Quantum cryptography and its application frontiers

Romain Alleaume

SORBONNE UNIVERSITÉ

RAPPORT SCIENTIFIQUE PRÉSENTÉ POUR L'OBTENTION D'UNE HABILITATION À DIRIGER DES RECHERCHES

Quantum cryptography and its application frontiers

Author: Romain ALLÉAUME

Final version, made publicly available on October 14 2021, after the defense (on 24/09/2021).

Composition du jury

Rapporteurs

Stephanie WEHNER	Professeur, QuTech, Université Technologique de Delft
Hugo ZBINDEN	Professeur, Université de Genève
Andrew SHIELDS	Head of Quantum Technology Division, Toshiba, Cambridge

Examinateurs

Pascale SENELLART	Directrice de Recherche, CNRS
Gilles ZEMOR	Professeur, Université de Bordeaux
Nicolas TREPS	Professeur, Sorbonne Université

to Aurore, Antoine and Camille.

Acknowledgements

Let me first warmly thank Stephanie Wehner, Hugo Zbinden and Andrew Shields for reviewing the present manuscript, as well as Pascale Senellart, Gilles Zémor and Nicolas Treps for accepting to participate in my habilitation committee. Their outstanding scientific contributions, and the different ways with which they approach research and technology constitute models that I have tried to learn from. It is an honor for me that they have accepted to be part of my jury and I look forward to the defense.

Telecom Paris has been a great place to work along these years. Even if I cannot name all of them, I would like to thank my colleagues, students, as well as the administrative and management staff of the Telecom Paris, for making the school such a special place. I want to specially thank Michel Riguidel, who has given me the opportunity to directly dive into quantum European research, a beautiful and foundational learning experience for me. I also want to thank Henri Maitre and Talel Abdessalem for their trust and support expressed at many occasions, that has been instrumental to the development of the quantum activity at Telecom Paris and LTCI and now in the stimulating context of IP Paris and the QUANTUM center.

I want to thank Philippe Grangier, Anthony Leverrier, and Eleni Diamanti, for the regular, stimulating and sometimes even heated discussions that we share, yet always in a friendly spirit. I would like also to thank Norbert Lütkenhaus, for being such a kind and trusted source of scientific advice over the years. I also would like to thank Iordanis Kerenidis, and Eleni another time, for the initiative to set up the Paris Center for Quantum Computing. It has been a wonderful opportunity to learn more about the computer science side of quantum, and to get to know better great quantum colleagues at IRIF and Inria Secret. Thanks in particular to Jean-Pierre Tillich, Frederic Magniez, Sophie Laplante, André Chailloux and Alex Grilo, for advices and enjoyable discussions.

It has been wonderful to work as a team at Telecom Paris during many years with Eleni Diamanti, Damian Markham and Elham Kashefi. I would like to thank them for many great memories, and for their unique way to combine never-ending optimism, great coolness and high working standards. It was a bitter moment to see them leave in 2016, but great to continue to have many opportunities to work together, which I am very happy about. Over the next few years, the action of Gerard Memmi and Yves Poilane and also the motivation and the decisive team effort with Isabelle Zaquine and Filippo Miatto, has allowed us to look forward and I am grateful to them about this.

I also realize the importance, especially even more after two years spent on "Zoom", of the network of European colleagues and scientific friends working on quantum communications and quantum cryptography, and of its quality. I want to thank the CIVIQ team and in particular Valerio Pruneri for his leadership and his attention to ideas and people. It is a great pleasure to work with Vicente Martin, Momtchil Peev Imran Kahn, Vladimir Usenko, Tobias Gehring and Ulrich Andersen, in this context, and more broadly to travel at their sides on the long-term quantum communications journey. A great thank also, for the colleagues and friends at AIT, in particular Andreas Poppe, Hannes Hübel, Christoph Pacher, which which we share a long collaboration history, initiated on quantum networks, and now on CV-QKD and quantum cybersecurity. I look forward to continuing this collaboration in EuroQCI and contribute to build a quantum industry. A very special thank to Yves Jaouen, and Cedric Ware. It is great to collaborate with them on the frontier between quantum and classical coherent communications. Thanks Yves for sharing your wisdom on the experimental secrets of the optical communication platform, and your decisive and always warm-hearted support to make it “quantum”.

