lossy channel, with T the transmittance (defined as $T = 10^{-\alpha L/10}$, $\alpha = 0.2dB/km$), for the detector efficiency η, the visibility of the detection V and p_{dark} the dark-count probability per detector the estimated error probability per channel use p_e is calculated is Appendix B.

Lemma 7.2.1 (MUB-QCT: Correctness) *The MUB-QCT protocol is ε_{PE}-correct.*

Proof: The MUB-QCT protocol outputs different keys $(S_A; S_B)$, if error correction fails to produce identical key bits, which happens if the estimated error probability np_e exceeds the threshold value ε_{PE}. Thus, the MUB-QCT protocol is ε_{PE}-correct.

□

Secretness

Lemma 7.2.2 (MUB-QCT: Secrecy) *For an optimal immediate measurement that Eve performs on the input state ρ_x, the MUB-QCT is secret with*

$$I(X;Z) \leq \varepsilon_{sec} \tag{7.21}$$

where, $\varepsilon_{sec} = \log_2 d + \log_2\left(\frac{\sqrt{d}+1}{d+1}\right)$.

Proof: To insure the secrecy of the MUB-QCT protocol, a security criterion is to bound on the mutual information of Eve

$$\begin{aligned} I(X;Z) &= H(X) - H(X|Z) \\ &\leq H(X) - H_{min}(X|Z) \end{aligned} \tag{7.22}$$

where, we have used the fact that $H(X|Z) \geq H_{min}(X|Z)$ where $H_{\min}(X|Z)$ is the min entropy defined as

$$H_{\min}(X|Z) = -\log_2 \Big(P_{guess}(X|Z) \Big) \tag{7.23}$$

Thus following Equation 7.19

$$I(X;Z) \leq H(X) - H_{min}(X|Z) = \log_2 d + \log_2 \Big(\frac{\sqrt{d}+1}{d+1} \Big) \tag{7.24}$$

□

Very notably, the bound on Eve information can be achieved under QCT security model, by only considering the input state and not Bob measurement's results.

7.3 Security of 1-MUB-QCT-(1, log d) protocol

7.3.1 Preliminaries: Randomness Extractor

Randomness is an essential resource for information theory, cryptography, and computation. However, most sources of randomness exhibit only weak forms of unpredictability. The goal of randomness extraction is to distill (almost) perfect randomness from a weak source of randomness. A general model for weak random sources was given by David Zuckerman [Zuc90, Zuc96b] who suggested to "measure" the amount of randomness a probability distribution contains by its min-entropy where the min-entropy of a distribution X on $\{0,1\}^n$ is defined by $H_{\min}(x) = -\log(P_{guess}(X = x))$. In other words, a distribution has min-entropy at least k if the probability of every element is bounded by 2^{-k}. Intuitively, such a distribution contains k random bits.

Consider the goal of designing an extractor for all distributions X with $H_{\min}(X) \geq n-1$. That is a function $E : \{0,1\}^n \to \{0,1\}$ such that for every distribution X on $\{0,1\}^n$ the distribution $E(X)$ is a random bit. (Note that here we only want to extract a single random bit.) It is easy to see that no such function E exists. This is because every such function E has a bit b such that the set $S = \{x \mid E(x) = b\}$ is of size at least 2^{n-1}. It follows that the distribution X which is uniformly distributed on X has $H_{\min}(X) \geq n-1$ and yet $E(X)$ is fixed to the value b.

Thus, we will need to settle for a weaker concept of the extractor. We will allow the extractor to use an additional input: A "short seed" of truly random bits. We require that for every distribution X with sufficient min-entropy, the extractor's output distribution is (close to) uniform. Naturally, we want the seed to be smaller than the output of the extractor. Extractors were first defined by Nisan and Zuckerman [NZ96].

Definition 7.3.1 (ϵ-close) *Let X and Y be random variables defined on the same sample space $\mathcal{S}$ with probability distributions p_X and p_Y, respectively. X and Y are ϵ-close in the trace distance (Definition 1.34) iff*

$$D(X,Y) \leq \epsilon \tag{7.25}$$

Definition 7.3.2 (Extractor) *A (k, ϵ)-extractor is a function*

$$\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m \tag{7.26}$$

such that for every distribution X on $\{0,1\}^n$ with $H_{\min}(X) \geq k$ the distribution $\mathrm{Ext}(X,Y)$ (where Y is uniformly distributed in $\{0,1\}^d$) is ϵ-close to the uniform distribution on $\{0,1\}^m$

The input of an extractor contains two independent sources of randomness: the source and the seed. In some applications, it is required that the extractor's output will be uniform even to someone who gets to know the seed. A way of enforcing such a condition is to demand that even if the seed is concatenated to the output, the resulting distribution is close to uniform.

Definition 7.3.3 (Strong extractor) *A (k, ϵ)-extractor is a function*

$$\mathrm{Ext} : \{0,1\}^n \times \{0,1\}^d \to \{0,1\}^m \tag{7.27}$$

such that for every distribution X on $\{0,1\}^n$ with $H_{\min}(X) \geq k$ the distribution $Y \circ \mathrm{Ext}(X,Y)$[1] *(where Y is uniformly distributed in $\{0,1\}^d$) is ϵ-close to the uniform distribution on $\{0,1\}^m$*

However, this is not quite enough for most applications, and we want an even stronger statement. In particular, imagine that some side information E about X is provided, increasing the guessing probability to $P_{guess}(X|E)$. For example, such side information could come from an earlier application of an extractor to the same source. Thus, a strong statement asks the output to be entirely random even with respect to such side information, i.e., uniform and uncorrelated from E. Classically, it is known that extractors are indeed robust against classical side information [57], yielding a uniform output whenever the min-entropy about X given access to side information E is sufficiently high. Especially with respect to cryptographic applications, we thereby again want extractors that work for any source X of sufficiently high entropy $H_{\min}(X|E)$ without any additional assumptions about the source.

Quantum to quantum randomness extractors

In a classical world, the sources of randomness are described by probability distributions, and the randomness extractors are families of (deterministic) functions taking each possible value of the source to a binary string. To understand the definition of quantum extractors, it is convenient to see a classical extractor as a family of permutations acting on the source's possible values. This family of permutations should satisfy the following property; for any probability distribution on input bit strings with high min-entropy, applying a typical permutation from the family to the input induces an almost uniform probability distribution on a prefix of the output. We define a quantum to quantum extractor in a similar way by allowing the operations performed to be general unitary transformations and the input to the extractor to be quantum.

Constructions for QQ-extractors are well known in quantum information theory due to a notion known as 'decoupling,' which plays a central role in quantum information theory. In general, a map that transforms a state ρ_{AE} into a state that is close to a product state $\sigma_A \otimes \rho_E$ is a decoupling map. Decoupling processes thereby typically take the form of choosing a random unitary from a set $\{U_1, \ldots, U_L\}$ to $A = A_1 A_2$ and tracing out (i.e., ignoring) the system A_2. For certain classes of unitaries such as (almost) unitary 2 -designs, the resulting state $\rho_{A_1 E}$ is close to maximally mixed on A_1 and uncorrelated from E, whenever $H_{\min}(A \mid E)$ is sufficiently large.

[1] The operator $\circ$ is a string concatenation operation corresponding to joining character strings end-to-end.

Definition 7.3.4 (QQ-Extractors) *Let $A = A_1A_2$ with $n = \log|A|$. Define the trace-out map $\mathrm{Tr}_{A_2} : \mathcal{L}(A) \to \mathcal{L}(A_1)$ by $\mathrm{Tr}_{A_2}(.) = \sum_{a_2} \langle a_2|(.)|a_2\rangle$, where $\{|a_2\rangle\}$ is an orthonormal basis of A_2 For $k \in [-n, n]$ and $\varepsilon \in [0, 1], a(k, \varepsilon) - QQ$ -extractor is a set $\{U_1, \ldots, U_L\}$ of unitary transformations on A such that for all states $\rho_{AE} \in \mathcal{S}(AE)$ satisfying $H_{\min}(A \mid E)_\rho \geq k$, we have*

$$\frac{1}{L}\sum_{i=1}^{L}\left\|\mathrm{Tr}_{A_2}\left[U_i\rho_{AE}U_i^\dagger\right] - \frac{\mathbb{I}_{A_1}}{|A_1|}\otimes\rho_E\right\|_1 \leq \varepsilon \tag{7.28}$$

$\log L$ is called the seed size of the QQ -extractor.

have arbitrarily large dimension. The quantity $H_{\min}(A|E)$ measures the uncertainty that an adversary has about the system A. As it is usually impossible to model an adversary's knowledge, abound on the conditional min-entropy is often all one can get. A notable difference with the classical setting is that the conditional min-entropy k can be harmful when the systems A and E are entangled. In fact, in many cryptographic applications, this case is the most interesting.

Quantum to classical randomness extractors

When characterizing the power of a source to supply randomness it is hence a natural question to ask, how much classical randomness we can extract from a quantum system. To tackle this question we here take on the study of quantum-to classical randomness extractors (QC-extractors). A Quantum to classical randomness extractor (QC-extractor) extracts an almost uniform classical randomness from a physical source ρ_{AE}, by performing measurements on the quantum state ρ_A. It is formally defined in [BFW14] as,

Definition 7.3.5 (QC-extractor [BFW14]) *Let $A = A_1A_2$ be a quantum system, $n = \log|A|$. Then, for $k \in [-n, n]$ and $\varepsilon \in [0, 1]$, a (k, ε)-QC-extractor is a set $\{U_1, \ldots, U_L\}$ of unitary transformation such that for all state ρ_{AE} satisfying $H_{min}(A|E) \geq k$, we have*

$$\frac{1}{L}\sum_{j=1}^{L}\left|\left|\hat{\Pi}^j_{A\to X_1}(\rho_{AE}) - \frac{\mathbb{I}_{A_1}}{|A_1|}\otimes\rho_E\right|\right| \leq \varepsilon. \tag{7.29}$$

As opposed to classical-to-classical extractors (CC-extractors) given by functions $\mathrm{Ext}(\cdot, R)$ mapping the outcome of the randomness source to a string K, a QC-extractor is described by projective measurements whose outcomes correspond to a classical string K. That is, a QC-extractor is a set of measurements $\left\{\hat{\Pi}^1_{A\to K}, \ldots, \hat{\Pi}^L_{A\to K}\right\}$, where the random seed R determines the measurement $\mathcal{M}^R_{A\to K}$ that we will perform. The measurement map $\{\hat{\Pi}^j_{A\to X_1}(\rho_{AE})\}$ is a defined as

$$\hat{\Pi}^j_{A\to X_1}(\rho_{AE}) := \mathcal{I}_{A_1\to X_1}\left(\mathcal{T}_{A\to A_1}\left(U_j\rho_{AE}U_j^\dagger\right)\right) \tag{7.30}$$

where, $\mathcal{I}_{A_1\to X_1}$ is a canonical identity map i.e., $\mathcal{I}_{A_1\to X_1}(|i\rangle\langle j|_{A_1}) = |i\rangle\langle j|_{X_1}$ and

$$\mathcal{T}_{A\to A_1}(\cdot) = \sum_{a_1,a_2}\langle a_1a_2|(\cdot)|a_1a_2\rangle|a_1\rangle\langle a_1| \tag{7.31}$$

where, $|a_1\rangle$, $|a_2\rangle$ (standard) orthonormal bases of A_1, A_2 respectively.

The measurement map $\{\hat{\Pi}^j_{A\to X_1}(\rho_A)\}$ consist in choosing a random unitary from a set $\{U_1, \ldots, U_L\}$ applying it on ρ_A and then tracing out the system A_2, i.e., for $A = A_1A_2$ measurements $\hat{\Pi}^j_{A\to X_1}(\rho_A)$ consisting of applying a random unitary U_j on ρ_A, followed by a measurement $\mathcal{T}(\cdot)_{A\to A_1}$ on A_1, thus yields a QC-extractor.

QC-extractors based on full set of MUBs

Definition 7.3.6 (Pair-wise independent permutation) *A family $\mathcal{P}$ of permutations of a set of d elements $[d]$, is pair-wise independent if for all $i_1 \neq i_2$ and $j_1 \neq j_2$, and if σ is uniformly distributed over $\mathcal{P}$,*

$$\Pr\{\sigma(i_1) = j_1, \sigma(i_2) = j_2\} = \frac{1}{d(d-1)}. \tag{7.32}$$

In this paper, permutations of basis elements of a Hilbert space A should be seen as a unitary transformation on A. Total number of pair-wise independent permutations for a set of d-elements are $|\mathcal{P}| = \frac{\binom{d}{d/2}}{2}$, which for a large value of d is approximately equal to 2^{d-1}.

A construction of QC-extractor based on full set of mutually unbiased bases (MUBs) and a set $\mathcal{P}$ of pair-wise independent permutations was provided in [BFW14]. The upper bounds on the maximum amount of randomness that can be extracted then follows from the following [Theorem III.8, [BFW14]]:

Theorem 7.3.7 (QC-extractor based on full set of MUBs) *Let $A = A_1A_2$, $n = \log|A|$, $|A$ a prime power, and let $\mathcal{T}_{A\to A_1}$ be the measurement map as defined in Equation (7.31). Then if $\{U_1, \ldots, U_{|A|+1}\}$ defines a full set of mutually unbiased bases, we have*

$$\frac{1}{|\mathcal{P}|(|A|+1)} \sum_{P_\sigma \in \mathcal{P}} \sum_{\theta=1}^{|A|+1} \left|\left| \hat{\Pi}^{\theta\sigma}_{A\to X_1}(\rho_{AE}) - \frac{\mathbb{I}_{A_1}}{|A_1|} \otimes \rho_E \right|\right| \leq \varepsilon \tag{7.33}$$

for $\varepsilon = \sqrt{\frac{|A_1|}{|A|+1} 2^{-H_{\min}(A|E)}}$, where $\hat{\Pi}^{\theta\sigma}_{A\to X_1}(\rho_{AE}) = \mathcal{T}_{A\to A_1}\left(P_\sigma U_\theta \rho_{AE} (P_\sigma U_\theta)^\dagger\right)$, $\mathcal{P} = \{P_\sigma\}$, is a set of pair-wise independent matrices. In particular, the set $\{P_\sigma U_\theta : P_\sigma \in \mathcal{P}, \theta \in [|A|+1]\}$ defines a (k, ε)-QC-extractor provided

$$\log|A_1| \leq n + k - 2\log(1/\varepsilon) \tag{7.34}$$

and the number of the unitaries is $L = (|A|+1)|\mathcal{P}|$.

Full set of MUBs along with the set of pair wise independent permutations forms a strong QC-randomness extractor i.e., even if the unitaries (U_θ, P_σ) are revealed to an adversary Eve after the measurement $\hat{\Pi}^{\theta\sigma}_{A\to X_1}(\rho_{AE})$ following holds,

$$\left|\left| \rho_{X_1 E U_\theta P_\sigma} - \frac{\mathbb{I}_{A_1}}{|A_1|} \otimes \rho_{E U_\theta P_\sigma} \right|\right| \leq \sqrt{\frac{|A_1|}{|A|+1} 2^{-H_{\min}(A|E)}} \tag{7.35}$$

where

$$\rho_{X_1 E U_\theta P_\sigma} := \left(\frac{1}{|\theta||\sigma|} \sum_{\theta,\sigma} \hat{\Pi}^{\theta\sigma}_{A\to X_1}(\rho_{AE})\right) \otimes |\theta\rangle\langle\theta| \otimes |\sigma\rangle\langle\sigma| \tag{7.36}$$

7.3.2 Reduction of optimal eavesdropping attack strategy to QC-extractor

Optimal attack strategy Due to the QCT security model, Eve strategy is restricted to two alternatives:

I Eve stores the input quantum state ρ_x in her quantum storage and later performs a measurement at time t_{comp} given the information (θ, σ) that will then be revealed to her, and she obtains $z \in \{0, 1\}$.

II Eve performs an immediate measurement on input state ρ_x and obtains a classical outcome ω. At time t_{comp}, she performs post-measurement classical decoding using (θ, σ) and ω to obtain $z \in \{0, 1\}$.

Lemma 7.3.1 *For strategy* I*, the guessing probability to guess the key bit is* $P^{\mathrm{I}}_{guess}(X|E) \leq \frac{1}{2} + o\Big(\frac{1}{d}\Big)$.

Proof: If Eve follows the strategy I, her success probability to guess the bit x correctly can be upper bounded usung tfollowing property that if $\frac{1}{2}\Big|\Big|\mathcal{N}_{t_{coh}}(\rho_x) - \frac{\mathbb{I}_d}{d}\Big|\Big|_1 \leq \epsilon$ then P_{guess} is not larger than $\frac{1}{2} + \epsilon$, as presented in [WWQ+19] and proved in [Ren08]. Given the decoherence model described in Equation (5.2), the guessing probability is then,

$$P^{\mathrm{I}}_{guess}(X|E) \leq \frac{1}{2} + o\Big(\frac{1}{d}\Big). \tag{7.37}$$

□

Lemma 7.3.2 *For strategy* II*, the guessing probability to guess the key bit is* $P^{\mathrm{II}}_{guess}(X|E) \leq \frac{1}{2} + \Omega\Big(\frac{1}{d}\Big)$.

Proof: For strategy II, one simple strategy for Eve is to perform a measurement in a random MUB, followed by post-measurement decoding. For this strategy, Eve can successfully guess the key bit with probability at least

$$P^{\mathrm{II}}_{guess}(X|E) \geq \frac{1}{2} + \mathcal{O}\Big(\frac{1}{d}\Big). \tag{7.38}$$

We now prove that this guessining probability is infact also an upper bound. We considering the measurement in a fixed basis followed by a post-measurment decoding, as Eve has no preferable measurement basis since the full set of MUBs forms 2-design [GKR]). Based on the work of Berta et. al., [BFW14] on Quantum to Classical Randomness Extractors, we can establish that such generic strategy II, reduces to applying a strong QC-extractor to ρ_x.

For the side information E, that Eve can get on X, the optimal immediate measurement is equivalent to the measurement map $\mathcal{T}_{A\to A_1}$ in Equation (7.31). Corresponding to tracing out A_2 (defined by $\{|r\rangle\} : r \in [d/2]$) from the quanum state ρ_A (Equation 2), and then measuring the remaining system A_1 in the (standard) orthonormal basis $\{|\omega\rangle\}$, obtaining a classical outcome $\omega \in \{0, 1\}$. Following which we have

$$\mathcal{T}_\omega(\rho_{xE}) = \mathcal{T}_{A\to A_1}(\rho_{xE}) \tag{7.39}$$

$$= \mathcal{T}_{A\to A_1}\Big(\frac{1}{|\theta||\sigma|}\sum_{\theta\sigma} P_\sigma U_\theta \rho_{AE} (P_\sigma U_\theta)^\dagger\Big) \tag{7.40}$$

$$= \frac{1}{|\theta||\sigma|}\sum_{\theta,\sigma} \hat{\Pi}^{\theta\sigma}_{A\to\omega}(\rho_{AE}) \tag{7.41}$$

Which, following Theorem 7.3.7, corresponds to accessing the output of a strong QC-extractor based on a full set of MUBs [BFW14]. Moreover, a full set of MUBs forms a stromg QC-Extractor i.e., even if the unitaries (U_θ, P_σ) are revealed at t_{comp}, following holds,

$$\left|\left|\rho_{xEU_\theta P_\sigma} - \frac{\mathbb{I}_{A_1}}{|A_1|} \otimes \rho_{EU_\theta P_\sigma}\right|\right| \leq \varepsilon \tag{7.42}$$

where $\rho_{xEU_\theta P_\sigma} := \mathcal{T}_{A\to A_1}(\rho_{xE}) \otimes |\theta\rangle\langle\theta| \otimes |\sigma\rangle\langle\sigma|$, and $\varepsilon = \sqrt{\frac{|A_1|}{|A|+1} 2^{-H_{\min}(A|E)}}$.

We have $|A| = d$, $|A_1| = 2$, and $H_{min}(A|E) \geq \log_2 |A_2| = \log_2 d - 1$. Putting all these value in the expression of ε, we get

$$\varepsilon \leq \frac{2}{\sqrt{d(d+1)}}. \tag{7.43}$$

The success probability to guess the key bit is then

$$P^{\text{II}}_{guess}(X|Z) \leq \frac{1}{2} + \frac{1}{\sqrt{d(d+1)}} \sim \frac{1}{2} + \mathcal{O}\Big(\frac{1}{d}\Big) \tag{7.44}$$

Equation (7.44) proves the matching upper bound for guessing probability as in Equation (7.38). Indicating that measurement in a fixed MUB is essentially the optimal immediate measurement strategy strategy. Following Equation (7.38) and (7.44) we have

$$P^{\text{II}}_{guess}(X|Z) \leq \frac{1}{2} + \Omega\Big(\frac{1}{d}\Big) \tag{7.45}$$

□

Proposition 7.3.1 (Optimal attack strategy) *Strategy II is the optimal attack strategy for Eve to guess the key bit.*

Proof: The proof follows from Lemma 7.3.1 and Lemma 7.3.2. □

7.3.3 Security of the protocol

At the end of the MUB-QCT protocol Alice and Bob hold classical random variables X and Y, while Eve holds a classical random variable Z and decohered quantum memory. Moreover, Eve does not know the random variable X other than her knowledge of Z, thus, following I. Csiszár, J. Körner [CK78a] the MUB-QCT setting reduces to an effective wiretap scenario, as shown in figure (6.2). As a result, a positive key rate can be obtained as

$$R \geq I(X;Y) - I(X;Z), \tag{7.46}$$

which requires to bound Eve's information $I(X;Z)$. Following guessing probability (7.45) Eve's mutual information is bounded as

$$I(X;Z) \sim \Omega\Big(\frac{1}{d}\Big) \tag{7.47}$$

Very notably, the upper bound on Eve information can be achieved by only considering the input state and not Bob measurement's results. For $I(X;Y) = 1 - h_2(p_e)$, this implies a positive key rate can be distilled if the estimated bit error rate $p_e < \frac{1}{2} - \frac{c}{\sqrt{d}}$ for a constant $c > 1$.

After the parameter estimation, Alice and Bob abort the protocol if the estimated error probability per channel use p_e exceeds the threshold error probability per channel use ε_{th}. For a lossy channel, with T the transmittance (defined as $T = 10^{-\alpha L/10}$, $\alpha = 0.2dB/km$), for the detector efficiency η, the visibility of the detection V and p_{dark} the dark-count probability per detector the estimated error probability per channel use p_e can be calculated as (See B for detailed calculation)

$$p_e = \frac{T\eta(1-V) + p_{dark}}{T\eta + 2p_{dark}} \tag{7.48}$$

For single copy of the quantum state sent per channel use the key rates per channel use 7.46 as a function of the distance is plotted in the figure 7.2.