The long-term collaboration with IdQuantique and their team, has also played an important role in my career and certainly in the decision to start SeQureNet with Nicolas Aliacar that I want to thank for his friendship and trust. I want to thank Grégoire Ribordy, Nicolas Gisin, Hugo Zbinden and Bruno Huttner for many great moments at their sides, and congratulate them for the 20 years of IDQ. It has also been a great pleasure to participate to the collective effort, steered by the Toshiba team, towards industry standards for QKD, with the ETSI QKD Industry Standardization Group. Let me thank in particular Marco Lucamarini, for many enlightening discussions as well as Tom Chapuran, Alan Mink, Ivo Petro Degiovanni, Marco Gramegna and obviously Andrew Shields and Martin Ward for bringing their driving energy and professionalism to his forum that is now truly playing a central role in QKD industrialization, and notably security certification.

Let me finally conclude by thanking my students and post-docs, and in particular Rupesh Kumar, who worked with me as a post-doc and was the driving force in our experimental CV-QKD papers. Let me also mention my former and current PhD students Aurélien, Hao, Adrien, Nilesh, Raphaël, Francesco and Guillaume. It has been great - and still is - working with them, hopefully learn how to become a better supervisor. I has been great also to learn from their questions and vision as we tried to explore together new paths within the quantum cryptographic landscape. I want to thank them for their commitment and passion, as we slowly climbed this mountain together. This would not have been possible without them. I hope they also enjoyed the journey and look very much forward to future hikes.

List of publications

Preprints and Working drafts

1. Nilesh Vyas and Romain Alléaume. Everlasting secure key agreement with performance beyond qkd in a quantum computational hybrid security model. *arXiv preprint arXiv:2004.10173*, 2020

2. Ravi Raghunathan, Guillaume Ricard, Baptiste Lefaucher, Antoine Henry, Filippo Miatto, Isabelle Zaquine, and Romain Alléaume. Parallelizable synthesis of arbitrary single-qubit gates with linear optics and time-frequency encoding. *In Preparation*, 2021

3. Raphaël Aymeric and Romain Alléaume. Covert continuous variable quantum key distribution. *In Preparation*, 2021

4. Shihan Sajeed, Romain Alléaume, and Hoi-Kwong Lo. A direct look at quantum secure communication. *In Preparation*, 2022

Articles published in peer-reviewed scientific journals

1. Rupesh Kumar, Francesco Mazzoncini, Hao Qin, and Romain Alléaume. Experimental vulnerability analysis of qkd based on attack ratings. *Scientific Reports*, 22:9564, 2021

2. Hao Qin, Rupesh Kumar, Vadim Makarov, and Romain Alléaume. Homodyne-detector-blinding attack in continuous-variable quantum key distribution. *Physical Review A*, 98(1):012312, 2018

3. Adrien Marie and Romain Alléaume. Self-coherent phase reference sharing for continuous-variable quantum key distribution. *Physical Review A*, 95(1):012316, 2017

4. Hao Qin, Rupesh Kumar, and Romain Alléaume. Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution. *Physical Review A*, 94(1):012325, 2016

5. Rupesh Kumar, Hao Qin, and Romain Alléaume. Coexistence of continuous variable qkd with intense dwdm classical channels. *New Journal of Physics*, 17(4):043027, 2015

6. Romain Alléaume, Cyril Branciard, Jan Bouda, Thierry Debuisschert, Mehrdad Dianati, Nicolas Gisin, Mark Godfrey, Philippe Grangier, Thomas Länger, Norbert Lütkenhaus, et al. Using quantum key distribution for cryptographic purposes: a survey. *Theoretical Computer Science*, 560:62–81, 2014

7. Aurélien Bocquet, Romain Alléaume, and Anthony Leverrier. Optimal eavesdropping on quantum key distribution without quantum memory. *Journal of Physics A: Mathematical and Theoretical*, 45(2):025305, 2011