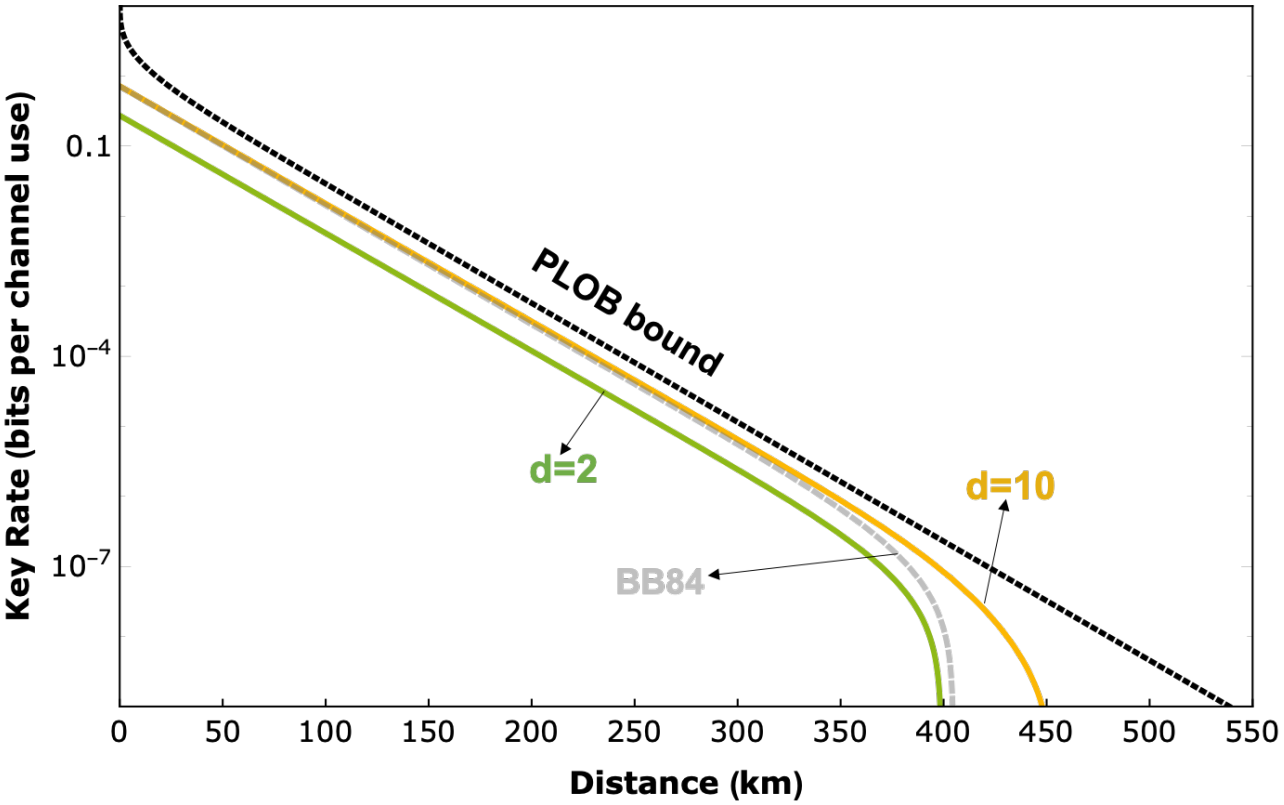


Figure 7.2: Key rate per channel use as a function of distance. The parameters assumed in the plots are: Loss 0.2dB/Km; $P_{dark} = 10^{-6}$; efficiency of detectors $\eta = 25\%$; visibility $V = 98\%$. Since MUB-QCT can be implemented with 2 detection modes (2-single photon detectors) we also plot 2-modes PLOB bound [PLOB17a] as a benchmark..

Chapter 8

Security of MUB-QCT protocol with multiple copies per channel use

The proof for 1-MUB-QCT is valid against general attacks, in the QCT security model, thanks to the reduction of Eve optimal strategy to observing the output of a strong randomness extractor. In the multiple copy case, this proof strategy however does not carry over. In particular, the randomization of a full set of MUBs defines a 2-design that is not sufficient to randomize multiple copies, for $m > 1$.

The 1-MUB-QCT protocol considered the quantum communication of a single qudit state ρ_x from Alice to Bob. In such case we have shown that Eve's information vanishes as $O(1/d)$. This in principle leaves the room to operate secure key establishment, a higher number of copies, i.e. m copies of ρ_x per channel use: this is the m-MUB-QCT protocol.

Interestingly the m-MUB-QCT protocol could open the way to higher key rates and long-distance operation, while keeping implementation simple and using with coherent states with mean photon numbers $\sim m$.

In section 8.1 we first present possible Eavesdropping strategies when Alice sends multiple copies per channel use. These possible Eavesdropping strategies are categorized as *single copy fixed measurement*, *collective measurement* and *adaptive measurement*. We also present a special kind of adaptive measurement called *proactive MUB-measurement* where Eve proactively measures each copy in a different MUB.

8.1 Possible attack strategies for multiple copies per channel use

8.1.1 Individual measurement

In this attack strategy Eve is restricted to perform same individual measurement (which she performs on a single copy), on each of the m-copies of the quantum state. For any locally optimal scheme, the optimization is done by minimizing the error probability of the measurement of only a single copy. Here we consider the case where each measurement is also performed independently, i.e. without any information obtained from the measurement of other copies. The scheme reduces to a simple

binomial decision problem, with probability of error

$$P_{error}^{\text{Fix}}(X|Z)_m = \sum_{i=1}^{\lceil m/2 \rceil} \binom{m}{i} P_{guess}(X|Z)^i (1 - P_{guess}(X|Z))^{m-i} \tag{8.1}$$

8.1.2 Collective measurement

For any number of copies $m \geq 1$, the minimum possible error probability can be obtained in principle by measuring all m copies of the state using a *collective measurement*. This attack strategy corresponds to performing a measurement at once on the collective state of all m-copies [ABB+05].

8.1.3 Adaptive measurement

In the simplest scenario Eve can perform an optimal single-copy measurement on the first copy, use the outcome of the measurement to define the optimal measurement on the next copy, and finally the outcome of the optimal measurement on last copy in the sequence decides the result of the overall measurement [ABB+05].

8.2 Security analysis of m-MUB-QCT against restricted attacks

We can however perform security analysis against restricted attacks, by considering two relaxations:

- *Non-adaptive attacks*. This corresponds to assuming that Eve cannot update her attack strategy adaptively, over the m copies.
- *Individual attacks*. This corresponds to discard the possibility of correlated attacks over different channel use. We conjecture that individual attacks are likely to be the best strategy if the security of the ephemeral encryption is valid throughout the full session (during the n consecutive channel uses).

We consider a specific *non-adaptive attack* strategy, **Proactive MUB measurement,** in which Eve proactively measures each of the m copies in a different MUB, where she obtains a sequence of m classical measurement outcomes $\{a_1, a_2, \ldots, a_m\}$, such that for each $i \in [m]$, $a_i \in [d]$. This is followed by a post-measurement decoding at time t_{comp}, using $(\{a_i\}, \sigma, \theta)$.

8.2.1 Security analysis: m-MUB-QCT-(1, log d) protocol

Proactive MUB Measurement

Eve proactively measures each copy individually in a different bases, chosen from the full set of MUBs. After measuring all the copies, Eve obtains a sequence of m classical measurement outcomes $\{a_1, a_2, \ldots, a_m\}$, such that for each $i \in [m]$, $a_i \in \{0, 1\}$ for the 1 bit case. This is followed by a post-measurement decoding at time t_{comp}, using $(\{a_i\}, \sigma, \theta)$.

For $m \geq d + 1$ a post-measurement decoding strategy, which results in guessing the key bit x with certainty consist of applying P_σ on one of the a_i, for which the measurement was done in the correct basis U_θ.

For $m < d+1$, using the fact that the set of permutation operations commutes with MUB basis change [Ric03], we can reduce to the simpler case without permutation, where Eve measures each copy in a different MUB, and learns the correct it only if her measurement basis coincides with θ. As a result, Eve's mutual information increases linearly with m as

$$I^{\text{Pro}}(X;Z) \sim \mathcal{O}\Big(\frac{m}{d}\Big) \tag{8.2}$$

This implies while performing proactive MUB-measurement, Eve cannot guess x perfectly when significantly less than d copies of the state $|\psi_{x,r}^{\theta,\sigma}\rangle$ are sent by Alice.

Individual attack

We now analyze the case when Alice send m copies of the quantum state per channel use. She prepares m copies of the qudit state, $P_\sigma U_\theta |i_{xr}\rangle\langle i_{xr}| (P_\sigma U_\theta)^\dagger$, using same basis θ and local randomness r. She send the state $\rho_x^{(m)}$ to Bob over a quantum channel, where,

$$\rho_x^{(m)} = \frac{1}{|r||\theta||\sigma|} \sum_{r,\theta} \Big(P_\sigma U_\theta |i_{xr}\rangle\langle i_{xr}| (P_\sigma U_\theta)^\dagger . \Big)^{\otimes m}. \tag{8.3}$$

Eve is restricted to perform the same individual fixed measurement on each of the m copies. As a result, Eve obtains a m-bit long sequence $\{z_i\}$, where, each z_i is equal to x with guessing probability P_{guess} (Equation (7.45)) and differs with $1 - P_{guess}$. An obvious choice for decoding the key bit is to use *majority rule*, according to which the largest number of occurrences of a bit value in the $\{z_i\}$ is the value of input bit.
Let $\{B_i\}$ be an i.i.d. sequence of Bernoulli random variables with parameter $1 - P_{guess}$ i.e., $b_i = 1$ with probability $1 - P_{guess}$ and $b_i = 0$, with probability P_{guess}. Then, we can write $z_i = x \ominus b_i$, i.e., $Z_i = X$ iff $b_i = 0$.

Error in decoding due to majority rule occurs if the number of times the incorrect value of x, in the m-bit long sequence $\{z_i\}$, turnouts to be greater than $\frac{m}{2}$. i.e.,

$$P_{error}^{\text{Fix}}(X|Z)_m = \Pr\Big[\sum_{i=1}^{m} B_i > \frac{m}{2}\Big]. \tag{8.4}$$

Error probability can be bounded using the Chernoff bound [Mou16], according to which if $\{B_i\}$ is a sequence of Bernoulli random variables with parameter p then

$$\Pr\Big[\sum_{i=1}^{m} B_i > mp + t\Big] \geq \frac{1}{2}\Big(1 - \sqrt{1 - \exp\Big(\frac{-2t^2}{mp}\Big)}\Big) \tag{8.5}$$

For $p = 1 - P_{guess}$, $t = m/d$

$$\begin{aligned} P_{error}^{\text{Fix}}(X|Z)_m &\geq \frac{1}{2}\Big(1 - \sqrt{1 - \exp\Big(\frac{-4m}{d^2 - 2d}\Big)}\Big). \\ &\geq \frac{1}{2}\Big(1 - \sqrt{1 - \Big(1 - \frac{4m}{d^2}\Big)}\Big). \\ &\geq \frac{1}{2} - \frac{\sqrt{m}}{d} \end{aligned} \tag{8.6}$$

where we have used the approximation $\exp(-a) \approx 1 - a$ for $a < 1$. As a result

$$P_{guess}^{\text{Fix}}(X|Z)_m \leq \frac{1}{2} + \frac{\sqrt{m}}{d} \tag{8.7}$$

$$I^{\text{Fix}}(X;Z)_m = \mathcal{O}\Big(\frac{\sqrt{m}}{d}\Big) \tag{8.8}$$

Implying that when restricting Eve to perform fixed optimal measurements on each copy, $m \leq \mathcal{O}(d^2)$ copies can be sent, while the accessible information is still negligible.

Analysis

For m-MUB-QCT-$(1, \log d)$ protocol, we found out that the proactive MUB measurement strategy is more efficient than the single copy fixed measurement. It moreover allows secure key distribution with input states containing up to $O(d)$ photons, implying a significant performance increase, characterized by a $O(d)$-multiplication of key rate. As a result, we conjecture that the proactive MUB-measurement attack strategy is the best optimal non-adaptive attack strategy.

8.2.2 Security analysis: m-MUB-QCT-(log d, log d) protocol

Alice prepares m copies of the qudit state, ρ_x, using same basis θ. The m copy state of ρ_x is then defined as

$$\rho_x^{(m)} = \frac{1}{|\theta|} \sum_{\theta} (U_\theta |x\rangle\langle x| U_\theta^\dagger)^{\otimes m}. \tag{8.9}$$

When Eve performs proactive MUB-measurement, as discussed in the section 8.2.1, Eve's mutual information increases linearly with m as

$$I^{\text{Pro}}(X;Z) \sim \mathcal{O}\Big(\frac{m}{d}\Big) \tag{8.10}$$

This implies while performing proactive MUB-measurement, Eve cannot guess x perfectly when significantly less than d copies of the quantum state are sent by Alice.

For individual attack strategy Eve is restricted to perform same individual measurement (which she performs on a single copy), on each of the m-copies of the quantum state. When Alice sends m copies of the quantum state, an adversary wins if she is able to guess at least 1 copy correctly. Let $P(s,m)$, $(s \leq m)$, be the probability of guessing s copies when m copies are provided. Then, the guessing probability for adversary is

$$P_{guess}(m) = P(1,m) + P(2,m) + \ldots + P(m-1,m) + P(m,m) \tag{8.11}$$

Success probability of guessing s copies correctly, when m copies are sent, is described by the Binomial distribution,

$$P(s,m) = \frac{m!}{(m-s)!.s!} (P_{guess})^s (1 - P_{guess})^{m-s} \tag{8.12}$$

Using which $P_{guess}(m)$ is calculated as

$$P_{guess}(m) = 1 - (1 - P_{guess})^m = 1 - \Big(1 - \frac{1+\sqrt{d}}{1+d}\Big)^m \sim \mathcal{O}\Big(\frac{m}{\sqrt{d}}\Big) \tag{8.13}$$

This implies that $m < \mathcal{O}(\sqrt{d})$ copies can be sent, while the guessing probability $P_{guess}(m)$ is still negligible. For example, if $d = 10^6$ then $m < 10^3$ can be sent while still guaranteeing the security of the key.

As a result, for m-MUB-QCT-$(\log, \log d)$ protocol, we found out that the single copy fixed measurement is more efficient than proactive MUB measurement strateg. It moreover allows secure key distribution with input states containing up to $O(\sqrt{d})$ photons. However, the number of detectors required increases with the increase, which can in result decrease the achievable transmission distance due to errors from multiple detectors.

Challenges: Security of the m-MUB-QCT protocol against adaptive attacks.

In the multi-copy case, the security analysis presented so far does not account for general attacks (in particular adaptive strategies), for which we do not know if the proactive MUB measurement is optimal. Thus, the question of the optimal attack in the multiple copy case remains open and a direction for our future work.

Chapter 9

Performance analysis of the MUB-QCT protocol

9.1 Introduction

In this chapter we analyze the performance efficiency of the MUB-QCT protocol. We also discuss the important functionality offered by the MUB-QCT protocol. In chapter 6.3.3 we demonstrated that MUB-QCT enables everlasting secure key distribution with input states containing up to $O(\sqrt{d})$ photons. This leads to a series of important improvements when compared to QKD: on the functional side, the ability to operate securely between one sender and many receivers, whose implementation can moreover be untrusted; significant performance increase, characterized by a $O(\sqrt{d})$ multiplication of key rates and an extension by $25km \times \log(d)$ of the attainable distance over fiber. Implementable with a large number of modes with current or near-term multimode photonics technologies, the MUB-QCT construction has the potential to provide a radical shift to the performance and practicality of quantum key distribution.

9.2 Noise tolerance:

The maximum tolerable error rate (the error threshold for $R = 0$) as a function of d is

$$\varepsilon_{th} \sim 1/2 - \mathcal{O}(1/d) \tag{9.1}$$

i.e., up to 50% for large d. Thus, higher the d higher is the resilience to noise, allowing the lower signal to noise ratio for the received signal, which can be translated into longer transmission distances. High dimensional encoding in the MUB-QCT protocol allows high resilience to noise by offering a maximum tolerable error rate of up to 50% for large d. Key rate per channel use for the MUB-QCT protocol as a function of error rate for different values of d is plotted in Figure 9.1. The figure explains that the maximum tolerable error rate increases as the dimension of the Hilbert space increases.

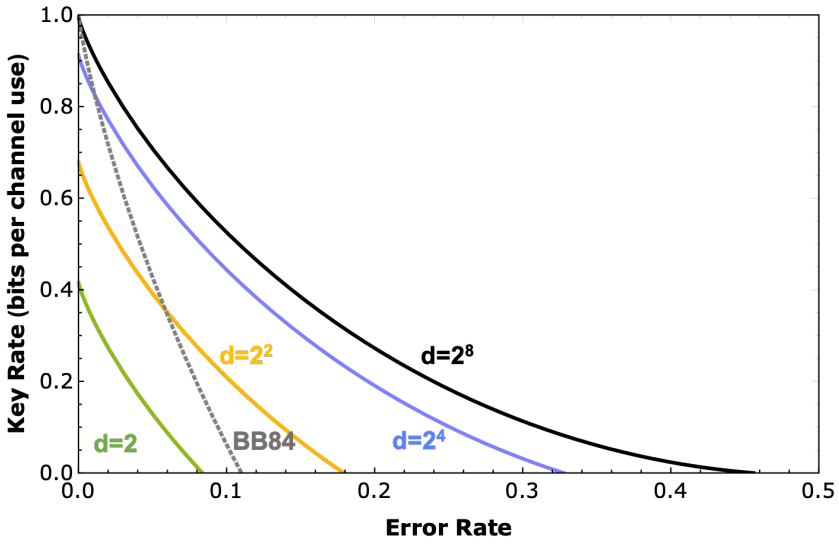


Figure 9.1: Key rate per channel use for the MUB-QCT protocol as a function of error rate for different values of d.

9.3 Resource requirements:

In MUB-QCT, the number of detectors remains constant irrespective of the dimension of the quantum system. MUB-QCT protocol's detectors requirement remains fixed, i.e., two detectors (to distinguish a bit), irrespective of the quantum system's dimension. The MUB-QCT protocol can be implemented with only two detectors, irrespectively of d. As mentioned earlier, the measurement apparatus consists of two detectors, such that a click in each corresponds to one of the bit value i.e., 0 or 1.

This is completely in contrast to the high-dimensional QKD, where, the detectors requirement scales linearly with d. HD-QKD schemes [LPD+13, LBZ+19, LBZ+16a, JPLS19] also offers high tolerance to noise for large d, and the ability to encode $\log_2 d$ bits of information on single photon is an additional advantage. However, the efficient implementation of such schemes requires d-single-photon detectors, financially restricting the use of large d. Thus, the MUB-QCT protocol significantly relaxes the financial dependency, while still allowing to distill secret keys at long distances, as compare to HD-QKD.

Protocol	Information per channel use	Error-tolerance	Number of detectors	Trust assumptions on the hardware
(P&M) HD-QKD	$\log_2 d$ bits	$\leq 50\%$ for large d	d	All devices in Alice and Bob's lab are trusted.
MUB-QCT	1 bit	$\leq 50\%$ for large d	2	Bob's measurement device does not need to be trusted.

Table 9.1: Comparison of the prepare and measure HD-QKD with the MUB-QCT protocol.

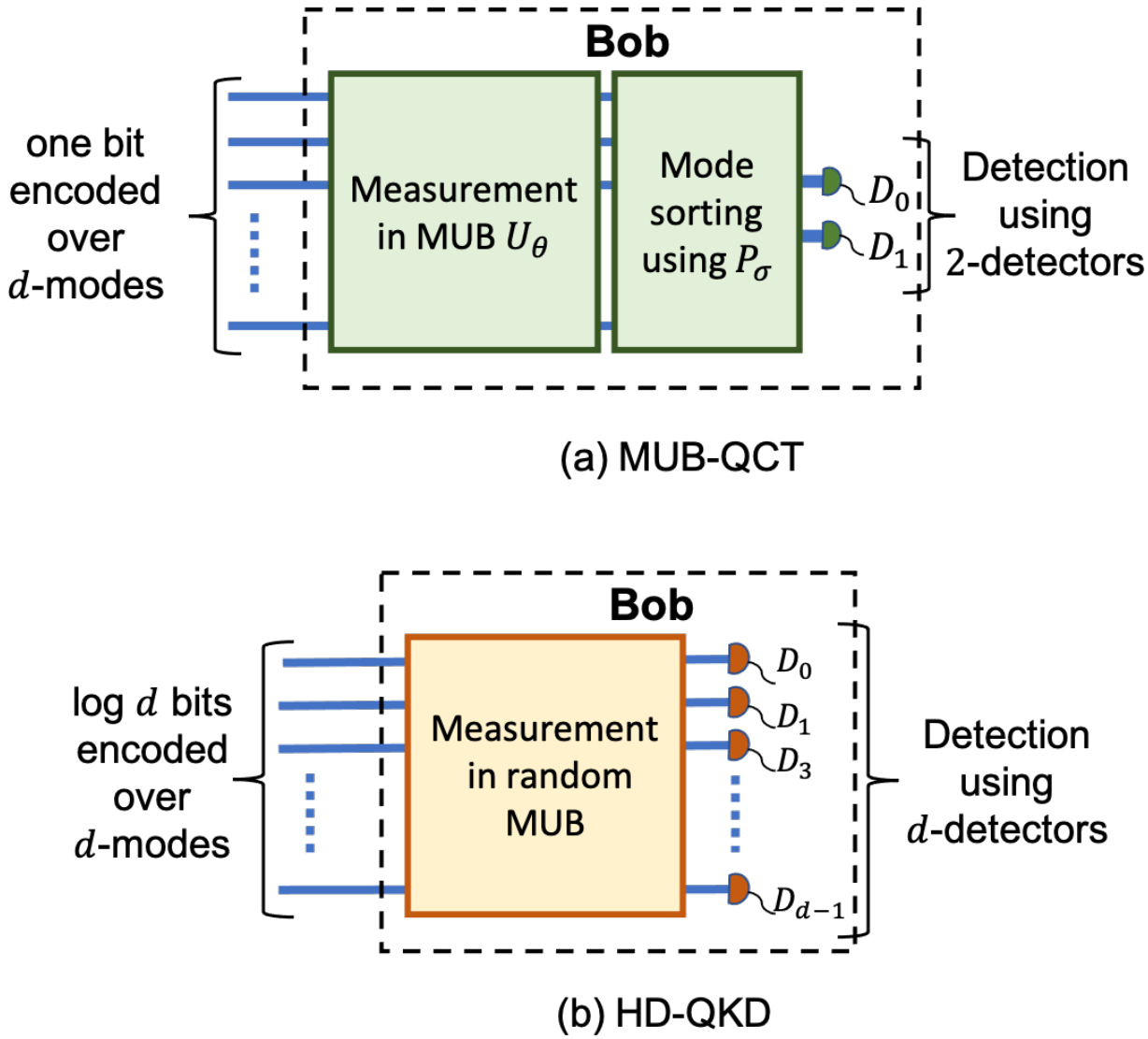


Figure 9.2: (a)The MUB-QCT protocol's detectors requirement remains fixed, i.e., two detectors (to distinguish a bit), irrespective of d. This, significantly relaxes resource requirements compared to (b) HD-QKD schemes [LPD+13, LBZ+16a], which requires d-single-photon detectors.

9.4 Improved rate and reachable distance

9.4.1 m-MUB-QCT-(1, log d) Protocol

In this case when encoding one bit and sending m-copies of the quantum state the secret key rate for a loss channel is defined as

$$\begin{aligned} R &\geq (1-(1-T)^m)H_{min}(X|Z) - H(X|Y) \\ &\geq (1-(1-T)^m)(-\log(P^{\text{Pro}}_{guess}(X|Z)_m)) + p_c \log p_c + p_e \log p_e \end{aligned} \tag{9.2}$$

Analyzing the plot in Figure 9.3, we observe three distinct regimes, *Constant rate regime*: short distance, where the secret key rate is constant and commensurate to those of data communication

rates, as at-least one photons always get clicked in detectors; *Single copy regime*: longer distances, where the key rate is similar to the single copy case, scaling as the transmissivity T, and decays exponentially with distance; *Cutoff regime*: extremely long distances, where detector dark count rates sharply limit the secret key rate.

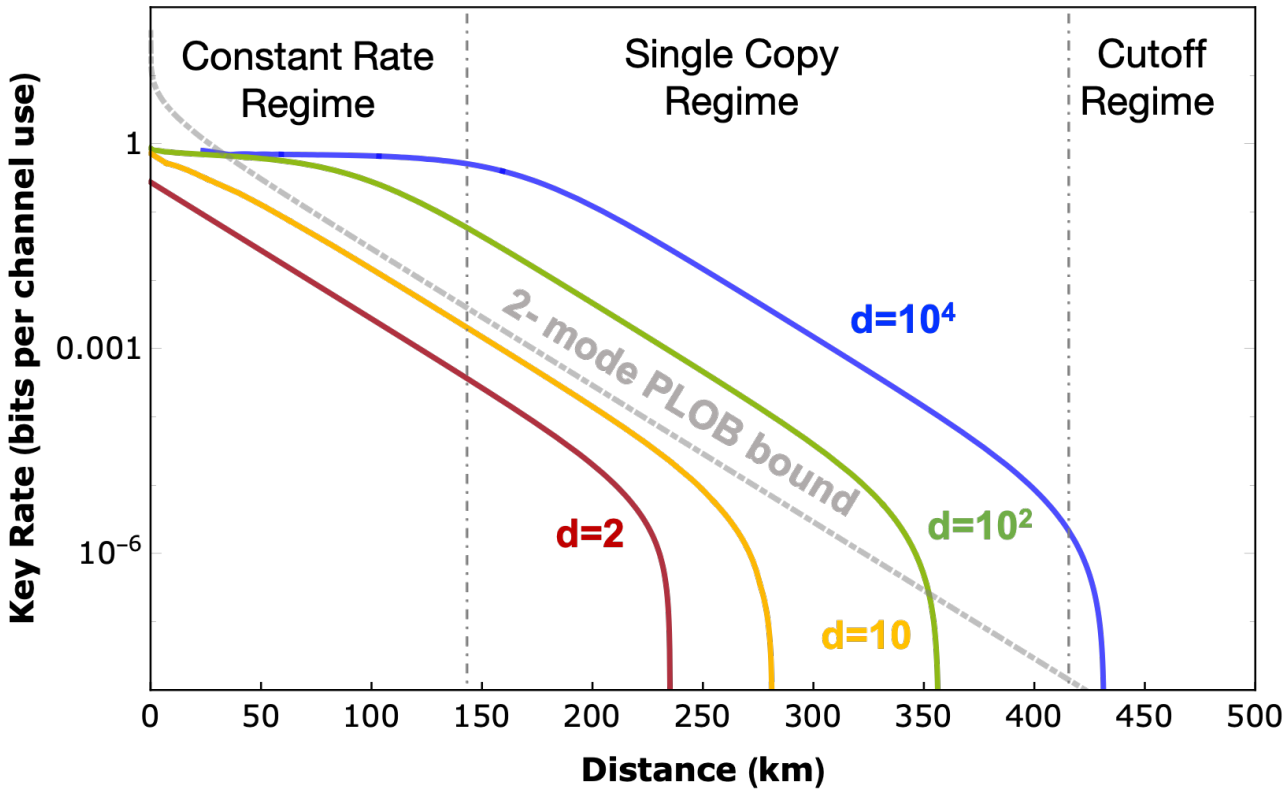


Figure 9.3: Key rate per channel use as a function of distance, for proactive MUB measurement strategy. The key rates are maximized against the photon number m. The parameters assumed in the plots are: Loss 0.2dB/Km; $P_{dark} = 10^{-6}$; efficiency of detectors $\eta = 25\%$; visibility $V = 98\%$. Since MUB-QCT can be implemented with 2 detection modes (2-single photon detectors) we also plot 2-modes PLOB bound [PLOB17a] as a benchmark..

We proved that when performing MUB-QCT using a d-dimensional quantum system, $m < d$ copies of a quantum state can be sent per channel use. This ability to send multiple copies has a striking consequence as it can offer high tolerance to the error in detection due to channel loss, resulting in an important and significant performance boost, characterized by a $O(d)$ multiplication of key rates and an extension by $50km \times \log(d)$ of the attainable distance over fiber. This is evident from the Figure (9.3), where the key rate is plotted for different values of d and is optimized by maximizing the key rate for different value of m. Analyzing the plots, we found that as we go to high dimensions the key rate per channel use increases. For $d \sim 10$ the performance of the MUB-QCT is comparable to that of BB84 protocol and for $d > 10^2$, there is a significant improvement in the performance.

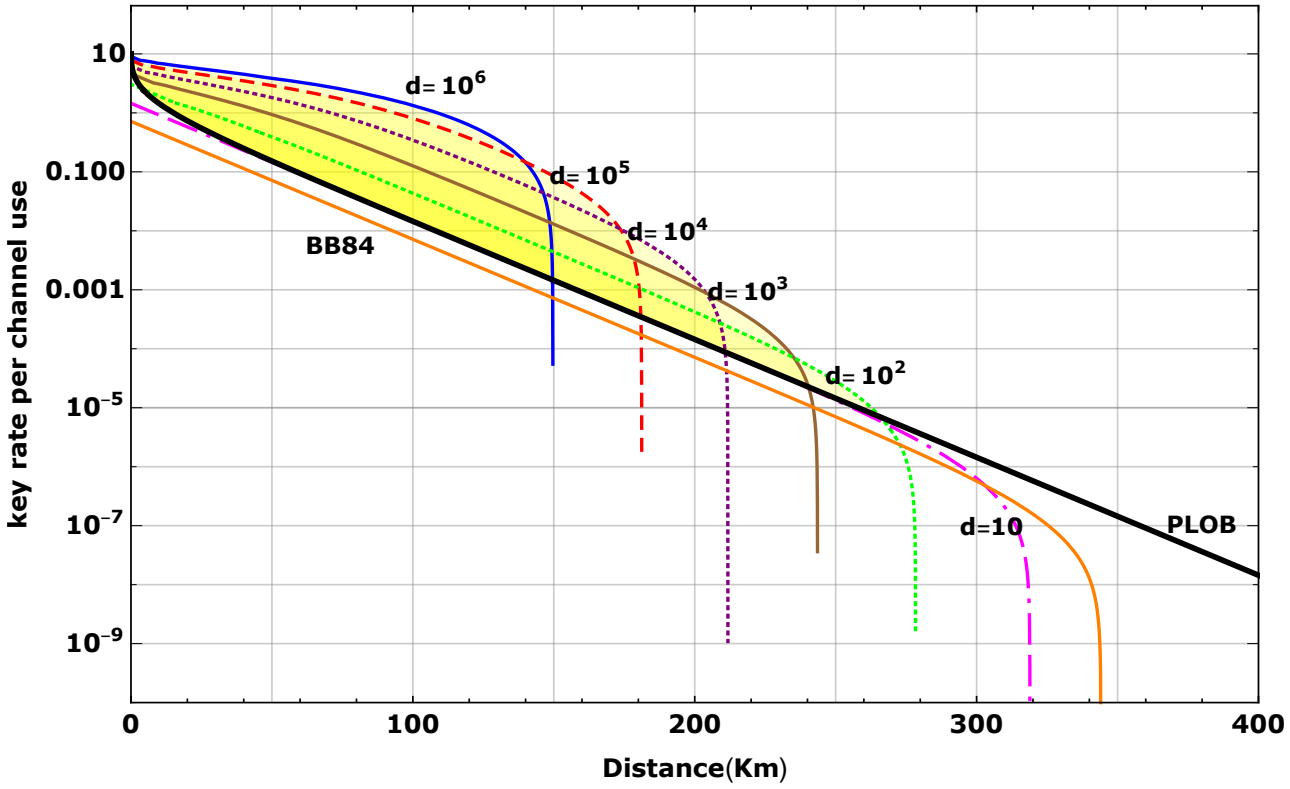


Figure 9.4: Plot of key rate per channel use as a function for distance(Km) for superconducting nanowire single-photon detectors (SNSPDs) with $p_{dark} = 10^{-8}$, $\eta = 66\%$, and $V = 98\%$. The plots for $d = 10^6, 10^5, 10^4, 10^3, 100, 10$ are optimized by maximizing the key rate as a function of distance for different value of m.

9.4.2 m-MUB-QCT-(log d, log d) Protocol

For the $\log d$ case, when sending m-copies of the quantum state the secret key rate for a loss channel is defined as

$$\begin{aligned} R &\geq (1-(1-T)^m) H_{min}(X|Z) - H(X|Y) \\ &\geq (1-(1-T)^m)(-\log(P_{guess}(m))) + p_c \log p_c + p_e \log\left(\frac{p_e}{d-1}\right) \end{aligned} \tag{9.3}$$

We plot Equation (9.3), for single photon detectors based on superconducting nanowire single-photon detectors (SNSPDs) [YCY+16], in Figure 9.4. Observing the Figure 9.4, we see that the achievable distance decreases as we increase the dimension, which is due to errors in detection increases with the increase in number of detectors. As a result, it is advantageous to use m-MUB-QCT-$(1, \log d)$ protocol.

9.5 MDI-type security

Figure (9.5), presents the trust assumptions required on hardware to prove security in (a) prepare and measure QKD, (b) MDI QKD, and (c) MUB-QCT. In general, hardware in Alice and Bob's labs comprise classical storage, a classical processing device and a device to perform quantum operations. This hardware may require some trust factor depending on their utility in the protocol. For instance,

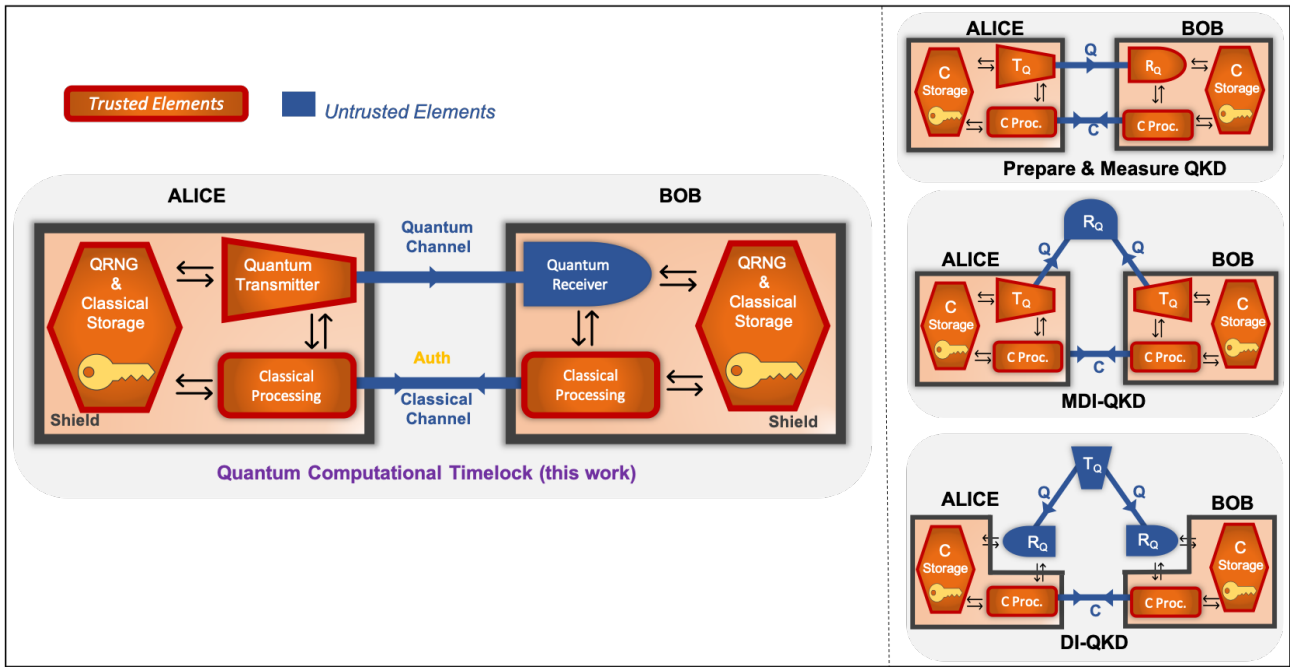


Figure 9.5: Trust assumptions on the hardware, required to prove security in different key distribution protocols. Elements that are trusted to work according to their specifications are represented in orange color, while, for elements in blue color, no assumptions are made on the internal working and specifications, removing an important constraint on the security of the protocol. The black color boundary represents the shield, which ensures that these devices do not leak any information out of the lab. In the figure shorthand notations are defined as, T_Q: quantum transmitter, R_Q: quantum receiver C: classical, and, Q quantum. The yellow color key is a short key required to generate short-term-secure encryption in QCT and also serve as an initial password to authenticate the classical channel.

in preparation and measure type QKD protocols it is assumed that these devices work exactly according to their specifications, and are shielded, i.e., they do not leak any information from leaking out of the lab. As a result of this, it is required for Alice to know the specifications of devices in Bob's lab, in another way, the security of the protocol inherently depends on the security of these devices. However, such a condition is difficult to ensure when implementing the protocol, as many attacks have been demonstrated to be directed towards quantum devices [QFLM07, ZFQ+08, LWW+10].

In Measurement Device Independent (MDI) QKD [LCQ12, BP12], any detector vulnerability is removed by making no trust assumption on the measurement devices, which is the most crucial part of the implementation and quantum transmitter and only classical processing devices are assumed to work according to their specifications. Consequently, the measurement device is located outside Alice and Bob's lab, as shown in the Figure (9.5). As a result, the security of the protocol does not depend on the security of measurement devices, offering an important implementation security advantage.

Device independent (DI) QKD [ER14, ABG+07] is another security framework providing unparalleled security, which holds irrespective of the quality and internal working of quantum devices (transmitter and receiver). However, DI-QKD makes some important assumptions like, there is no information leakage from trusted parties' locations and Alice and Bob have access to trusted randomness. These two assumptions are the cryptographic analogous of the locality (no-signaling) and

free-will loophole respectively. This high level of security can only be established under conditions which are very difficult to achieve experimentally. As a result, DI-QKD although, guarantee unprecedented security, yet, it is not the panacea for secure key distribution as it is difficult to implement and still requires important trust assumptions, that may not be much easier to comply with, than the one for prepare and measure QKD.

In Quantum Computational Timelock, MUB-QCT protocol, Alice and Bob are not required to estimate the errors by monitoring their channel, to bound Eve's information on the secret key. To bound Eve's information, Alice and Bob are required to calculate only the accessible information of the Eve, which depends on the input state prepared by Alice's quantum source and does not depend on Bob's measurement device. As a result, Alice is not required to know the specifications of measurement devices on Bob's side. Thus, the security is independent of any trust assumption on the measurement device. However, this kind of security is guaranteed only if the assumptions of the QCT security model holds. We call this, MDI-type security, as the security is similar to the MDI QKD protocol provided some additional restrictions.

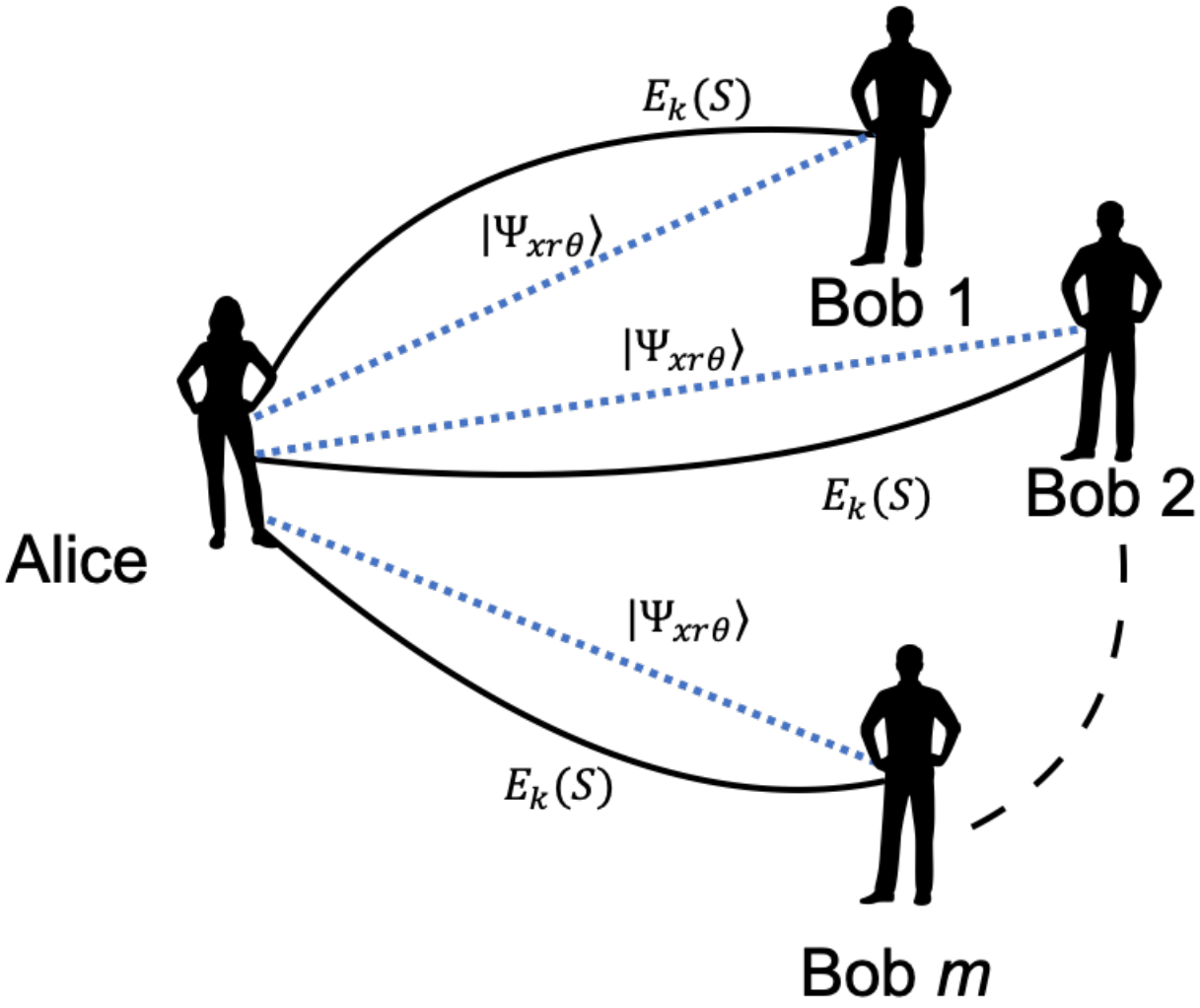


Figure 9.6: Multiparty MUB-QCT: m copies of the state $|\Psi_{xr\theta}\rangle$ generated can be sent to m authorized parties (Bob) simultaneously, allowing them to distill same key together.

9.6 Multiparty key distribution

The possibility of sending multiple copies of the quantum state per channel use can be exploited to realize multiparty key distribution in the QCT security model. In principle, m multiple copies prepared by Alice can be transmitted to at most m authorized Bobs, allowing them to distill the same key, as depicted in Figure (9.6). A general description of a m-party MUB-QCT distribution would consist of,

- Alice and m authorized parties exchange the classical secret (encoding bases) using a short term secure encryption.
- Alice prepares m-identical copies of a qudit state using the classical secret and send one copy to each of the m-parties.
- Each party then measures the individual state as directed by the classical secret.
- After multiple channel use, they perform information reconciliation on their strings to distill a secret key.

Its clear that in a d-dimension there can be at most $m < \sqrt{d}$ parties. However, to enhance the performance per party the number of parties can be reduced to $m' < m$ allowing to send on average m/m' copies of the same state per channel per party.

Chapter 10

Conclusion

10.1 Brief review of the results presented in the thesis

Extending the functionality and overcoming the performance limitation under which QKD can operate requires either quantum repeaters or new security models. Investigating the latter option, we introduced a new *Quantum Computational Timelock* (QCT) security model (Chapter 5), where we assume that an encryption scheme is computationally secure for a time longer than the decoherence time of quantum memories. We discussed the rational (5.6) of using a hybrid security model combining both quantum and computational assumptions. We also discussed the validity (5.7) of these assumptions against the state of the art quantum and computational technologies.

In chapter 6, we proposed the key establishment in the QCTsecurity model. We constructed a specific key establishment protocol that we call the MUB-QCT key distribution protocol, where the classical message is encoded on a d-dimensional quantum state using a complete set of Mutually Unbiased Bases (MUBs) (6.3). We proposed multiple versions of the MUB-QCT protocol

- 1-MUB-QCT-$(\log d, \log d)$: where for one copy of the quantum state sent per channel use, $\log d$ bits of information is encoded on a qudit using a full set of MUBs.
- 1-MUB-QCT-$(1, \log d)$: where for one copy of the quantum state sent per channel use, a bit is encoded on a qudit using a full set of MUBs and a complete set of pair-wise independent permutations. .
- m-MUB-QCT-$(\log d, \log d)$: multiple copy case where m copies of a qudit encoding $\log d$ bits of information is sent per channel use.
- m-MUB-QCT-$(1, \log d)$: multiple copy case where m copies of a qudit encoding a bit is sent per channel use.

We proved the security of 1-MUB-QCT protocols by upper bounding Eve's information for the optimal eavesdropping attack strategy, which corresponds to immediate measurement followed by a post measurement decoding (Chapter 7). For 1-MUB-QCT-$(1, \log d)$ protocol we show that for an adversary this optimal strategy reduces to accessing the output of a strong QC-extractor. We show that for the 1-MUB-QCT-$(\log d, \log d)$ protocol Eve's information is upper bounded as $\mathcal{O}(1/\sqrt{d})$ while for the 1-MUB-QCT-$(1, \log d)$ Eve's information is upper bounded as $\mathcal{O}(1/d)$.

Since the MUB-QCT protocol defines an effective wire-tap scenario, we showed that the key rate in the asymptotic limit for the MUB-QCT protocol, can be derived using following Csiszár and

Körner formula [CK78b]:

$$R \geq I(X;Y) - I(X;Z) \geq H_{min}(X|Z) - H(X|Y) \tag{10.1}$$

This allows to make several observations, regarding the properties of 1-MUB-QCT protocol

- **High noise tolerance for large d :** Similarly to high-dimensional QKD [CBKG02a], 1-MUB-QCT protocol allows high resilience to noise by offering tolerable error rate of up to 50% for large d
- **Fixed resource requirements:** The 1-MUB-QCT $(1, \log d)$ protocol can be implemented with only two detectors, irrespectively of d . This relaxes resource requirements compared to HD-QKD schemes, requiring d-single-photon detectors [DBD+17].
- **MDI security:** In the MUB-QCT protocol, the upper bound on Eve information can be achieved by only considering the input state and not Bob measurement's results. Consequently, the implementation of Bob's measurement device is not required to be trusted to guarantee security, as displayed on Figure 9.5.

We showed that the m-MUB-QCT protocol opens the way to higher key rates and long-distance operation, while keeping implementation simple and using with coherent states with mean photon numbers $\sim m$. We proved the security of the m-MUB-QCT protocol against a specific non-adaptive attack strategy called the proactive MUB measurement strategy , where Eve measures each copy in a a different MUB and showed that it allows secure key distribution with input states containing up to $O(d)$ photons for m-MUB-QCT-$(1, \log d)$ protocol, implying a significant performance increase, characterized by a $O(d)$-**multiplication of key rate** as shown in Figure 9.3. The possibility of sending multiple copies of the quantum state per channel use can moreover be leveraged to perform **multiparty key distribution** between one Alice and multiple Bobs

Our results illustrate that hybrid approaches to quantum cryptography constitute a promising and practical route to extend the performance and functionality of quantum cryptography. In particular, our newly proposed MUB-QCT protocol enables everlasting security key establishment - not achievable with classical means - with performance significantly outperforming those of QKD.

10.2 Comparison with related work

Our work is in particular related to the recently proposed idea of *Quantum Enigma Machine* [GHK+14a] and *Quantum data locking* [LL14, LL15a] where the security is proved by upper bound Eve's accessible information in discrete as well as continuous variable settings [LL15b]. However, existing work on Quantum data locking systematically uses random coding arguments to build and prove the security of protocols, making the implementation so far not possible in practice.

Although further analysis is required on that matter, we conjecture that a fundamental difference between Quantum data locking (QDL) and our Quantum Computational Timelock (QCT) stems from the fact that Discrete Variable QDL constructions need to operate with a key much smaller than the channel capacity and thus much smaller than $\log(d)$ bits. This requirement stems from the constraint of obtaining a positive data locking rate [GHK+14a]. QCT, on the other hand, leverages on an additional short-term-secure encryption assumption. This enables Alice and Bob to share a secret S that is comparable to, or even possibly much larger than, $\log(d)$ bits. This gives rise to the possibility to use strong locking schemes, such as one based on a full family of MUBs, that are

moreover easy to implement with multimode coherent states, containing m photons on average. This is precisely what we propose in this article with the MUB-QCT construction.

On the other hand Quantum Data Locking, operating in a regime where the key is much smaller than $\log(d)$ bits requires to consider locking constructions over quantum codewords that are entangled with respect to mode partitions. This leads to constructions for which the measurement that Bob must perform, are in general entangled measurements between modes, and therefore difficult to implement in practice.

Flood-light QKD (FL-QKD) [ZZD+16, ZZWS17]. is another recently proposed protocol. It aims at providing performance level beyond what is achievable with QKD, in particular in terms of rate. FL-QKD consists in sending coherent light over a very large number of modes, while keeping mean photon number per mode below one to guarantee no-cloning. It is based on a two-way procedure, and the optical storage of a random coherent wavefront, used to perform a multimode homodyne measurement. FL-QKD could potentially allow Gbit/s secret-key rates over metropolitan-area distances. However, its current security analysis only guarantees protection against frequency-domain collective attacks and is still vulnerable to block-wise coherent attacks [ZZLS18]. Moreover, while it can have a decisive impact on rate (which we also expect for QCT), FL-QKD cannot be used to extend the distance, as compared to standard QKD.

Table 10.1: Overview of different quantum-based key distribution protocols in high dimension. In the table, d is the dimension of the system, T is the transmittance of the channel, and m is the number of photons that are sent per channel use.

Protocol	**Security Model**	**Secure Key Rate per channel use**	**Performance**
QKD: d dimension	Information Theoretic Sec.	$\sim T\log_2(d)$	- Less than one photon per channel use ($m<1$). - For fixed detection technology (p_d) and $T=10^{-L/50}$, $L_{max}<25\log(1/p_d)$.
Flood Light QKD [ZZD+16, ZZWS17]	Information Theoretic Sec.	$\sim mT[1-h_2(\frac{e^{-mT}}{2})$ $-\frac{Tm^2}{d}\log_2\frac{m+d}{m}]$	- $\mathcal{O}(m)$-fold secret key rate increase w.r.t. QKD. - no distance increase w.r.t. QKD. - Security proven for restricted attacks [ZZD+16, ZZLS18].
Quantum Data Locking Discrete Variable [LL14]	Time-limited Q memory	$\sim T\log_2(d)$	- Security is independent of channel monitoring. - $m=1$ (encoding on single photons).
Quantum Data Locking Continuous Variable [LL15a]	Time-limited Q memory	Direct Reconciliation $DR=1+\log(T/(1-T))$, Reverse Reconciliation $RR=1+\log(1/(1-T))$	- Security is independent of channel monitoring. - Constructions based on random codes.
Q. Comp. Timelock MUB-QCT **[our work]**	Time-limited Q memory Short-term sec. encryption	$\sim mT\log_2(d/m)$	- $\mathcal{O}(m)$-fold secret key rate increase w.r.t. QKD. - Security is independent of channel monitoring.

Chapter 11

Perspectives

In this chapter we describe different perspective for the future work.

11.1 QCT based on communication complexity

In this section we consider one-way communication complexity problems such as Hidden matching problem [BYJK08, GKRW06, GKK+07, Gav09] and Khot-Vishnoi game [BRSD11]. One important property of such problems is that they define an evaluation function, on n bit input, for which there is an an exponential separation between the classical one-way randomized communication complexity and the quantum one-way communication complexity. For hidden matching problem the classical one-way randomized communication complexity scales like $\Omega(\sqrt{n})$ bits and the quantum one-way communication complexity scales like $\mathcal{O}(\log n)$ qubits. While, the Khot-Vishnoi game offers quadratically stronger advantage over the Hidden matching game with the the classical one-way randomized communication complexity scales like $\Omega(n)$ bits and the quantum one-way communication complexity scales like $\mathcal{O}((\log n)^2)$ qubits.

The exponential separation between the classical and quantum communication complexity for such problems can be utilized to construct a key distribution protocol and prove their security in the QCT security model. The main idea to prove the security of a key distribution protocol in the QCT security model using communication complexity problem is to reduce an unauthorized Eve to a classical communication setting while authorized Alice and Bob are allowed to do quantum communication. The separation between the Eve's classical communication complexity and Alice-Bob's quantum communication complexity can then allow to send multiple copies per channel use ($\Omega(\sqrt{n})$ for QCT key distribution using Hidden matching problem and $\Omega(n)$ for QCT key distribution using Khot-Vishnoi game) while still bounding Eve's information to be less than the Alice and Bob's mutual information. As a result, will allow Alice and Bob to exchange secure keys over a long distance.

In the sections below, we describe the two communication complexity problems and propose the key distribution protocols in the QCT security model. Proving the security of the protocols is the possible direction for the future work.

11.1.1 Hidden matching game

The Hidden matching problem was introduced in quantum communication complexity by BarYossef et al. [BYJK08], and many variants of it were subsequently studied [GKRW06, GKK+07, Gav09].

This is a one-way communication complexity task involving two players Alice and Bob. It is described as follows. For any positive even integer n, Alice receives as input a string $x \in \{0,1\}^n$ while Bob receives a $n/2$ tuples matching σ_i uniformly randomly from $\mathcal{M}_n \in \{\sigma_1, .., \sigma_{n-1}\}$. Here $\mathcal{M}_n$ is the set of $n-1$ perfect disjoint matchings on n nodes. The objective of the problem is for Bob to output any one of the $n/2$ possible parity values $x_k \oplus x_l$ for a pair (k,l) that belongs to the matching σ_i with minimum communication resources. Here x_k, x_l are k^{th} and l^{th} bit of x respectively.

Optimal classical protocol

For this problem, the randomized classical lower bound of $\Omega(\sqrt{n})$ was shown by Bar-Yossefet al. [BYJK08] and Buhrman et al [BRSD11]. In high level, Alice's message should allow Bob to output the parity of an edge from each one of the possible matchings, in other words for $\mathcal{O}(n)$ different edges. No matter which edges one picks, they will always contain at least $\Omega(\sqrt{n})$ different bits of the input x, and hence Alice must send at least $\Omega(\sqrt{n})$ bits of information and hence communication. The proof structure for computing lower bound in [BRSD11] is as follows: if Alice's message to Bob is small, let's say c bit, then the set of inputs $x \in \{0,1\}^n$ for which Alice sends a particular message m, will be large (typically of the order of 2^{n-c}). This would mean that Bob will have very little knowledge of most of the bits of x. Using the KKL inequality [KKL88], this implies that Bob would not be able to correctly answer the parity $x_i \oplus x_j$ for most of the $\begin{pmatrix} n \\ 2 \end{pmatrix}$ tuples of the form (i,j). Even though Bob has some relaxation in a sense that he can output the parity outcome of any one of the $n/2$ tuples of σ_i, still it turns out that on average it is hard for him to output the correct parity outcome. Using this idea, and the KKL inequality, the classical lower bound to succeed with an error probability p_{error} is,

$$c \geqslant \frac{\log_2 e}{e}\left(\frac{1}{2} - p_{\text{error}}\right)\sqrt{n-1} \tag{11.1}$$

Bar-Yossef et al. also proved that this bound is tight by describing a randomized one-way protocol using birthday paradox argument to show that only $\mathcal{O}(\sqrt{n})$ classical bits is sufficient to implement the problem. The proof structure is as follows: Let us assume that Bob's matching set $\mathcal{M}_n$ is restricted to be one of the $n-1$ disjoint matchings. Since Alice has no information about which matching Bob has received, to maximize the winning condition she encodes her message to contain the parity information of at least one pair from each matching with high probability. Suppose she does this by sending c random bits of the input x or equivalently $c(c-1)/2$ tuples to Bob. Each perfect disjoint matching σ_i that Bob would receive has $n/2$ tuples. Thus the matching set $\mathcal{M}_n$ has in total $n(n-1)/2$ distinct tuples. The probability that none of the tuples that Alice sends to Bob is in the matching σ_i received by Bob is,

$$p_{\text{error}} = \left(1 - \frac{1}{n-1}\right)^{c(c-1)/2} \approx \exp\left(-c^2/2n\right) \tag{11.2}$$

For $p_{\text{error}} \leqslant 0.1$, the communication c is

$$c \geqslant \sqrt{2\log_e 10}\sqrt{n} \tag{11.3}$$

Quantum protocol

Using a simple quantum protocol, the above task can be solved by transmitting exponentially fewer number of qubits. Alice encodes her input $x \in \{0,1\}^n$ into the following superposition:

$$|x\rangle = \frac{1}{\sqrt{n}} \sum_{k=1}^{n} (-1)^{x_k} |k\rangle \tag{11.4}$$

where x_k is the k-th bit of the string x. She then sends it to Bob. For any matching $\sigma_i \in \mathcal{M}_n$ that Bob has as input, there exists a measurement by Bob which allows him to give the correct answer with certainty. To do so, he just measures the quantum state in the basis $\left\{\frac{1}{\sqrt{2}}(|k\rangle \pm |l\rangle\right\}, \forall (k,l) \in \sigma_i$. The outcome $\frac{1}{\sqrt{2}}(|k\rangle + |l\rangle)$ occurs iff $x_k \oplus x_l = 0$ whereas $\frac{1}{\sqrt{2}}(|k\rangle - |l\rangle)$ occurs iff $x_i \oplus x_j = 1$. Thus Bob gets the parity result of one of the tuples $(k,l) \in \sigma_i$ with certainty. This protocol uses only $\log_2 n$ qubits, and hence both the communication and the transmitted information is exponentially better than the classical counterpart.

QCT key distribution using Hidden matching

Notations: The Hidden Matching problem is built around an β-matching M, that constitutes part of the input given to Bob. M consists of a sequence of βn disjoint edges $(i_1, j_1), \cdots (i_{\beta n}, j_{\beta n})$ over $[n]$. In the following n will be assumed to be even. We will call $\mathcal{M}_{\beta n}$ the set of all such β-matchings on n bits. If $\beta = 1/2$ the matching is perfect and if $\beta < 1/2$ the matching is partial. We can view M as an $\beta n \times n$ matrix with two ones per rows, 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 βn-bit string $z = z_1, \cdots, z_l, \cdots, z_{\beta n}$ where $z_l = x_{i_l} \oplus x_{j_l}$.
β-Partial Matching Problem Using the notations above, we can define the following β-Partial Matching (βPM) problem Alice input $x \in_R \{0,1\}^n$ Bob input β-matching $M \in_R \mathcal{M}_{\beta n}$ and $\omega \in \{0,1\}^{\beta n}$ Promise on the Alice-Bob input: There is a bit b such that $\omega = Mx \oplus b^{\beta n}$ (equivalently, we have either $Mx \equiv z = \omega$ or $Mx = \bar{\omega}$). Communication model Classical or Quantum one-way communication between A and B Goal Bob evaluates b

Theorem 11.1.1 *Let $\beta \in (0, 1/4]$. The classical bounded-error one-way communication complexity of the β-Partial Matching problem is $R_1(\beta PM) = \Theta(\sqrt{n/\beta})$, while the quantum bounded-error one-way complexity is $Q^1(\beta PM) = O(\log(n)/\beta)$*

QCT-HM key distribution: Alice and Bob can communication with short-term security over a classical channel using computational encryption E_k (short-term secure key k, can either be a public or secret key, and has been previously shared with another, out-of-band channel). Alice generates an instance x, M of the $\frac{1}{4}$-Partial Matching Problem and sends M, ω to Bob (with short-term security) with $\omega = Mx \oplus b^{n/4}$. Alice wants to send information about b to Bob, with long-term (everlasting) security against Eve. Alice uses one-way quantum communication (over a quantum channel of transmission $T = t^2$) to send the encrypted mode coherent state $|\alpha\rangle_x$ (see below) with mean photon number $|\alpha^2|$ to Bob. Bob measures according to the partial matching, leading to a mutual information $I(A:B) \sim T\,|\alpha^2|$ (in the high loss- no error regime). Because of the QCT security model, Eve's best strategy to learn information about b is to measure $|\alpha\rangle_x$ immediately, i.e. before knowing anything about M. Using the mapping introduced in [AL14], Eve's accessible information scales like $O\left(|\alpha|^2 \log n\right)$ bits. Using theorem 11.1.1, this leads to a vanishingly (in n) small upper bound on $I(A:E)$, provided the total number of photons sent by Alice is $o(\sqrt{n})$.

Protocol 4 QCT Key distribution protocol using Hidden matching

- *Alice randomly generates a β-matching M with $\beta = 1/4$*
- *Alice also locally randomly generate a n bit vector, called x.*
- *Alice also locally randomly generate a bit b.*
- *Alice evaluates $\omega \in \{0,1\}^{n/4}$ as $\omega = Mx \oplus b^{\beta n}$ (where the matrix product is limited to the βn edges of the matching M and where $b^{\beta n}$ is a vector with either βn 0s or βn 1s).*
- *Alice then sends (M, ω) to Bob using computational encryption E_k.*
- *Alice then uses the quantum channel to send Bob the multimode coherent state of α^2 photons, encoded in one supermode x, this state is.*

$$|\alpha\rangle_x \equiv \otimes_{i=1}^{n} \left| \frac{(-1)^{x_i}\alpha}{\sqrt{n}} \right\rangle_i$$

- *Assuming a pure lossy channel, Bob receives $|t\alpha\rangle_x$. Since Bob knows the Hidden Matching instance (M, ω), he can perform the (orthogonal) measurement associated to M, with only two photon counters. with probability $T|\alpha|^2$ (in the high loss regime) Bob receives one photon with probability $(2\beta)^2$) the click obtained by Bob falls within the β-matching M else, i.e. with probability $1 - (2\beta)^2$), we have an erasure due to the matching.*
- *In case there is no erasure (probablility $(2\beta)^2$), Bob then gets a "signal' click that perfectly discriminates $b = 0$ and $b = 1$*

11.1.2 Khot-Vishnoi Game

Khot Vishnoi game is characterized by a two parameters an integer n, which is considered to be a power of 2, and a "noise parameter" $\eta \in [0, 1/2]$. Consider the group $\{0,1\}^n$ of all n -bit strings with '$\oplus$' denoting bitwise addition mod 2, and let H be the subgroup containing the n Hadamard codewords. This subgroup partitions $\{0,1\}^n$ into $2^n/n$ cosets of n elements each. Alice receives an input coset, chosen at random from a set of shifted Hadamard codewords

$$x = u \oplus H. \tag{11.5}$$

This coset of codewords can be written as $\{u + H\}$, with $u \in_R \{0,1\}^n$. These codewords are orthogonal to each other and are consist of n vectors of length 2^n. Alice adds a string of low Hamming weight $z \in \{0,1\}^n$ to her input which reads

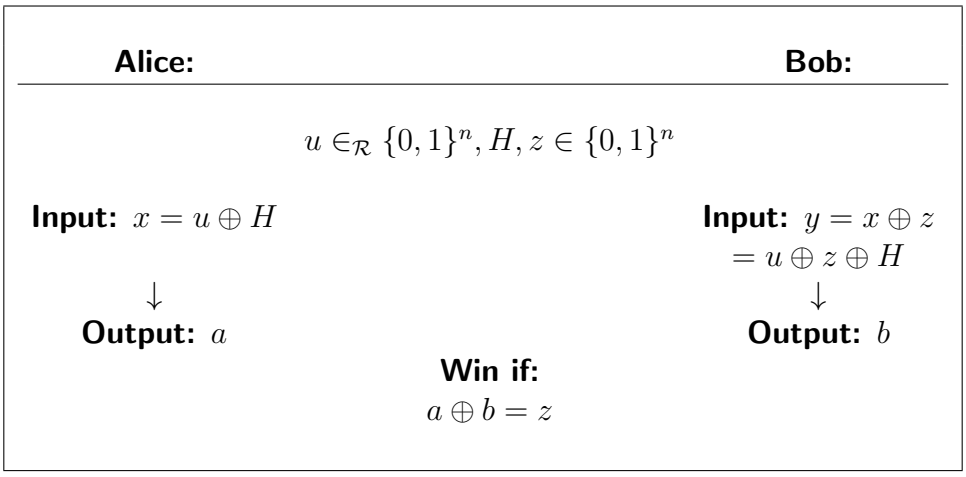
$$y = x \oplus z = u \oplus z \oplus H, \tag{11.6}$$

and send as an input coset to Bob. This adding of extra string is also known as bias, where each bit is set to 1 with probability η, independently of other bits. Notice that addition of z gives a natural bijection between the two cosets, mapping each element of the first coset to a relatively nearby element of the second coset; namely, the distance between the two elements is the Hamming weight

of z, which is typically around ηn. Both players are now suppose to output an element from their coset and they win the game if the elements matches under this bijection. In other words, Alice outputs an element $a \in x$ and Bob outputs $b \in y$, they win the game iff

$$a \oplus b = z \tag{11.7}$$

Notice that the number of possible inputs to each player is $2^n/n$ and the number of possible outputs for each player is n.



Classical Value of the Khot-Vishnoi game:

In [BRSD11] there exists a strategy whose winning probability is roughly $1/n^{\eta/(1-\eta)}$. To get some intuition for this game, first think of η as some small constant (even though we will eventually choose it close to $1/2$), and consider the following natural classical strategy: Alice and Bob each output the element of their coset that has highest Hamming weight. The idea is that if a is the element of highest Hamming weight in Alice's coset x, we expect $a \oplus z$ to also be of high Hamming weight (because it is close to a in Hamming distance), and so Bob is somewhat likely to pick it. We now give a brief back-of-the-envelope calculation suggesting that the winning probability of this strategy is of order $1/n^{\eta/(1-\eta)}$; since it is not required for our main result, we will not attempt to make this argument rigorous.

Let $t \geq 0$ be such that the probability that a binomial $B(n, 1/2)$ variable is greater than $(n+t)/2$ is $1/n$. Recalling that a binomial distribution $B(n,p)$ can be approximated by the normal distribution $N(np, np(1-p))$, and that the probability that a normal variable is greater than its mean by s standard deviations is approximately $e^{-s^2/2}$, we can essentially choose t to be the solution to $e^{-t^2/(2n)} = 1/n($ so $t = \sqrt{2n \ln n})$. Then we expect Alice's n -element coset to contain exactly one element of Hamming weight greater than $(n+t)/2$. Since the element a that Alice picks is the one of highest Hamming weight, we assume for simplicity that its Hamming weight is $(n+t)/2$. The players win the game if and only if $a \oplus z$ has the highest weight among Bob's n elements, which we heuristically approximate by the event that $a \oplus z$ has Hamming weight at least $(n+t)/2$. The Hamming weight of $a \oplus z$ is distributed as the sum of $B((n+t)/2, 1-\eta)$ and $B((n-t)/2, \eta)$, which can be approximated as above by the normal distribution $N((n+t)/2 - \eta t, n\eta(1-\eta))$. Hence for the Hamming weight of $a \oplus z$ to be at least $(n+t)/2$, the normal variable needs to be greater than its mean by $\eta t/\sqrt{n\eta(1-\eta)}$ standard deviations, and the probability of this happening is approximately $e^{-\eta^2 t^2/(2n\eta(1-\eta))} = 1/n^{\eta/(1-\eta)}$, as claimed.

Now we show that no classical strategy can be substantially better. The main technical tool used in the proof is the so-called Bonami-Beckner hypercontractive inequality, which is applicable to our setting because we choose u uniform and $u \oplus z$ may be viewed as a "noisy version" of u.

Theorem 11.1.2 *For any n which is a power of 2, and any $\eta \in [0, 1/2]$, every classical strategy for the Khot-Vishnoi game has winning probability at most $1/n^{\eta/(1-\eta)}$.*

Proof: Recall that the inputs are generated as follows: we choose a uniformly random $u \in \{0,1\}^n$ and an η -biased $z \in \{0,1\}^n$, and define the respective inputs to be the cosets $u \oplus H$ and $u \oplus z \oplus H$. We can assume without loss of generality that Alice's and Bob's behavior is deterministic. Define functions $A, B : \{0,1\}^n \to \{0,1\}$ by $A(u) = 1$ if and only if Alice's output on $u \oplus H$ is u, and similarly for Bob. Notice that by definition, these functions attain the value 1 on exactly one element of each coset. Recall that the players win if and only if the sum of Alice's output and Bob's output equals z. Hence for all $u, z, \sum_{h \in H} A(u \oplus h)B(u \oplus z \oplus h)$ is 1 if the players win on input pair $u \oplus H, u \oplus z \oplus H$ and 0 otherwise. Therefore, the winning probability is given by

$$\mathop{\mathbb{E}}_{u,z}\left[\sum_{h \in H} A(u \oplus h)B(u \oplus z \oplus h)\right] = \sum_{h \in H} \mathop{\mathbb{E}}_{u,z}[A(u \oplus h)B(u \oplus z \oplus h)] \tag{11.8}$$

$$= n \mathop{\mathbb{E}}_{u,z}[A(u)B(u \oplus z)] \tag{11.9}$$

where the second equality uses the fact that for all $h, u \oplus h$ is uniformly distributed.

We use the framework of hypercontractivity (see e.g. [O'D08]), which we briefly explain now. Specifically, for a function $F : \{0,1\}^n \to \mathbb{R}$, define its p -norm by $\|F\|_p = \left(\mathbb{E}_x\left[|F(u)|^p\right]\right)^{1/p}$ where the expectation is uniform over all $u \in \{0,1\}^n$. The noise-operator $T_{1-2\eta}$ adds "η -noise" to each of F 's input bits; more precisely, $\left(T_{1-2\eta}F\right)(u) = \mathbb{E}_z[F(u \oplus z)]$, where z is an η -biased "noise string." The linear operator T_ρ is diagonal in the Fourier basis: it just multiplies each character function $\chi_S (S \subseteq [n])$ by the factor $\rho^{|S|}$. It is easy to see that $\mathbb{E}_u\left[F(u) \cdot \left(T_\rho G\right)(u)\right] = \mathbb{E}_u\left[\left(T_{\sqrt{\rho}}F\right)(u) \cdot \left(T_{\sqrt{\rho}}G\right)(u)\right]$. The Bonami-Beckner inequality implies $\|T_\rho F\|_2 \leq \|F\|_{1+\rho^2}$ for all $\rho \in [0,1]$. We now have,

$$\begin{aligned}
\mathop{\mathbb{E}}_{u,z}[A(u)B(u \oplus z)] &= \mathop{\mathbb{E}}_{u}\left[A(u)\left(T_{1-2\eta}B\right)(u)\right] \\
&= \mathop{\mathbb{E}}_{u}\left[\left(T_{\sqrt{1-2\eta}}A\right)(u) \cdot \left(T_{\sqrt{1-2\eta}}B\right)(u)\right] \\
&\leq \left\|T_{\sqrt{1-2\eta}}A\right\|_2 \cdot \left\|T_{\sqrt{1-2\eta}}B\right\|_2 \\
&\leq \|A\|_{2-2\eta} \cdot \|B\|_{2-2\eta} \\
&= \left(\mathop{\mathbb{E}}_{u}[A(u)]\right)^{1/(2-2\eta)} \cdot \left(\mathop{\mathbb{E}}_{u}[B(u)]\right)^{1/(2-2\eta)} \\
&= \frac{1}{n^{1/(1-\eta)}}
\end{aligned}$$

Here the first inequality is Cauchy-Schwarz, and the second is the hypercontractive inequality. We complete the proof by noting that $n/n^{1/(1-\eta)} = 1/n^{\eta/(1-\eta)}$. □

Quantum strategy for the Khot-Vishnoi game:

In this section we describe a good quantum strategy for the Khot-Vishnoi game, following the ideas of Kempe, Regev, and Toner [KRT09]]and the SDP-solution of [KV13].

Theorem 11.1.3 *For any n which is a power of 2, and any $\eta \in [0, 1/2]$, there exists a quantum strategy that wins the Khot-Vishnoi game with probability at least $(1-2\eta)^2$, using a maximally entangled state with local dimension n.*

Proof: For $a \in \{0,1\}^n$, let $v^a \in \mathbb{R}^n$ denote the unit vector $((-1)^{a_i}/\sqrt{n})_{i\in[n]}$. Notice that for all a, b we have $\langle v^a, v^b \rangle = 1 - 2d(a,b)/n$, where $d(a,b)$ denotes the Hamming distance between a and b. In particular, the n vectors v^a, as a ranges over a coset of H, form an orthonormal basis of $\mathbb{R}^n$.

The quantum strategy is as follows. Alice and Bob start with the n -dimensional maximally entangled state. Alice, given coset $x = u \oplus H$ as input, performs a projective measurement in the orthonormal basis given by $\{v^a \mid a \in x\}$ and outputs the value a given by the measurement. Bob proceeds similarly with the basis $\{v^b \mid b \in y\}$ induced by his coset $y = x \oplus z \oplus H$. A standard calculation now shows that the probability to obtain the pair of outputs a, b is $\langle v^a, v^b \rangle^2 / n$. Since the players win iff $b = a \oplus z$, the winning probability on inputs x, y is given by

$$\frac{1}{n}\sum_{a\in x} \langle v^a, v^{a\oplus z}\rangle^2 = \frac{1}{n}\sum_{a\in x}(1 - 2d(a, a\oplus z)/n)^2 = (1-2|z|/n)^2 \tag{11.10}$$

where $|z|$ denotes the Hamming weight (number of 1 s) of the η -biased string z. Taking expectation and using convexity, the overall winning probability is

$$\mathop{\mathbb{E}}_{z}\left[(1-2|z|/n)^2\right] \geq (\mathop{\mathbb{E}}_{z}[1-2|z|/n])^2 = (1-2\eta)^2 \tag{11.11}$$

□

QCT Key distribution Protocol based on Khot-Vishnoi game:

Let n be an integer, which is considered to be a power of 2, and let H be a set of n Hadamard codewords. Let $\{U_u\}$ be a set of unitaties for $u \in |2^n|$ and $\{\mathcal{B}_z\}$ be a set of diagonal unitary matrices with $z \in |2^n|$ such that each diagonal element is set to 1 with probability $\eta = 1/2 - 1/\log n$. Alice chooses u and z at random and timelocks it using a t_{comp} secure encryption scheme and shares it with Bob. Alice then encodes a bit $a \in \{0,1\}$on a n-dimensional quantum state using U_u and $\mathcal{B}_z$ as

$$\rho_a = \frac{1}{|u||z|}\sum_{u,z} \mathcal{B}_z U_u \Big(\frac{1}{|r|}\sum_{r} |i_{ar}\rangle\langle i_{ar}|\Big)(\mathcal{B}_z U_u)^\dagger \tag{11.12}$$

for a vector state $|i_{ar}\rangle \in H$ with $i_{ar} = \frac{n}{2} \times a + r$ and $r \in [n/2]$

Alice sends this state ρ_a to Bob on a insecure quantum channel. Knowing u and z Bob decodes the bit by performing a projective measurement M_b^{uz} on ρ_a and obtains an outcome$b \in \{0,1\}$. Bob's measurement is defined by two-outcome POVM $\{M_b^{uz}\}_{b\in\{0,1\}}$ as

$$M_b^{uz} = \sum_{u,z}(\mathcal{B}_z U_u)^\dagger \Big(\sum_{r} |i_{br}\rangle\langle i_{br}|\Big)\mathcal{B}_z U_u. \tag{11.13}$$

Protocol 5 QCT Protocol based on Khot-Vishnoi Game

Input: Alice: $(a \in \{0,1\}, u \in [2^n], z \in [2^n],$
$r \in [n/2])$, **Bob:** $(\mathrm{Enc}(u,z), \mathrm{Dec}, \rho_a)$.

Output: Alice: $a \in \{0,1\}$, **Bob:** $b \in \{0,1\}$.

The protocol:

I **Data generation:**

- *Alice chooses* $a \in \{0,1\}$, $u \in [2^n]$, $z \in [2^n]$,, *and* $r \in [n/2]$, *uniformly at random.*

II **Time lock:**

- *Alice time locks* u *and* z *using a time-lock encryption scheme* Enc, *and sends it to Bob.*
- *Bob decrypts it immediately using the decryption function* Dec, *to obtain* (u, z).

III **Quantum communication:**

- *State preparation: Alice prepare a qudit state* ρ_a, *Equation (11.12).*
- *Distribution: Alice sends qudit system,* ρ_a, *to Bob.*
- *Measurement: Bob measures each quantum state using a POVM,* M_b^{uz} *(11.13), and outputs the result* $b \in \{0,1\}$.

After k *channel use Alice and Bob outputs:* $(a^k \in \{0,1\}^k, b^n \in \{0,1\}^k)$. *Following which they perform classical post-processing.*

11.2 Prove the security of QCT construction using other tools

11.2.1 Bitwise quantum to classical randomness extractors

Construction of bitwise quantum to classical randomness extractor is composed of unitaries acting on single qudits followed by some measurements in the computational basis. An appealing feature of the measurements defined by these unitaries is that they can be implemented with current technology. In addition to computational efficiency, the fact that the unitaries act on a single qubit is often a desirable property for the design of cryptographic protocols in which the creation of randomness is not the only requirement for security.

The unitaries considered for bitwise QC Extractor are even simpler. They are composed of unitaries V acting on single qudits followed by permutations P of the computational basis elements. As the measurement $\mathcal{T}$ commutes with the permutations P, we can first apply V, then measure in the computational basis and finally apply the permutation to the (classical) outcome of the measurement. In addition to the computational efficiency, the fact that the unitaries act on single qudits, is often a desirable property for the design of cryptographic protocols. In particular, the application to the noisy storage model that we present in Section V does make use of this fact.

Let $d \geq 2$ be a prime power so that there exists a complete set of mutually unbiased bases in dimension d. We represent such a set of bases by a set of unitary transformations $\{V_0, V_1, \ldots, V_d\}$ mapping these bases to the standard basis. For example, for the qubit space $(d = 2)$, we can choose

$$V_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad V_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad V_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ i & -1 \end{pmatrix}$$

Defining the the set $\mathcal{V}_{d,n}$ of unitary transformations on n qudits by $\mathcal{V}_{d,n} := \{V = V_{u_1} \otimes \cdots \otimes V_{u_n} | u_i \in \{0, \ldots, d\}\}$. $\mathcal{P}$ denotes a family of pair-wise independent permutations.

Theorem 11.2.1 *Let $A = A_1A_2$ with $|A| = d^n, |A_1| = d^{\xi n}, |A_2| = d^{(1-\xi)n}$, and d a prime power. Consider the map $\mathcal{T}_{A\to A_1}$ as defined in Equation (7). Then for $\delta \geq 0$ and $\delta' > 0$,*

$$\frac{1}{|\mathcal{P}|}\frac{1}{(d+1)^n}\sum_{P\in\mathcal{P}}\sum_{V\in\mathcal{V}_{d,n}}\left\|\mathcal{T}_{A\to A_1}\left(PV\rho_{AE}(PV)^\dagger\right) - \frac{\mathbb{I}_{A_1}}{|A_1|}\otimes\rho_E\right\|_1 \leq \sqrt{2^{(1-\log(d+1)+\xi\log d)n}\left(1+2^{-H^{\delta}_{\min}(A|E)_\rho+z}\right)} + 2\left(\delta+\delta'\right)$$

where $\mathcal{V}_{d,n}$ is defined as above, $\mathcal{P}$ is a set of pair-wise independent permutation matrices, and $z = \log\left(\frac{2}{\delta'^2}+\frac{1}{1-\delta}\right)$. In particular, the set $\{PV : P\in\mathcal{P}, V\in\mathcal{V}_{d,n}\}$ is $a(k,\varepsilon)$ -extractor provided

$$\log|A_1| \leq (\log(d+1)-1)n + \min\{0,k\} - 4\log(1/\varepsilon) - 7$$

and the number of unitaries is

$$L = (d+1)^n d^n\left(d^n-1\right)$$

The proof can be found in [BFW14].

QCT key distribution based on bitwise quantum to classical randomness extractor

The QCT key establishment protocol can be constructed using the unitaries as considered to for the bitwise QC Extractor. The security of such a protocol can then follow from bitwise QC extractor construction. The main idea will be to show that the optimal eavesdropping strategy for an adversary reduces to obtaining an output of a bitwise QC extractor. These unitaries are easy to generate experimentally and can provide a solution to the implementation challange as described in the section 11.3

11.2.2 Pseudo-random quantum states

An quantum information-theoretic conjecture was proposed by Ji, Liu and Song [JLS18] (CRYPTO 2018), which suggested that a uniform superposition with random binary phase is statistically indistinguishable from a Haar random state. That is, any polynomial number of copies of the aforementioned state is within exponentially small trace distance from the same number of copies of a Haar random state. This conjecture was later proved by Zvika Brakerski Omri Shmueli in [BS19].

As a consequence of this, a provable elementary construction of pseudorandom quantum states from post-quantum pseudorandom functions is possible. Moreover, replacing the pseudorandom function with a (2t)-wise independent function, results in an explicit construction for quantum state t-designs for all t.

In terms of computational complexity, this construction uses circuits with restricted structure known in the literature as HT, which contains a single parallel layer of Hadamard gates, followed by a circuit of Toffoli gates. Such a restricted model of quantum computation is enough to approximate the Haar measure.

QCT key distribution based on pseudo-random quantum states

The QCT key establishment protocol can be constructed where Alice generates a n-qubit uniform superposition state with only binary phase, $\frac{1}{\sqrt{2^n}}\sum_{x\in\{0,1\}^n}(-1)^{f(x)}|x\rangle$, where $f : \{0,1\}^n \to \{0,1\}$ is a random function. Using a (2t)-wise independent function as f makes it perfectly indistinguishable

from a completely random function. The t-design construction can be implemented by an HT circuit, comprising of a single parallel layer of Hadamard gates, followed by a circuit of Toffoli gates. The idea to prove security of such a protocol will be to show that for an unauthorized adversary the direct input state received is a pseudorandom state and is indistinguishable from the Haar measure.

11.3 Identify and demonstrate specific implementation routes

In this section we explore the possible implementation of the MUB-QCT protocol. We first explain the important experimental challenges for the implementation of the protocol. We then briefly review different high-dimensional encodings that have been demonstrated experimentally. We then propose a sketch of a possible high dimensional MUB-QCT protocol using spatial modes and finally we discuss the suitability of QCT key distribution protocol with coherent state encoding.

11.3.1 Implementation challenges for the MUB-QCT protocol

As observed in chapter 9, MUB-QCT protocol can offer important performance gains (like high tolerance to errors and improved reachable distance by sending multiple copies per channel use) when implemented in high dimension. However, operating high-dimensional encodings, communication, and detection is one of the major challenge in the implementation of the MUB-QCT protocol.

It will be challenging to generate a high-dimensional quantum state that can implement the MUBs. Using spatial modes encoding, the d-dimensional Hadamard basis can be generated from the computational basis using a combination of beam-splitters. Any other (one of the d-1) MUB can be generated by transforming the Hadamard basis using phase modulators (for example see Figure 11.1). The permutation of the modes can be done using the switches. However, as the dimension of the problem increases the circuit complexity also increases and will be very challenging to demonstrate it experimentally.

11.3.2 Review of different high dimensional encodings

To date, multiple high-dimensional quantum systems have been investigated, including position-momentum[ZSW08], temporal-spectral [TBZG00, TAZG04, Qi06, NWS+13, LZS+14, AKBH07], and orbital angular momentum (OAM) [SBF+17a, MMLO+15a, MDG+13]. Existing time or spectral encoding techniques indicate the possibility to operate with d as large as 10^3 and possibly $10^5 - 10^8$ [ZZWS17] with existing or near-term technologies.

Initial security analysis by Cerf et al. for discrete large alphabet QKD showed improved resilience against noise and loss [CBKG02b]. However, the proposed scheme with its two early proposals-one using OAM and another using temporal-spectral encoding-was challenging to demonstrate. The main difficulty lies in the measurement of discrete high-dimensional states within at least two mutually unbiased bases. Efficient implementation of the scheme for the two proposed degrees of freedom required single-photon detectors that scale with the dimensionality d -prohibiting the use of large d. Therefore, there has been a strong desire in developing HD QKD schemes with the ability to measure higher-order correlations using only a few single photon detectors. Ant Thus, MUB-QCT provides one solution to the problem as it requires only two detectors irrespective of the dimension of the encoding.

The development of temporal-spectral encoded HD QKD spurred record demonstrations of secret key capacity at 7.4 secret bits per detected photon [ZZH+15] and secret key generation rates of

23Mbps [LBZ+16b] and 26.2Mbps [ILC+17] with $d = 16$ at 0.1 dB loss and $d = 4$ at 4 dB induced loss, respectively. Furthermore, a $43 - \text{km}$ (12.7 dB loss) field demonstration between two different cities show a maximum secret key generation rate of 1.2Mbps [LBZ+16b].

High-dimensional QKD with OAM has also witnessed rapid development due as it is directly compatible with free-space QKD systems [EFKZ17]. Since OAM modes rely on the preparation and the measurement of discrete highdimensional states, the security proofs extend directly from the work by Cerf et al. Recently, the security proof has also been successfully extended to include finite-key analysis for composable security [BMF+16]. Moreover, MUB-QCT can be implemented with OAM.

A photon carrying an OAM information has a helical or twisted wave front with an azimuthal phase φ which wraps around ℓ (helicity) times per wavelength. For the popular Laguerre-Gauss mode, a photon carrying an $\ell\hbar$ OAM can be described as $\left|\Psi_Z^\ell\right\rangle = e^{i\ell\varphi}.\ell$ is an unbounded integer, which allows arbitrarily high encoding dimension, but practically one limits $\ell \in [-L, L]$ to achieve a dimensionality $d = 2L + 1$. A mutually unbiased basis set can be constructed using a linear combination of OAM modes

$$\left|\Psi_X^n\right\rangle = \frac{1}{\sqrt{d}} \sum_{\ell=-L}^{L} \exp\left(i\frac{2\pi n\ell}{d}\right) \left|\Psi_Z^\ell\right\rangle \tag{11.14}$$

All $d+1$ sets of quantum states can be generated using a spatial light modulator (SLM) [NAL90], a digital micro-mirror device (DMD) [BCWP13], or a tunable liquid crystal device known as q -plates [ZYC14, SMD+11].

The first laboratory demonstration of high-dimensional OAM QKD achieved a secret key generation rate of 2.05 bits per sifted photon using a seven-dimensional alphabet ($L = 3$ and $d = 7$) [MMLO+15b] More recently, a 300-m free-space field demonstration in Ottawa with four-dimensional quantum states achieved 0.65 bits per detected photon with an error rate of 11% : well below the QKD error rate threshold for $d = 4$ at 18% [SBF+17b]. Although moderate turbulence was present during the experiment, going to longer distances will require active turbulence monitoring and compensation [RXH+14].

OAM demonstrations involving SLM, DMD, and q -plates so far have required a time in the order of 1 ms to reconfigure limiting the QKD clock rate in the kHz regime. While q -plates can potentially be operated at GHz rates by using electrooptic tuning, these have yet to be demonstrated [KPN+09]. One appealing new direction is the use of photonic integrated circuits (PICs), which may dramatically reduce the configuration time. Thermo-optically tuned on-chip ring resonators have demonstrated a switching time of $20\mu\text{s}$ [SCW+14, CHZ+16]. More recently, precise control of OAM mode generation has been demonstrated using a 16×16 optical phase array which allows for generation of higher fidelity OAM states [SML+14]. Furthermore, large scale onchip MEMS-actuation has also been demonstrated with a switching time of $2.5\mu\text{s}$ with the potential of application to OAM generation and control [HSQ+15].

11.3.3 QCT with coherent state encoding

In chapter 9, we observed that under the restricted scenario MUB-QCT protocol allows sending $m < d$ number of copies per channel use. In optical terms, it means we can send multiple photons per channel use. A multi-photon coherent state is easy to generate and operate on experimentally. Therefore, MUB-QCT protocol can have implementation benefits when operated with coherent state encoding.

A coherent state have photons distributed in the Poisson distribution, i.e., the probability of detecting n-photons in a coherent state is

$$P_\mu(n) = \frac{\mu^n e^{-\mu}}{n!} \tag{11.15}$$

Where, $\mu = |\alpha|^2$ is the average number of photons. In the limit, where the mean photon number sent by Alice is very large, the Poisson distribution can be approximated to a Gaussian distribution with the mean of the distribution μ and the standard deviation $\sqrt{\mu}$. The average number of photons that can hit the detector is then equal to the mean photon number of the coherent state.

In chapter 9 we showed that the upper bound on the number of copies of the quantum state that Alice can send, such that Eve's accessible information on the secret key is less than the mutual information between Alice and Bob is $m < d$. This implies that, if a coherent state with the number of photons μ, for $\mu + 4\sqrt{\mu} < d$, is prepared by Alice, then with very high probability (corresponding to the 4 σ confidence, i.e., 99.994%), Eve's accessible information on the secret key can be bounded to be less than the mutual information between Alice and Bob.

As a result, MUB-QCT is well suited to be implemented with continuous variables, which make use of only standard telecommunication components that are manageable, cheaper, much more mature from a technological point of view, and most suitable candidates for long-range quantum communication. To explore QCT key distribution protocols using the continuous variable coherent state encodings and proving their security is an are of interest and a possible direction for the future work.

11.3.4 Spatial mode high dimensional encoding

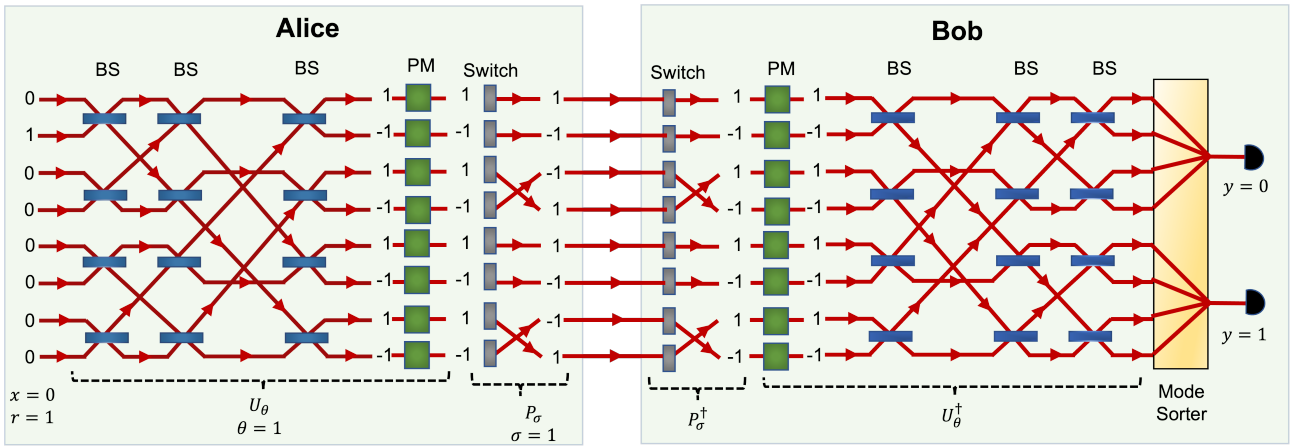


Figure 11.1: A sketch of possible implementation of the $1 - MUB - QCT - (1, 3)$ protocol, for single channel use. The value of different parameters considered are as following: $x = 0$, $r = 1$, $\theta = 1$, and $\sigma = 1$. The modes considered are spatial modes. Acronyms used in the figure are, BS: Beam Splitter, PM: Phase Modulator.

We have proposed the MUB-QCT protocol for key distribution in a very theoretical and abstract way. Therefore, in this section we propose a sketch of a possible experimental implementation of high dimensional MUB-QCT protocol using spatial modes. Figure 11.1, presents a sketch of possible implementation of the $1 - MUB - QCT - (1, 3)$ protocol, where one bit is encoded on a

2^3 dimensional quantum system. The modes considered are spatial modes. In the figure, for a single channel use, the value of different parameters considered are as following: $x = 0$, $r = 1$, $\theta = 1$, and $\sigma = 1$. Alice encodes the state $|\psi_{01}^{11}\rangle$ (Equation 6.5) on a 2^3 dimensional state. To encode this state she chooses the state $|i_{01}\rangle$ (for $x = 0$ and $r = 1$) in the computational basis. This state is represented by the column vector $(0, 1, 0, 0, 0, 0, 0, 0)$. If Alice intends to choose the computational basis as the encoding basis she can directly send this state to the apply the permutation. However, if the chosen basis is one of the rest d MUBs then Alice first performs a Hadamard transformation using a series of beam spliters (BS) followed by a phase modulators (PM) on each mode. Phase modulation can be used to transform the state in Hadamard basis to a state in rest of the $(d-1)$ MUB. The permutation of the modes is done using switches. In the figure 11.1, the same is represented for $\theta = 1$ (Hadamard basis) and $\sigma = 1$. On receiving the quantum state from Alice, Bob, who knows the value of θ and σ performs the reverse operations as depicted in the figure 11.1. Finally she uses mode sorter to divide the d modes into a pair of $d/2$ modes and send each pair to one of the two detectors. A signal in either of the detector corresponds to the Bob's bit measurement value. Finding a practical way to implement experimentally the MUB-QCT protocol is an important direction for our future work.

Appendix A

Bounding the norm of sum of l rank-1 projector

Following inequality holds for the sum of l rank-1 projectors acting on an arbitrary finite dimensional Hilbert space $\mathbb{C}^d$

$$\begin{aligned} ||O_1 + \ldots + O_l|| &\leq 1 + (l-1)\cos\phi \\ \cos\phi &= \max_{i,j>1} ||O_i O_j|| \end{aligned} \tag{A.1}$$

Proof: Let us introduce an an auxiliary Hilbert space $\mathbb{C}^l$, and define a standard basis $|i\rangle, i = 1, \ldots, l$, for this space. Consider then an operator Q acting on $\mathbb{C}^l \otimes \mathbb{C}^d$

$$Q = \sum_i |1\rangle\langle i| \otimes O_i \tag{A.2}$$

which is a block matrix with the first blockrow containing the projectors O_i. Using the fact that $||Q^\dagger Q|| = ||QQ^\dagger||$, we have

$$\begin{aligned} QQ^\dagger &= |1\rangle\langle 1| \otimes \sum_i O_i, \\ Q^\dagger Q &= \sum_{ij} |i\rangle\langle j| \otimes O_i O_j \end{aligned} \tag{A.3}$$

Clearly $||QQ^\dagger|| = ||O_1 + \cdots + O_l||$, therefore, it is now the task to bound $||QQ^\dagger||$. We can write

$$Q^\dagger Q = \sum_i |i\rangle\langle i| \otimes O_i + \sum_{j=1}^{l-1} \sum_i |i\rangle\langle i \oplus j| \otimes O_i O_{i\oplus j} \tag{A.4}$$

where $\oplus$ denotes addition modulo l. This decomposition amounts to writing $Q^\dagger Q$ as a block diagonal matrix plus a sum of $l-1$ matrices, each with a block structure and containing only displaced diagonals (i.e. have the structure of a block permutation matrix).

The first term of the right had side of the above equation has operator norm

$$\Big|\Big| \sum_i |i\rangle\langle i| \otimes O_i \Big|\Big| = \max_i ||O_i|| = 1 \tag{A.5}$$

since the operator norm of a block diagonal operator is the maximal operator norm of any block, which in our case is unity. For each of the remaining terms we can use the fact that the operator norm, being equal to the largest singular value, is invariant under the transformation $Q \to UQV$ where U and V are unitary operators. Choosing $U = \mathbb{1} \otimes \mathbb{1}$ and $V_j = \sum_i |i \oplus j\rangle \otimes \mathbb{1}$, we see that

$$U \sum_i |i \oplus j\rangle \otimes O_i O_{i\oplus j} V_j = \sum_i |i\rangle\langle i| \otimes O_i O_{i\oplus j} \tag{A.6}$$

and thus

$$\Big|\Big| \sum_i |i\rangle\langle i \oplus j| \otimes O_i O_{i\oplus j} \Big|\Big| = \max_i ||O_i O_{i\oplus j}|| \tag{A.7}$$

again due to the block structure of the transformed matrix. Since $\max_i ||O_i O_{i\oplus j}|| \leq \max_{i,j>1} ||O_i O_{i\oplus j}|| = \cos\phi$, we can place the same bound $\cos\phi$ on each of the $l-1$ terms. Finally by using repeatedly the triangle inequality we obtain

$$||O_1 + \ldots + O_l|| \leq 1 + (l-1)\cos\phi, \tag{A.8}$$

Appendix B

Calculation for threshold error probability

Consider a lossy channel, with T the transmittance of the channel, defined as $T = 10^{-\alpha L/10}$, $\alpha = 0.2dB/km$. Let there be d detectors, with η be the detector efficiency, V be the visibility of the detection and p_{dark} the dark-count probability per detector then,

I When sending m-copies, the probability that at-least one copy reaches one of the detector is $(1-(1-T)^m)$ and the probability that no signal reaches the detector is $(1-T)^m$.

II The probability that there is click due to signal in a detector is

$$P[\text{click due to signal}] = \Big(\sum_{i=1}^{m} C_i^m (T\eta)^i (1-T\eta)^{m-i}\Big). \tag{B.1}$$

The probability that the signal is detected correctly in a good detector is

$$P[\text{click due to signal in a good detector}] = \Big(\sum_{i=1}^{m} C_i^m (T\eta)^i (1-T\eta)^{m-i}.V^i\Big). \tag{B.2}$$

Similarly, the probability that the signal is detected correctly in the bad detectors

$$P[\text{click due to signal in bad detectors}] = \Big(\sum_{i=1}^{m} C_i^m (T\eta)^i (1-T\eta)^{m-i}.(1-V^i)\Big) \tag{B.3}$$

III Since there are d detectors the probability of click in k detectors due to dark counts is

$$P[\text{click in } k \text{ detectors due to dark count}] = C_k^d (p_{dark})^k (1-p_{dark})^{d-k} \tag{B.4}$$

Which for $k=1$ is $(d)p_{dark}(1-p_{dark})^{d-1} \approx dp_{dark}$ for $p_{dark} << 1$, and the probability that there is no click due to dark count is, $(1-p_{dark})^d$. Thus, the probability that there is click in a good detector due to dark counts is

$$P[\text{click in good detector due to dark count}] = (d)p_{dark}\frac{1}{(d)} = p_{dark}. \tag{B.5}$$

Similarly, the probability that there is click in the bad detectors due to dark counts is

$$P[\text{click in bad detector due to dark count}] = (d)p_{dark}\frac{d-1}{(d)} = (d-1).p_{dark}. \tag{B.6}$$

IV Probability that there is a click in the detector is

$$\begin{aligned} P[\text{click}] &= P[\text{click due to signal}] \times P[\text{click in a detector due to dark count}] \\ &= \Big(\sum_{i=1}^{m} C_i^m (T\eta)^i (1-T\eta)^{m-i}\Big) \times dp_{dark} \end{aligned} \tag{B.7}$$

Let P_{right} is the probability that there is a click in a detector and is correctly detected, while, P_{wrong} the probability that there is a click in a detector and an error in detection. Then, the probability P_{right} is then the sum of three different events

$$\begin{aligned} P_{right} =& P[\text{click due to signal in good detector and no click due to dark counts}] \\ &+ P[\text{no click due to signal and there is click due to dark count in a good detector}] \\ &+ P[\text{click due to signal in good detector and click due to dark count in a good detector}] \\ =& \Big(\sum_{i=1}^{m} C_i^m (T\eta)^i (1-T\eta)^{m-i}.V^i\Big)(1-p_{dark})^d + (1-T\eta)^m p_{dark} \\ &+ \Big(\sum_{i=1}^{m} C_i^m (T\eta)^i (1-T\eta)^{m-i}.V^i\Big)p_{dark} \end{aligned} \tag{B.8}$$

Similarly, the probability p_{wrong} is the sum of three different events

$$\begin{aligned} P_{wrong} =& P[\text{click due to signal in bad detector and no click due to dark counts}] \\ &+ P[\text{no click due to signal and there is click due to dark count in bad detectors}] \\ &+ P[\text{click due to signal in bad detector and click due to dark count in bad detectors}] \\ =& \Big(\sum_{i=1}^{m} C_i^m (T\eta)^i (1-T\eta)^{m-i}.(1-V^i)\Big)(1-p_{dark})^d + (1-T\eta)^m (d-1)p_{dark} \\ &+ \Big(\sum_{i=1}^{m} C_i^m (T\eta)^i (1-T\eta)^{m-i}.(1-V^i)\Big)(d-1)p_{dark} \end{aligned} \tag{B.9}$$

Let, p_c be the probability that there is a correct detection given that there is a click in detector, and let, p_e be the probability that there is a wrong detection given that there is a click in detector, then

$$p_c = \frac{P_{right}}{P[\text{click}]} \tag{B.10}$$

$$p_e = \frac{P_{wrong}}{P[\text{click}]} \tag{B.11}$$

Bibliography

[ABB+05] A. Acín, E. Bagan, M. Baig, Ll. Masanes, and R. Muñoz Tapia. Multiple-copy two-state discrimination with individual measurements. *Phys. Rev. A*, 71:032338, Mar 2005.

[ABB+14] R. Alléaume, C. Branciard, J. Bouda, T. Debuisschert, M. Dianati, N. Gisin, M. Godfrey, P. Grangier, T. Länger, N. Lütkenhaus, Christian Monyk, P. Painchault, M. Peev, A. Poppe, T. Pornin, J. Rarity, R. Renner, G. Ribordy, M. Riguidel, L. Salvail, A. Shields, H. Weinfurter, and A. Zeilinger. Using quantum key distribution for cryptographic purposes: A survey. *Theor. Comput. Sci.*, 560:62–81, 2014.

[ABG+07] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 98:230501, Jun 2007.

[ACB+18] M H Abobeih, J Cramer, M A Bakker, N Kalb, M Markham, D J Twitchen, and T H Taminiau. One-second coherence for a single electron spin coupled to a multi-qubit nuclear-spin environment. *Nature communications*, 9(1):2552–2552, 06 2018.

[AF04] R Alicki and M Fannes. Continuity of quantum conditional information. *Journal of Physics A: Mathematical and General*, 37(5):L55–L57, jan 2004.

[AKBH07] Irfan Ali-Khan, Curtis J. Broadbent, and John C. Howell. Large-alphabet quantum key distribution using energy-time entangled bipartite states. *Phys. Rev. Lett.*, 98:060503, Feb 2007.

[All15] Romain Alléaume. A hybrid security model for quantum cryptography allowing to design practical schemes for long-distance key distribution with everlasting security. In *QCrypt 2015*, 2015.

[AM16] Antonio Acín and Lluis Masanes. Certified randomness in quantum physics. *Nature*, 540(7632):213–219, 2016.

[ANS20] ANSSI. Should quantum key distribution be used for secure communications?, 2020.

[ANSV08] K. M. R. Audenaert, M. Nussbaum, A. Szkoła, and F. Verstraete. Asymptotic error rates in quantum hypothesis testing. *Communications in Mathematical Physics*, 279(1):251–283, 2008.

[AW02] R. Ahlswede and A. Winter. Strong converse for identification via quantum channels. *IEEE Trans. Inf. Theory*, 48:569–579, 2002.

[BB14] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, 2014. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[BBCM95a] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer. Generalized privacy amplification. *IEEE Trans. Inf. Theory*, 41:1915–1923, 1995.

[BBCM95b] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer. Generalized privacy amplification. *IEEE Trans. Inf. Theory*, 41:1915–1923, 1995.

[BBR+18] Alberto Boaron, Gianluca Boso, Davide Rusca, Cédric Vulliez, Claire Autebert, Misael Caloz, Matthieu Perrenoud, Gaëtan Gras, Félix Bussières, Ming-Jun Li, Daniel Nolan, Anthony Martin, and Hugo Zbinden. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.*, 121:190502, Nov 2018.

[BBRV02] S. Bandyopadhyay, P. Boykin, V. Roychowdhury, and F. Vatan. A new proof for the existence of mutually unbiased bases. *Algorithmica*, 34:512–528, 2002.

[BBV+14] Erwan Bimbard, Rajiv Boddeda, Nicolas Vitrant, Andrey Grankin, Valentina Parigi, Jovica Stanojevic, Alexei Ourjoumtsev, and Philippe Grangier. Homodyne tomography of a single photon retrieved on demand from a cavity-enhanced cold atom memory. *Phys. Rev. Lett.*, 112:033601, Jan 2014.

[BCWP13] P. Blanche, D. Carothers, J. Wissinger, and N. Peyghambarian. Digital micromirror device as a diffractive reconfigurable optical switch for telecommunication. *Journal of Micro/Nanolithography, MEMS, and MOEMS*, 13, 2013.

[BDCZ98] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller. Quantum repeaters: The role of imperfect local operations in quantum communication. *Phys. Rev. Lett.*, 81:5932–5935, Dec 1998.

[Ber] D. Bernstein. Cost-benefit analysis of quantum cryptography.

[Ber09] Daniel J Bernstein. Introduction to post-quantum cryptography. In *Post-quantum cryptography*, pages 1–14. Springer, 2009.

[BFW14] M. Berta, Omar Fawzi, and S. Wehner. Quantum to classical randomness extractors. *IEEE Transactions on Information Theory*, 60:1168–1192, 2014.

[BHE+18] Frédéric Bouchard, Khabat Heshami, Duncan England, Robert Fickler, Robert W. Boyd, Berthold-Georg Englert, Luis L. Sánchez-Soto, and Ebrahim Karimi. Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons. *Quantum*, 2:111, December 2018.

[BHK05] Jonathan Barrett, Lucien Hardy, and Adrian Kent. No signaling and quantum key distribution. *Phys. Rev. Lett.*, 95:010503, Jun 2005.

[BMF+16] Kamil Brádler, Mohammad Mirhosseini, Robert Fickler, Anne Broadbent, and Robert Boyd. Finite-key security analysis for multilevel quantum key distribution. *New Journal of Physics*, 18(7):073030, Jul 2016.

[BP06] H. Bechmann-Pasquinucci. Eavesdropping without quantum memory. *Phys. Rev. A*, 73:044305, Apr 2006.

[BP12] Samuel L. Braunstein and Stefano Pirandola. Side-channel-free quantum key distribution. *Phys. Rev. Lett.*, 108:130502, Mar 2012.

[BR05] Mihir Bellare and Phillip Rogaway. *Introduction to Modern Cryptography*. 2005.

[BRR13] G. Brassard and Paul Raymond-Robichaud. Can free will emerge from determinism in quantum theory. *arXiv: Quantum Physics*, pages 41–61, 2013.

[BRR17] G. Brassard and Paul Raymond-Robichaud. The equivalence of local-realistic and no-signalling theories. *arXiv: Quantum Physics*, 2017.

[BRR19] Gilles Brassard and Paul Raymond-Robichaud. Parallel lives: A local-realistic interpretation of "nonlocal" boxes. *Entropy*, 21(1):87, Jan 2019.

[BRSD11] Harry Buhrman, Oded Regev, Giannicola Scarpa, and Ronald De Wolf. Near-optimal and explicit bell inequality violations. In *Proceedings - 26th Annual IEEE Conference on Computational Complexity, CCC 2011*, Proceedings of the Annual IEEE Conference on Computational Complexity, pages 157–166, 2011. 26th Annual IEEE Conference on Computational Complexity, CCC 2011 ; Conference date: 08-06-2011 Through 10-06-2011.

[Bru98] Dagmar Bruß. Optimal eavesdropping in quantum cryptography with six states. *Phys. Rev. Lett.*, 81:3018–3021, Oct 1998.

[BS15] Anne Broadbent and Christian Schaffner. Quantum cryptography beyond quantum key distribution. *Designs, Codes and Cryptography*, 78(1):351–382, Dec 2015.

[BS19] Zvika Brakerski and Omri Shmueli. (pseudo) random quantum states with binary phase. *ArXiv*, abs/1906.10611, 2019.

[BW18] Kamil Brádler and Christian Weedbrook. Security proof of continuous-variable quantum key distribution using three coherent states. *Phys. Rev. A*, 97:022310, Feb 2018.

[BYJK08] Ziv Bar-Yossef, T. S. Jayram, and Iordanis Kerenidis. Exponential separation of quantum and classical one-way communication complexity. *SIAM Journal on Computing*, 38(1):366–384, 2008.

[BZ07] I. Bengtsson and K. Zyczkowski. *Geometry of Quantum States: An Introduction to Quantum Entanglement*. Cambridge University Press, 2007.

[CBKG02a] Nicolas J Cerf, Mohamed Bourennane, Anders Karlsson, and Nicolas Gisin. Security of quantum key distribution using d-level systems. *Physical review letters*, 88(12):127902, 2002.

[CBKG02b] Nicolas J. Cerf, Mohamed Bourennane, Anders Karlsson, and Nicolas Gisin. Security of quantum key distribution using d-level systems. *Phys. Rev. Lett.*, 88:127902, Mar 2002.

[CCE+16a] Y.-W. Cho, G. T. Campbell, J. L. Everett, J. Bernu, D. B. Higginbottom, M. T. Cao, J. Geng, N. P. Robins, P. K. Lam, and B. C. Buchler. Highly efficient optical quantum memory with long coherence time in cold atoms. *Optica*, 3(1):100–107, Jan 2016.

[CCE+16b] Y.-W. Cho, G. T. Campbell, J. L. Everett, J. Bernu, D. B. Higginbottom, M. T. Cao, J. Geng, N. P. Robins, P. K. Lam, and B. C. Buchler. Highly efficient optical quantum memory with long coherence time in cold atoms. *Optica*, 3(1):100–107, Jan 2016.

[CFL+14] L. C. Comandar, B. Fröhlich, M. Lucamarini, K. A. Patel, A. W. Sharpe, J. F. Dynes, Z. L. Yuan, R. V. Penty, and A. J. Shields. Room temperature single-photon detectors for high bit rate quantum key distribution. *Applied Physics Letters*, 104(2):021101, 2014.

[CHT18] Claudio Carmeli, Teiko Heinosaari, and Alessandro Toigo. State discrimination with postmeasurement information and incompatibility of quantum measurements. *Phys. Rev. A*, 98:012126, Jul 2018.

[CHZ+16] Kenan Cicek, Ziyang Hu, Jiangbo Zhu, Laura Meriggi, Shimao Li, Zhichao Nong, Shengqian Gao, Ning Zhang, Xuyang Wang, Xinlun Cai, Marc Sorel, and Siyuan Yu. Integrated optical vortex beam receivers. *Opt. Express*, 24(25):28529–28539, Dec 2016.

[CK78a] I. Csiszár and J. Körner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, 24:339–348, 1978.

[CK78b] Imre Csiszár and Janos Korner. Broadcast channels with confidential messages. *IEEE transactions on information theory*, 24(3):339–348, 1978.

[CLF+16] L. C. Comandar, M. Lucamarini, B. Fröhlich, J. F. Dynes, A. W. Sharpe, S. W. B. Tam, Z. L. Yuan, R. V. Penty, and A. J. Shields. Quantum key distribution without detector vulnerabilities using optically seeded lasers. *Nature Photonics*, 10(5):312–315, 2016.

[CLW+13] Yi-Hsin Chen, Meng-Jung Lee, I-Chung Wang, Shengwang Du, Yong-Fan Chen, Ying-Cheng Chen, and Ite A. Yu. Coherent optical memory with high storage efficiency and large fractional delay. *Phys. Rev. Lett.*, 110:083601, Feb 2013.

[CM97a] Christian Cachin and Ueli Maurer. Unconditional security against memory-bounded adversaries. In *Annual International Cryptology Conference*, pages 292–306. Springer, 1997.

[CM97b] Christian Cachin and Ueli M. Maurer. Linking information reconciliation and privacy amplification. *J. Cryptol.*, 10(2):97–110, mar 1997.

[CMnTM+08] J. Calsamiglia, R. Muñoz Tapia, Ll. Masanes, A. Acin, and E. Bagan. Quantum chernoff bound as a measure of distinguishability between density matrices: Application to qubit and gaussian states. *Phys. Rev. A*, 77:032311, Mar 2008.

[CT06] T.M. Cover and J.A. Thomas. *Elements of Information Theory*. Wiley, 2006.

[CW79a] L. Carter and M. Wegman. Universal classes of hash functions. *J. Comput. Syst. Sci.*, 18:143–154, 1979.

[CW79b] L. Carter and M. Wegman. Universal classes of hash functions. *J. Comput. Syst. Sci.*, 18:143–154, 1979.

[DBD+17] Yunhong Ding, Davide Bacco, Kjeld Dalgaard, Xinlun Cai, Xiaoqi Zhou, Karsten Rottwitt, and Leif Katsuo Oxenløwe. High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits. *npj Quantum Information*, 3(1):1–7, 2017.

[DFSS05] I.B. Damgard, S. Fehr, L. Salvail, and C. Schaffner. Cryptography in the bounded quantum-storage model. pages 449–458, 2005.

[DFSS08] Ivan B Damgård, Serge Fehr, Louis Salvail, and Christian Schaffner. Cryptography in the bounded-quantum-storage model. *SIAM Journal on Computing*, 37(6):1865–1890, 2008.

[DFW14] Frederic Dupuis, Omar Fawzi, and Stephanie Wehner. Entanglement sampling and applications. *IEEE Transactions on Information Theory*, 61(2):1093–1112, 2014.

[DH00] David Deutsch and Patrick Hayden. Information flow in entangled quantum systems. *Proceedings of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, 456(1999):1759–1774, Jul 2000.

[DHL+04] David P. DiVincenzo, Michał Horodecki, Debbie W. Leung, John A. Smolin, and Barbara M. Terhal. Locking classical correlations in quantum states. *Phys. Rev. Lett.*, 92:067902, Feb 2004.

[DLQY16] Eleni Diamanti, Hoi-Kwong Lo, Bing Qi, and Zhiliang Yuan. Practical challenges in quantum key distribution. *npj Quantum Information*, 2(1), Nov 2016.

[DM04] Stefan Dziembowski and Ueli Maurer. On generating the initial key in the bounded-storage model. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 126–137. Springer, 2004.

[DS13] M. H. Devoret and R. J. Schoelkopf. Superconducting circuits for quantum information: An outlook. *Science*, 339(6124):1169–1174, 2013.

[EFKZ17] Manuel Erhard, Robert Fickler, Mario Krenn, and Anton Zeilinger. Twisted photons: new quantum perspectives in high dimensions. *Light: Science & Applications*, 7(3):17146–17146, Oct 2017.

[Eke91] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.

[ENG+14] C. Erven, N. Ng, N. Gigov, R. Laflamme, S. Wehner, and G. Weihs. An experimental implementation of oblivious transfer in the noisy storage model. *Nature Communications*, 5(1):3418, 2014.

[ER14] Artur Ekert and Renato Renner. The ultimate physical limits of privacy. *Nature*, 507(7493):443–447, 2014.

[EVGC+18] J. L. Everett, P. Vernaz-Gris, G. T. Campbell, A. D. Tranter, K. V. Paul, A. C. Leung, P. K. Lam, and B. C. Buchler. Time-reversed and coherently enhanced memory: A single-mode quantum atom-optic memory without a cavity. *Phys. Rev. A*, 98:063846, Dec 2018.

[FGS+18a] 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(1):1450, 2018.

[FGS+18b] 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(1):1450, 2018.

[FHS13] Omar Fawzi, Patrick Hayden, and Pranab Sen. From low-distortion norm embeddings to explicit uncertainty relations and efficient information locking. *J. ACM*, 60(6), November 2013.

[FHT03] A. A. Fedotov, P. Harremoës, and F. Topsøe. Refinements of pinsker's inequality. *IEEE Trans. Inf. Theory*, 49:1491–1498, 2003.

[FLD+17] Bernd Fröhlich, Marco Lucamarini, James F. Dynes, Lucian C. Comandar, Winci W.-S. Tam, Alan Plews, Andrew W. Sharpe, Zhiliang Yuan, and Andrew J. Shields. Long-distance quantum key distribution secure against coherent attacks. *Optica*, 4(1):163–167, Jan 2017.

[Fur14] Fabian Furrer. Reverse-reconciliation continuous-variable quantum key distribution based on the uncertainty principle. *Physical Review A*, 90(4), Oct 2014.

[Gav09] Dmitry Gavinsky. Classical interaction cannot replace quantum nonlocality, 2009.

[GB01] Shafi Goldwasser and Mihir Bellare. Lecture notes in cryptography, 2001.

[GDL19] Shouvik Ghorai, Eleni Diamanti, and Anthony Leverrier. Composable security of two-way continuous-variable quantum key distribution without active symmetrization. *Physical Review A*, 99(1), Jan 2019.

[GG01] Frédéric Grosshans and Philippe Grangier. Quantum cloning and teleportation criteria for continuous quantum variables. *Phys. Rev. A*, 64:010301, Jun 2001.

[GG02a] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88:057902, Jan 2002.

[GG02b] Frédéric Grosshans and Philippe Grangier. Reverse reconciliation protocols for quantum cryptography with continuous variables. *arXiv: Quantum Physics*, 2002.

[GHK+14a] Saikat Guha, Patrick Hayden, Hari Krovi, Seth Lloyd, Cosmo Lupo, Jeffrey H. Shapiro, Masahiro Takeoka, and Mark M. Wilde. Quantum enigma machines and the locking capacity of a quantum channel. *Phys. Rev. X*, 4:011016, Jan 2014.

[GHK+14b] Saikat Guha, Patrick Hayden, Hari Krovi, Seth Lloyd, Cosmo Lupo, Jeffrey H Shapiro, Masahiro Takeoka, and Mark M Wilde. Quantum enigma machines and the locking capacity of a quantum channel. *Physical Review X*, 4(1):011016, 2014.

[GKK+07] Dmitry Gavinsky, J. Kempe, Iordanis Kerenidis, R. Raz, and R. D. Wolf. Exponential separations for one-way quantum communication complexity, with applications to cryptography. In *STOC '07*, 2007.

[GKR] M. Grassl, A. Klappenecker, and M. Rotteler. Graphs, quadratic forms, and quantum codes. *Proceedings IEEE International Symposium on Information Theory,*.

[GKRW06] Dmitry Gavinsky, J. Kempe, O. Regev, and R. D. Wolf. Bounded-error quantum state identification and exponential separations in communication complexity. In *STOC '06*, 2006.

[Gol09] Oded Goldreich. *Foundations of cryptography: volume 2, basic applications*. Cambridge university press, 2009.

[GVW+15] Marissa Giustina, Marijn A. M. Versteegh, Sören Wengerowsky, Johannes Handsteiner, Armin Hochrainer, Kevin Phelan, Fabian Steinlechner, Johannes Kofler, Jan-Åke Larsson, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Morgan W. Mitchell, Jörn Beyer, Thomas Gerrits, Adriana E. Lita, Lynden K. Shalm, Sae Woo Nam, Thomas Scheidl, Rupert Ursin, Bernhard Wittmann, and Anton Zeilinger. Significant-loophole-free test of bell's theorem with entangled photons. *Phys. Rev. Lett.*, 115:250401, Dec 2015.

[GW10] Deepthi Gopal and Stephanie Wehner. Using postmeasurement information in state discrimination. *Phys. Rev. A*, 82:022326, Aug 2010.

[Hat03] Lynn Hathaway. National policy on the use of the advanced encryption standard (aes) to protect national security systems and national security information. *National Security Agency*, 23, 2003.

[Hay16] M. Hayashi. *Quantum Information Theory: Mathematical Foundation*. Graduate Texts in Physics. Springer Berlin Heidelberg, 2016.

[HBD+15] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenberg, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, 2015.

[HEK+20] Adrian Holzäpfel, Jean Etesse, Krzysztof T Kaczmarek, Alexey Tiranov, Nicolas Gisin, and Mikael Afzelius. Optical storage for 0.53 s in a solid-state atomic frequency comb memory using dynamical decoupling. *New Journal of Physics*, 22(6):063009, jun 2020.

[Hel76] *Quantum Detection and Estimation Theory*. ISSN. Elsevier Science, 1976.

[HHL+15] Duan Huang, Peng Huang, Dakai Lin, Chao Wang, and Guihua Zeng. High-speed continuous-variable quantum key distribution without sending a local oscillator. *Opt. Lett.*, 40(16):3695–3698, Aug 2015.

[HIGM95] B. Huttner, N. Imoto, N. Gisin, and T. Mor. Quantum cryptography with coherent states. *Phys. Rev. A*, 51:1863–1869, Mar 1995.

[HL06] Matthias Heid and Norbert Lütkenhaus. Efficiency of coherent-state quantum cryptography in the presence of loss: Influence of realistic error correction. *Phys. Rev. A*, 73:052316, May 2006.

[HLSW04] Patrick Hayden, Debbie Leung, Peter W. Shor, and Andreas Winter. Randomizing quantum states: Constructions and applications. *Communications in Mathematical Physics*, 250(2):371–391, 2004.

[HLW+15] Duan Huang, Dakai Lin, Chao Wang, Weiqi Liu, Shuanghong Fang, Jinye Peng, Peng Huang, and Guihua Zeng. Continuous-variable quantum key distribution with 1 mbps secure key rate. *Opt. Express*, 23(13):17511–17519, Jun 2015.

[HN06] Danny Harnik and Moni Naor. On everlasting security in the ¡i¿hybrid¡/i¿ bounded storage model. In *Proceedings of the 33rd International Conference on Automata, Languages and Programming - Volume Part II*, ICALP'06, page 192–203, Berlin, Heidelberg, 2006. Springer-Verlag.

[Hol12] Alexander S. Holevo. *Quantum Systems, Channels, Information: A Mathematical Introduction*. De Gruyter, 2012.

[HSQ+15] Sangyoon Han, Tae Joon Seok, Niels Quack, Byung-Wook Yoo, and Ming C. Wu. Large-scale silicon photonic switches with movable directional couplers. *Optica*, 2(4):370–375, Apr 2015.

[Hwa03] Won-Young Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys. Rev. Lett.*, 91:057901, Aug 2003.

[ILC+17] Nurul T. Islam, Charles Ci Wen Lim, Clinton Cahall, Jungsang Kim, and Daniel J. Gauthier. Provably secure and high-rate quantum key distribution with time-bin qudits. *Science Advances*, 3(11):e1701491, Nov 2017.

[JKJL+13] 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(5):378–381, 2013.

[JLS18] Zhengfeng Ji, Yi-Kai Liu, and Fang Song. Pseudorandom quantum states. Cryptology ePrint Archive, Report 2018/544, 2018. https://ia.cr/2018/544.

[JPLS19] Yonggi Jo, Hee Park, Seung-Woo Lee, and Wonmin Son. Efficient high-dimensional quantum key distribution with hybrid encoding. *Entropy*, 21(1):80, Jan 2019.

[KKL88] J. Kahn, G. Kalai, and N. Linial. The influence of variables on boolean functions. *[Proceedings 1988] 29th Annual Symposium on Foundations of Computer Science*, pages 68–80, 1988.

[KL14] J. Katz and Y. Lindell. *Introduction to Modern Cryptography, Second Edition*. Chapman & Hall/CRC Cryptography and Network Security Series. Taylor & Francis, 2014.

[KPN+09] Ebrahim Karimi, Bruno Piccirillo, Eleonora Nagali, Lorenzo Marrucci, and Enrico Santamato. Efficient generation and sorting of orbital angular momentum eigenmodes of light by thermally tuned q-plates. *Applied Physics Letters*, 94(23):231124, 2009.

[KRBM07] Robert König, Renato Renner, Andor Bariska, and Ueli Maurer. Small accessible quantum information does not imply security. *Phys. Rev. Lett.*, 98:140502, Apr 2007.

[KRRR15] Norbert Kalb, Andreas Reiserer, Stephan Ritter, and Gerhard Rempe. Heralded storage of a photonic quantum bit in a single atom. *Phys. Rev. Lett.*, 114:220501, Jun 2015.

[KRT09] Julia Kempe, Oded Regev, and Ben Toner. Unique games with entangled provers are easy, 2009.

[KV13] Subhash A. Khot and Nisheeth K. Vishnoi. The unique games conjecture, integrality gap for cut problems and embeddability of negative type metrics into ℓ_1, 2013.

[KWW12a] R. Konig, S. Wehner, and J. Wullschleger. Unconditional security from noisy quantum storage. *IEEE Trans. Inf. Theor.*, 58(3):1962–1984, March 2012.

[KWW12b] Robert Konig, Stephanie Wehner, and Jürg Wullschleger. Unconditional security from noisy quantum storage. *IEEE Transactions on Information Theory*, 58(3):1962–1984, 2012.

[LÖ0] Norbert Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Phys. Rev. A*, 61:052304, Apr 2000.

[LBZ+16a] Catherine Lee, Darius Bunandar, Zheshen Zhang, Gregory R. Steinbrecher, P. Ben Dixon, Franco N. C. Wong, Jeffrey H. Shapiro, Scott A. Hamilton, and Dirk Englund. High-rate field demonstration of large-alphabet quantum key distribution, 2016.

[LBZ+16b] Catherine Lee, Darius Bunandar, Zheshen Zhang, Gregory R. Steinbrecher, P. Ben Dixon, Franco N. C. Wong, Jeffrey H. Shapiro, Scott A. Hamilton, and Dirk Englund. High-rate field demonstration of large-alphabet quantum key distribution, 2016.

[LBZ+19] Catherine Lee, Darius Bunandar, Zheshen Zhang, Gregory R. Steinbrecher, P. Ben Dixon, Franco N. C. Wong, Jeffrey H. Shapiro, Scott A. Hamilton, and Dirk Englund. Large-alphabet encoding for higher-rate quantum key distribution. *Opt. Express*, 27(13):17539–17549, Jun 2019.

[LCQ12] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 108:130503, Mar 2012.

[LCW+10] Yang Liu, Teng-Yun Chen, Jian Wang, Wen-Qi Cai, Xu Wan, Luo-Kan Chen, Jin-Hong Wang, Shu-Bin Liu, Hao Liang, Lin Yang, Cheng-Zhi Peng, Kai Chen, Zeng-Bing Chen, and Jian-Wei Pan. Decoy-state quantum key distribution with polarized photons over 200 km. *Opt. Express*, 18(8):8587–8594, Apr 2010.

[LG09] Anthony Leverrier and Philippe Grangier. Unconditional security proof of long-distance continuous-variable quantum key distribution with discrete modulation. *Phys. Rev. Lett.*, 102:180504, May 2009.

[LG11] Anthony Leverrier and Philippe Grangier. Continuous-variable quantum-key-distribution protocols with a non-gaussian modulation. *Phys. Rev. A*, 83:042312, Apr 2011.

[LGG10] Anthony Leverrier, Frédéric Grosshans, and Philippe Grangier. Finite-size analysis of a continuous-variable quantum key distribution. *Physical Review A*, 81(6), Jun 2010.

[LHA+16] Daniel J Lum, John C Howell, MS 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(2):022315, 2016.

[LL14] Cosmo Lupo and Seth Lloyd. Quantum-locked key distribution at nearly the classical capacity rate. *Phys. Rev. Lett.*, 113:160502, Oct 2014.

[LL15a] Cosmo Lupo and Seth Lloyd. Continuous-variable quantum enigma machines for long-distance key distribution. *Phys. Rev. A*, 92:062312, Dec 2015.

[LL15b] Cosmo Lupo and Seth Lloyd. Quantum data locking for high-rate private communication. *New Journal of Physics*, 17(3):033022, mar 2015.

[LL15c] Cosmo Lupo and Seth Lloyd. Quantum data locking for high-rate private communication. *New Journal of Physics*, 17(3):033022, mar 2015.

[LL15d] Cosmo Lupo and Seth Lloyd. Quantum data locking for high-rate private communication. *New Journal of Physics*, 17(3):033022, 2015.

[LLTG18] Yen-Yu Lai, Guin-Dar Lin, Jason Twamley, and Hsi-Sheng Goan. Single-nitrogen-vacancy-center quantum memory for a superconducting flux qubit mediated by a ferromagnet. *Phys. Rev. A*, 97:052303, May 2018.

[LMC05] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504, Jun 2005.

[LMR+11] M. Lettner, M. Mücke, S. Riedl, C. Vo, C. Hahn, S. Baur, J. Bochmann, S. Ritter, S. Dürr, and G. Rempe. Remote entanglement between a single atom and a bose-einstein condensate. *Phys. Rev. Lett.*, 106:210503, May 2011.

[LPD+13] M. Lucamarini, K. A. Patel, J. F. Dynes, B. Fröhlich, A. W. Sharpe, A. R. Dixon, Z. L. Yuan, R. V. Penty, and A. J. Shields. Efficient decoy-state quantum key distribution with quantified security. *Opt. Express*, 21(21):24550–24565, Oct 2013.

[Lup15] Cosmo Lupo. Quantum data locking for secure communication against an eavesdropper with time-limited storage. *Entropy*, 17(5):3194–3204, 2015.

[LWW+10] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 4:686–689, 2010.

[LYDS18] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature*, 557(7705):400–403, 2018.

[LZS+14] Catherine Lee, Zheshen Zhang, Gregory R. Steinbrecher, Hongchao Zhou, Jacob Mower, Tian Zhong, Ligong Wang, Xiaolong Hu, Robert D. Horansky, Varun B. Verma, Adriana E. Lita, Richard P. Mirin, Francesco Marsili, Matthew D. Shaw, Sae Woo Nam, Gregory W. Wornell, Franco N. C. Wong, Jeffrey H. Shapiro, and Dirk Englund. Entanglement-based quantum communication secured by nonlocal dispersion cancellation. *Phys. Rev. A*, 90:062331, Dec 2014.

[Mau93a] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE Trans. Inf. Theor.*, 39(3):733–742, May 1993.

[Mau93b] U.M. Maurer. Secret key agreement by public discussion from common information. *IEEE Transactions on Information Theory*, 39(3):733–742, 1993.

[MCG] D. MCGrew. Living with post q cryptography. *PQC2015*.

[MDCAF20] Tony Metger, Yfke Dulek, Andrea Coladangelo, and Rotem Arnon-Friedman. Device-independent quantum key distribution from computational assumptions. *arXiv preprint arXiv:2010.04175*, 2020.

[MDG+13] Mhlambululi Mafu, Angela Dudley, Sandeep Goyal, Daniel Giovannini, Melanie McLaren, Miles J. Padgett, Thomas Konrad, Francesco Petruccione, Norbert Lütkenhaus, and Andrew Forbes. Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases. *Physical Review A*, 88(3), Sep 2013.

[ML] Romain Alléaume Christopher Chunnilall Ivo Pietro Degiovanni Marco Gramegna Atilla Hasekioglu Bruno Huttner Rupesh Kumar Andrew Lord Norbert Lütkenhaus Vadim Makarov Vicente Martin Alan Mink Momtchil Peev Masahide Sasaki Alastair Sinclair Tim Spiller Martin Ward Catherine White Zhiliang Yuan Marco Lucamarini, Andrew Shields. Implementation security of quantum cryptography. *ETS White Paper*.

[MMKP03] D.J.C. MacKay, J.C. MacKay, D.J.C.M. Kay, and Cambridge University Press. *Information Theory, Inference and Learning Algorithms*. Cambridge University Press, 2003.

[MMLO+15a] Mohammad Mirhosseini, Omar S Magaña-Loaiza, Malcolm N O'Sullivan, Brandon Rodenburg, Mehul Malik, Martin P J Lavery, Miles J Padgett, Daniel J Gauthier, and Robert W Boyd. High-dimensional quantum cryptography with twisted light. *New Journal of Physics*, 17(3):033033, Mar 2015.

[MMLO+15b] Mohammad Mirhosseini, Omar S Magaña-Loaiza, Malcolm N O'Sullivan, Brandon Rodenburg, Mehul Malik, Martin P J Lavery, Miles J Padgett, Daniel J Gauthier, and Robert W Boyd. High-dimensional quantum cryptography with twisted light. *New Journal of Physics*, 17(3):033033, Mar 2015.

[Mou16] Nima Mousavi. How tight is chernoff bound? 2016.

[MQZL05] Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo. Practical decoy state for quantum key distribution. *Phys. Rev. A*, 72:012326, Jul 2005.

[MU88] Hans Maassen and J. B. M. Uffink. Generalized entropic uncertainty relations. *Phys. Rev. Lett.*, 60:1103–1106, Mar 1988.

[MW99] U. Maurer and S. Wolf. Unconditionally secure key agreement and the intrinsic conditional information. *IEEE Trans. Inf. Theory*, 45:499–514, 1999.

[MW00] Ueli Maurer and Stefan Wolf. Information-theoretic key agreement: From weak to strong secrecy for free. In Bart Preneel, editor, *Advances in Cryptology — EUROCRYPT 2000*, pages 351–368, Berlin, Heidelberg, 2000. Springer Berlin Heidelberg.

[MY98] D. Mayers and A. Yao. Quantum cryptography with imperfect apparatus. In *Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No.98CB36280)*, pages 503–509, 1998.

[NAL90] J.A. Neff, R.A. Athale, and S.H. Lee. Two-dimensional spatial light modulators: a tutorial. *Proceedings of the IEEE*, 78(5):826–855, 1990.

[NCC00] M.A. Nielsen, I.L. Chuang, and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge Series on Information and the Natural Sciences. Cambridge University Press, 2000.

[NJCM+12] 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(1):1326, 2012.

[NS09] Michael Nussbaum and Arleta Szkoła. The chernoff lower bound for symmetric quantum hypothesis testing. *The Annals of Statistics*, 37(2):1040–1057, 2009.

[NTH+11] N. Namekata, H. Takesue, T. Honjo, Y. Tokura, and S. Inoue. High-rate quantum key distribution over 100 km using ultra-low-noise, 2-ghz sinusoidally gated ingaas/inp avalanche photodiodes. *Opt. Express*, 19(11):10632–10639, May 2011.

[NWS+13] J. Nunn, L. J. Wright, C. Söller, L. Zhang, I. A. Walmsley, and B. J. Smith. Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion. *Opt. Express*, 21(13):15959–15973, Jul 2013.

[O'D08] Ryan O'Donnell. Some topics in analysis of boolean functions. In *Proceedings of the Fortieth Annual ACM Symposium on Theory of Computing*, STOC '08, page 569–578, New York, NY, USA, 2008. Association for Computing Machinery.

[oqst] NCSC Whitepaper on quantum security technologies.

[OTW+18] Antonio Ortu, Alexey Tiranov, Sacha Welinski, Florian Fröwis, Nicolas Gisin, Alban Ferrier, Philippe Goldner, and Mikael Afzelius. Simultaneous coherence enhancement of optical and microwave transitions in solid-state electronic spins. *Nature Materials*, 17(8):671–675, 2018.

[PAB+20a] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden. Advances in quantum cryptography. *Adv. Opt. Photon.*, 12(4):1012–1236, Dec 2020.

[PAB+20b] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. L. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi, and P. Wallden. Advances in quantum cryptography. *Adv. Opt. Photon.*, 12(4):1012–1236, Dec 2020.

[PGPBL09] Stefano Pirandola, Raul García-Patrón, Samuel L. Braunstein, and Seth Lloyd. Direct and reverse secret-key capacities of a quantum channel. *Phys. Rev. Lett.*, 102:050503, Feb 2009.

[PJH+17] Benjamin Pingault, David-Dominik Jarausch, Christian Hepp, Lina Klintberg, Jonas N. Becker, Matthew Markham, Christoph Becher, and Mete Atatüre. Coherent control of the silicon-vacancy spin in diamond. *Nature Communications*, 8(1):15579, 2017.

[PL08] Stefano Pirandola and Seth Lloyd. Computable bounds for the discrimination of gaussian states. *Phys. Rev. A*, 78:012331, Jul 2008.

[PLL+09] Momtchil Peev, Thomas Länger, Thomas Lorünser, Andreas Happe, Oliver Maurhart, Andreas Poppe, and Thomas Themel. The secoqc quantum-key-distribution network in vienna. In *Optical Fiber Communication Conference and National Fiber Optic Engineers Conference*, page OThL2. Optical Society of America, 2009.

[PLOB17a] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8(1):15043, 2017.

[PLOB17b] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nature communications*, 8(1):1–15, 2017.

[PLWP18] Panagiotis Papanastasiou, Cosmo Lupo, Christian Weedbrook, and Stefano Pirandola. Quantum key distribution with phase-encoded coherent states: Asymptotic security analysis in thermal-loss channels. *Phys. Rev. A*, 98:012340, Jul 2018.

[PPS04] K. Paterson, F. Piper, and R. Schack. Quantum cryptography: a practical information security perspective. *IACR Cryptol. ePrint Arch.*, 2004:156, 2004.

[Pre15] J. Preskill. *Lecture Notes for Physics 229:Quantum Information and Computation*. CreateSpace Independent Publishing Platform, 2015.

[QFLM07] B. Qi, C. Fung, H. Lo, and Xiongfeng Ma. Time-shift attack in practical quantum cryptosystems. *Quantum Inf. Comput.*, 7:73–82, 2007.

[Qi06] Bing Qi. Single-photon continuous-variable quantum key distribution based on the energy-time uncertainty relation. *Opt. Lett.*, 31(18):2795–2797, Sep 2006.

[Ren05] R. Renner. Security of quantum key distribution. In *Ausgezeichnete Informatikdissertationen*, 2005.

[Ren08] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6(01):1–127, 2008.

[Ric03] S. Rickles. Symmetries in physics: Understanding permutation symmetry. *arXiv: Quantum Physics*, 2003.

[RNL+10] K. Reim, J. Nunn, V. Lorenz, B. Sussman, K. C. Lee, N. Langford, D. Jaksch, and I. Walmsley. Towards high-speed optical quantum memories. *Nature Photonics*, 4:218–221, 2010.

[RXH+14] Yongxiong Ren, G. Xie, H. Huang, N. Ahmed, Yan Yan, Long Li, C. Bao, M. Lavery, M. Tur, M. Neifeld, R. Boyd, J. Shapiro, and A. Willner. Adaptive-optics-based simultaneous pre- and post-turbulence compensation of multiple orbital-angular-momentum beams in a bidirectional free-space optical link. 2014.

[SAA+07] Thomas Symul, Daniel J. Alton, Syed M. Assad, Andrew M. Lance, Christian Weedbrook, Timothy C. Ralph, and Ping Koy Lam. Experimental demonstration of post-selection-based continuous-variable quantum key distribution in the presence of gaussian noise. *Phys. Rev. A*, 76:030303, Sep 2007.

[SAA+10] C Simmon, M Afzelius, J Appel, A Boyer de la Giroday, SJ Dewhurst, N Gisin, CY Hu, A Jelezko, S Kröll, JH Müller, et al. Quantum memories: A review based on the european integrated project ?qubit applications (qap)? *European Physical Journal D*, 58:1–22, 2010.

[SARG04] Valerio Scarani, Antonio Acín, Grégoire Ribordy, and Nicolas Gisin. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Phys. Rev. Lett.*, 92:057901, Feb 2004.

[Sas17] Masahide Sasaki. Quantum networks: where should we be heading? *Quantum Science and Technology*, 2(2):020501, apr 2017.

[SBF+17a] Alicia Sit, Frédéric Bouchard, Robert Fickler, Jérémie Gagnon-Bischoff, Hugo Larocque, Khabat Heshami, Dominique Elser, Christian Peuntinger, Kevin Günthner, Bettina Heim, Christoph Marquardt, Gerd Leuchs, Robert W. Boyd, and Ebrahim Karimi. High-dimensional intracity quantum cryptography with structured photons. *Optica*, 4(9):1006–1010, Sep 2017.

[SBF+17b] Alicia Sit, Frédéric Bouchard, Robert Fickler, Jérémie Gagnon-Bischoff, Hugo Larocque, Khabat Heshami, Dominique Elser, Christian Peuntinger, Kevin Günthner, Bettina Heim, Christoph Marquardt, Gerd Leuchs, Robert W. Boyd, and Ebrahim Karimi. High-dimensional intracity quantum cryptography with structured photons. *Optica*, 4(9):1006–1010, Sep 2017.

[SBPC+09] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, Sep 2009.

[SC07] Raul Garcia-Patron Sanchez and Nicolas J. Cerf. Quantum information with optical continuous variables: from bell tests to key distribution. 2007.

[Sch10] Christian Schaffner. Simple protocols for oblivious transfer and secure identification in the noisy-quantum-storage model. *Phys. Rev. A*, 82:032308, Sep 2010.

[SCW+14] Michael J. Strain, Xinlun Cai, Jianwei Wang, Jiangbo Zhu, David B. Phillips, Lifeng Chen, Martin Lopez-Garcia, Jeremy L. O'Brien, Mark G. Thompson, Marc Sorel, and Siyuan Yu. Fast electrical switching of orbital angular momentum modes using ultra-compact integrated vortex emitters. *Nature Communications*, 5, September 2014.

[SFI+11] 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. Tsurumaru, 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. *Opt. Express*, 19(11):10387–10409, May 2011.

[Sha49] C. E. Shannon. Communication theory of secrecy systems. *The Bell System Technical Journal*, 28(4):656–715, 1949.

[SHF+14] Kaoru Shimizu, Toshimori Honjo, Mikio Fujiwara, Toshiyuki Ito, Kiyoshi Tamaki, Shigehito Miki, Taro Yamashita, Hirotaka Terai, Zhen Wang, and Masahide Sasaki. Performance of long-distance quantum key distribution over 90-km optical links installed in a field environment of tokyo metropolitan area. *J. Lightwave Technol.*, 32(1):141–151, Jan 2014.

[SK14] V. Scarani and C. Kurtsiefer. The black paper of quantum cryptography: Real implementation problems. *Theor. Comput. Sci.*, 560:27–32, 2014.

[SMD+11] Sergei Slussarenko, Anatoli Murauski, Tao Du, Vladimir Chigrinov, Lorenzo Marrucci, and Enrico Santamato. Tunable liquid crystal q-plates with arbitrary topological charge. *Opt. Express*, 19(5):4085–4090, Feb 2011.

[SML10] Douglas Stebila, Michele Mosca, and Norbert Lütkenhaus. The case for quantum key distribution. In Alexander Sergienko, Saverio Pascazio, and Paolo Villoresi, editors, *Quantum Communication and Quantum Networking*, pages 283–296, Berlin, Heidelberg, 2010. Springer Berlin Heidelberg.

[SML+14] Jie Sun, Michele Moresco, Gerald Leake, Douglas Coolbaugh, and Michael R. Watts. Generating and identifying optical orbital angular momentum with silicon photonic circuits. *Opt. Lett.*, 39(20):5977–5980, Oct 2014.

[SMSC+15] Lynden K. Shalm, Evan Meyer-Scott, Bradley G. Christensen, Peter Bierhorst, Michael A. Wayne, Martin J. Stevens, Thomas Gerrits, Scott Glancy, Deny R. Hamel, Michael S. Allman, Kevin J. Coakley, Shellee D. Dyer, Carson Hodge, Adriana E.

Lita, Varun B. Verma, Camilla Lambrocco, Edward Tortorici, Alan L. Migdall, Yanbao Zhang, Daniel R. Kumor, William H. Farr, Francesco Marsili, Matthew D. Shaw, Jeffrey A. Stern, Carlos Abellán, Waldimar Amaya, Valerio Pruneri, Thomas Jennewein, Morgan W. Mitchell, Paul G. Kwiat, Joshua C. Bienfang, Richard P. Mirin, Emanuel Knill, and Sae Woo Nam. Strong loophole-free test of local realism. *Phys. Rev. Lett.*, 115:250402, Dec 2015.

[SRLL02a] Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs. Continuous variable quantum cryptography: Beating the 3 db loss limit. *Phys. Rev. Lett.*, 89:167901, Sep 2002.

[SRLL02b] Ch. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs. Continuous variable quantum cryptography: Beating the 3 db loss limit. *Phys. Rev. Lett.*, 89:167901, Sep 2002.

[SS10] Lana Sheridan and Valerio Scarani. Security proof for quantum key distribution using qudit systems. *Phys. Rev. A*, 82:030301, Sep 2010.

[STW09] Christian Schaffner, B. Terhal, and S. Wehner. Robust cryptography in the noisy-quantum-storage model. *Quantum Inf. Comput.*, 9:963–996, 2009.

[SWV+09] D Stucki, N Walenta, F Vannel, R T Thew, N Gisin, H Zbinden, S Gray, C R Towery, and S Ten. High rate, long-distance quantum key distribution over 250 km of ultra low loss fibres. *New Journal of Physics*, 11(7):075003, jul 2009.

[Sá93] Jorge Sánchez. Entropic uncertainty and certainty relations for complementary observables. *Physics Letters A*, 173(3):233–239, 1993.

[TAZG04] R. T. Thew, A. Acín, H. Zbinden, and N. Gisin. Bell-type test of energy-time entangled qutrits. *Phys. Rev. Lett.*, 93:010503, Jul 2004.

[TBZG00] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin. Quantum cryptography using entangled photons in energy-time bell states. *Phys. Rev. Lett.*, 84:4737–4740, May 2000.

[TGW14] Masahiro Takeoka, Saikat Guha, and Mark M. Wilde. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nature Communications*, 5(1), Oct 2014.

[TL17] Marco Tomamichel and Anthony Leverrier. A largely self-contained and complete security proof for quantum key distribution. *Quantum*, 1:14, July 2017.

[TLWL18] Kiyoshi Tamaki, Hoi-Kwong Lo, Wenyuan Wang, and Marco Lucamarini. Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound, 2018.

[TNZ+07] Hiroki Takesue, Sae Woo Nam, Qiang Zhang, Robert H. Hadfield, Toshimori Honjo, Kiyoshi Tamaki, and Yoshihisa Yamamoto. Quantum key distribution over a 40-db channel loss using superconducting single-photon detectors. *Nature Photonics*, 1(6):343–348, 2007.

[Unr] Dominique Unruh. Protokollkomposition und komplexitat (protocol composition and complexity). phd thesis. *Universitat Karlsruhe (TH), Berlin, 2006*.

[Unr10] Dominique Unruh. Universally composable quantum multi-party computation. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 486–505. Springer, 2010.

[Unr13] Dominique Unruh. Everlasting multi-party computation. In *CRYPTO*, pages 380–397. Springer, 2013.

[Unr15a] Dominique Unruh. Revocable quantum timed-release encryption. *J. ACM*, 62(6), December 2015.

[Unr15b] Dominique Unruh. Revocable quantum timed-release encryption. *Journal of the ACM (JACM)*, 62(6):1–76, 2015.

[VGTE+18] Pierre Vernaz-Gris, Aaron D. Tranter, Jesse L. Everett, Anthony C. Leung, Karun V. Paul, Geoff T. Campbell, Ping Koy Lam, and Ben C. Buchler. High-performance raman memory with spatio-temporal reversal. *Opt. Express*, 26(10):12424–12431, May 2018.

[Wan05a] Xiang-Bin Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.*, 94:230503, Jun 2005.

[Wan05b] Xiang-Bin Wang. Decoy-state protocol for quantum cryptography with four different intensities of coherent light. *Phys. Rev. A*, 72:012322, Jul 2005.

[Wat18] John Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018.

[WB05] P. Wocjan and T. Beth. New construction of mutually unbiased bases in square dimensions. *Quantum Inf. Comput.*, 5:93–101, 2005.

[WCSL10a] Stephanie Wehner, Marcos Curty, Christian Schaffner, and Hoi-Kwong Lo. Implementation of two-party protocols in the noisy-storage model. *Phys. Rev. A*, 81:052336, May 2010.

[WCSL10b] Stephanie Wehner, Marcos Curty, Christian Schaffner, and Hoi-Kwong Lo. Implementation of two-party protocols in the noisy-storage model. *Phys. Rev. A*, 81:052336, May 2010.

[WPGP+12] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J. Cerf, Timothy C. Ralph, Jeffrey H. Shapiro, and Seth Lloyd. Gaussian quantum information. *Rev. Mod. Phys.*, 84:621–669, May 2012.

[WST08a] Stephanie Wehner, Christian Schaffner, and Barbara M. Terhal. Cryptography from noisy storage. *Phys. Rev. Lett.*, 100:220502, Jun 2008.

[WST08b] Stephanie Wehner, Christian Schaffner, and Barbara M Terhal. Cryptography from noisy storage. *Physical Review Letters*, 100(22):220502, 2008.

[WUZ+17] Ye Wang, Mark Um, Junhua Zhang, Shuoming An, Ming Lyu, Jing-Ning Zhang, L.-M. Duan, Dahyun Yum, and Kihwan Kim. Single-qubit quantum memory exceeding ten-minute coherence time. *Nature Photonics*, 11(10):646–650, Sep 2017.

[WWQ+19] X. Wang, Jing-Tao Wang, Ji-Qian Qin, Cong Jiang, and Zong-Wen Yu. Guessing probability in quantum key distribution. *npj Quantum Information*, 6:1–5, 2019.

[Wyn75] A. D. Wyner. The wire-tap channel. *The Bell System Technical Journal*, 54(8):1355–1387, 1975.

[WZ82] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886):802–803, 1982.

[XMZ+20] Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.*, 92:025002, May 2020.

[YCY+16] Hua-Lei Yin, Teng-Yun Chen, Zong-Wen Yu, Hui Liu, Li-Xing You, Yi-Heng Zhou, Si-Jing Chen, Yingqiu Mao, Ming-Qi Huang, Wei-Jun Zhang, Hao Chen, Ming Jun Li, Daniel Nolan, Fei Zhou, Xiao Jiang, Zhen Wang, Qiang Zhang, Xiang-Bin Wang, and Jian-Wei Pan. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.*, 117:190501, Nov 2016.

[YDD+09] Z L Yuan, A R Dixon, J F Dynes, A W Sharpe, and A J Shields. Practical gigahertz quantum key distribution based on avalanche photodiodes. *New Journal of Physics*, 11(4):045019, apr 2009.

[ZFQ+08] Yi Zhao, Chi-Hang Fred Fung, Bing Qi, Christine Chen, and Hoi-Kwong Lo. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A*, 78:042333, Oct 2008.

[ZSW08] Lijian Zhang, Christine Silberhorn, and Ian A. Walmsley. Secure quantum key distribution using continuous variables of single photons. *Phys. Rev. Lett.*, 100:110504, Mar 2008.

[ZXC+18] Qiang Zhang, Feihu Xu, Yu-Ao Chen, Cheng-Zhi Peng, and Jian-Wei Pan. Large scale quantum key distribution: challenges and solutions, *Invited*. *Opt. Express*, 26(18):24260–24273, Sep 2018.

[ZYC14] Zichen Zhang, Zheng You, and Daping Chu. Fundamentals of phase-only liquid crystal on silicon (lcos) devices. *Light: Science & Applications*, 3(10):e213–e213, 2014.

[ZZD+16] Quntao Zhuang, Zheshen Zhang, Justin Dove, Franco N. C. Wong, and Jeffrey H. Shapiro. Floodlight quantum key distribution: A practical route to gigabit-per-second secret-key rates. *Phys. Rev. A*, 94:012322, Jul 2016.

[ZZH+15] Tian Zhong, Hongchao Zhou, Robert D Horansky, Catherine Lee, Varun B Verma, Adriana E Lita, Alessandro Restelli, Joshua C Bienfang, Richard P Mirin, Thomas Gerrits, Sae Woo Nam, Francesco Marsili, Matthew D Shaw, Zheshen Zhang, Ligong

Wang, Dirk Englund, Gregory W Wornell, Jeffrey H Shapiro, and Franco N C Wong. Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding. *New Journal of Physics*, 17(2):022002, feb 2015.

[ZZLS18] Quntao Zhuang, Zheshen Zhang, Norbert Lütkenhaus, and Jeffrey H. Shapiro. Security-proof framework for two-way gaussian quantum-key-distribution protocols. *Phys. Rev. A*, 98:032332, Sep 2018.

[ZZWS17] Zheshen Zhang, Quntao Zhuang, Franco N. C. Wong, and Jeffrey H. Shapiro. Flood-light quantum key distribution: Demonstrating a framework for high-rate secure communication. *Phys. Rev. A*, 95:012332, Jan 2017.

List of Figures

List of Tables

ECOLE
DOCTORALE

Titre : Cryptographie quantique dans un modèle de sécurité hybride

Mots clés : Quantum Computational Timelock, Everlasting Security, Quantum cryptography, Quantum information theory, Quantum Key Distribution

Résumé : L'extension des fonctionnalités et le dépassement des limitations de performances de QKD nécessitent soit des répéteurs quantiques, soit de nouveaux modèles de sécurité. En étudiant cette dernière option, nous introduisons le modèle de sécurité Quantum Computational Timelock (QCT), en supposant que le cryptage sécurisé informatiquement ne peut être rompu qu'après un temps beaucoup plus long que le temps de cohérence des mémoires quantiques disponibles. Ces deux hypothèses, à savoir la sécurité informatique à court terme et le stockage quantique bruité, ont jusqu'à présent déjà été prises en compte en cryptographie quantique, mais seulement de manière disjointe. Une limite inférieure pratique du temps, pour laquelle le cryptage est sécurisé du point de vue informatique, peut être déduite de la sécurité à long terme supposée du schéma de cryptage AES256 (30 ans) et de la valeur du temps de cohérence dans les démonstrations expérimentales de stockage puis de récupération de quantum optiquement codé. l'information, au niveau d'un seul photon, va de quelques nanosecondes à quelques microsecondes. Compte tenu du grand écart entre la borne supérieure du temps de cohérence et la borne inférieure du temps de sécurité de calcul d'un schéma de chiffrement, la validité du modèle de sécurité QCT peut être supposée avec une très grande confiance aujourd'hui et laisse également une marge considérable pour sa validité dans le futur. En utilisant le modèle de sécurité QCT, nous proposons un protocole d'accord de clé explicite à dimension d que nous appelons MUB-Quantum Computational Timelock (MUB-QCT), où un bit est codé sur un état qudit en utilisant un ensemble complet de bases mutuellement impartiales (MUB) et une famille de permutations indépendantes par paires. La sécurité est prouvée en montrant que la borne supérieure sur les échelles d'information d'Eve est $\mathcal{O}(1/d)$. Nous montrons que MUB-QCT offre : une haute résilience aux erreurs (jusqu'à 50 $\%$ pour les grands d) avec des exigences matérielles fixes ; La sécurité MDI car la sécurité est indépendante de la surveillance des canaux et ne nécessite pas de faire confiance aux appareils de mesure. Nous prouvons également la sécurité du protocole MUB-QCT, avec plusieurs photons par utilisation de canal, contre les attaques non adaptatives, en particulier la mesure MUB proactive où eve mesure chaque copie dans un MUB différent suivi d'un décodage post-mesure. Nous prouvons que le protocole MUB-QCT permet une distribution sécurisée des clés avec des états d'entrée contenant jusqu'à $\mathcal{O}(d)$ photons, ce qui implique une amélioration significative des performances, caractérisée par une multiplication $\mathcal{O}(d)$ du taux de clé et une augmentation significative de la distance accessible. Ces résultats illustrent la puissance du modèle de sécurité QCT pour augmenter les performances de la cryptographie quantique tout en gardant un net avantage de sécurité par rapport à la cryptographie classique.

Institut Polytechnique de Paris
91120 Palaiseau, France

ECOLE DOCTORALE

Title : Quantum cryptography in a hybrid security model

Keywords : Quantum Computational Timelock, Everlasting Security, Quantum cryptography, Quantum information theory, Quantum Key Distribution

Abstract : Extending the functionality and overcoming the performance limitation of QKD requires either quantum repeaters or new security models. Investigating the latter option, we introduce the Quantum Computational Timelock (QCT) security model, assuming that computationally secure encryption may only be broken after time much longer than the coherence time of available quantum memories. These two assumptions, namely short-term computational security and noisy quantum storage, have so far already been considered in quantum cryptography, yet only disjointly. A practical lower bound on time, for which encryption is computationally secure, can be inferred from assumed long-term security of the AES256 encryption scheme (30 years) and the value of coherence time in experimental demonstrations of storage and then retrieval of optically encoded quantum information, at single-photon level range from a few nanoseconds to microseconds. Given the large gap between the upper bound on coherence time and lower bound on computational security time of an encryption scheme, the validity of the QCT security model can be assumed with a very high confidence today and also leaves a considerable margin for its validity in the future. Using the QCT security model, we propose an explicit d-dimensional key agreement protocol that we call MUB-Quantum Computational Timelock (MUB-QCT), where a bit is encoded on a qudit state using a full set of mutually unbiased bases (MUBs) and a family of pair-wise independent permutations. Security is proved by showing that upper bound on Eve's information scales as $\mathcal{O}(1/d)$. We show MUB-QCT offers : high resilience to error (up to 50$\%$ for large d) with fixed hardware requirements ; MDI security as security is independent of channel monitoring and does not require to trust measurement devices. We also prove the security of the MUB-QCT protocol, with multiple photons per channel use, against non-adaptive attacks, in particular, proactive MUB measurement where eve measures each copy in a different MUB followed by post-measurement decoding. We prove that the MUB-QCT protocol allows secure key distribution with input states containing up to $\mathcal{O}(d)$ photons which implies a significant performance boost, characterized by an $\mathcal{O}(d)$ multiplication of key rate and a significant increase in the reachable distance. These results illustrate the power of the QCT security model to boost the performance of quantum cryptography while keeping a clear security advantage over classical cryptography.

Institut Polytechnique de Paris
91120 Palaiseau, France