8. Paul Jouguet, Sébastien Kunz-Jacques, Thierry Debuisschert, Simon Fossier, Eleni Diamanti, Romain Alléaume, Rosa Tualle-Brouri, Philippe Grangier, Anthony Leverrier, Philippe Pache, et al. Field test of classical symmetric encryption with continuous variables quantum key distribution. *Optics Express*, 20(13):14030–14041, 2012

9. Jean-Loup Smirr, Sylvain Guilbaud, Joe Ghalbouni, Robert Frey, Eleni Diamanti, Romain Alléaume, and Isabelle Zaquine. Simple performance evaluation of pulsed spontaneous parametric down-conversion sources for quantum communications. *Optics express*, 19(2):616–627, 2011

10. Louis Salvail, Momtchil Peev, Eleni Diamanti, Romain Alléaume, Norbert Lütkenhaus, and Thomas Länger. Security of trusted repeater quantum key distribution networks. *Journal of Computer Security*, 18(1):61–87, 2010

11. Romain Alleaume, François Roueff, Eleni Diamanti, and N Lütkenhaus. Topological optimization of quantum key distribution networks. *New Journal of Physics*, 11(7):075002, 2009

12. Momtchil Peev, Christoph Pacher, Romain Alléaume, Claudio Barreiro, Jan Bouda, W Boxleitner, Thierry Debuisschert, Eleni Diamanti, M Dianati, JF Dynes, et al. The secoqc quantum key distribution network in vienna. *New Journal of Physics*, 11(7):075001, 2009

13. Anthony Leverrier, Romain Alléaume, Joseph Boutros, Gilles Zémor, and Philippe Grangier. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Physical Review A*, 77(4):042325, 2008

14. Mehrdad Dianati, Romain Alléaume, Maurice Gagnaire, and Xuemin Shen. Architecture and protocols of the future european quantum key distribution network. *Security and Communication Networks*, 1(1):57–74, 2008

Papers published or initiated during the PhD

15. Y Dumeige, R Alléaume, P Grangier, F Treussart, and J-F Roch. Controling the single-diamond nitrogen-vacancy color center photoluminescence spectrum with a fabry–perot microcavity. *New Journal of Physics*, 13(2):025015, 2011

16. Quyên Dinh Xuân, R Alléaume, Liantuan Xiao, F Treussart, B Journet, and J-F Roch. Intensity noise measurement of strongly attenuated laser diode pulses in the time domain. *The European Physical Journal Applied Physics*, 35(2):117–121, 2006

17. R Alléaume, F Treussart, G Messin, Y Dumeige, J-F Roch, A Beveratos, R Brouri-Tualle, J-P Poizat, and P Grangier. Experimental open-air quantum key distribution with a single-photon source. *New Journal of physics*, 6(1):92, 2004

18. Romain Alléaume, Francois Treussart, Jean-Michel Courty, and Jean-Francois Roch. Photon statistics characterization of a single-photon source. *New Journal of physics*, 6(1):85, 2004

19. Y Dumeige, F Treussart, R Alléaume, T Gacoin, J-F Roch, and P Grangier. Photo-induced creation of nitrogen-related color centers in diamond nanocrystals under femtosecond illumination. *Journal of luminescence*, 109(2):61–67, 2004

20. François Treussart, Romain Alléaume, Véronique Le Floch, LT Xiao, J-M Courty, and J-F Roch. Direct measurement of the photon statistics of a triggered single photon source. *Physical review letters*, 89(9):093601, 2002

21. François Treussart, Romain Alléaume, Véronique Le Floc'h, and Jean-François Roch. Single photon emission from a single molecule. *Comptes Rendus Physique*, 3(4):501–508, 2002

22. RA Michniak, R Alleaume, DN McKinsey, and JM Doyle. Alpha and beta particle induced scintillations in liquid and solid neon. *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment*, 482(1-2):387–394, 2002

Conference proceedings

1. Romain Alléaume, Raphaël Aymeric, Cédric Ware, and Yves Jaouën. Technology trends for mixed qkd/wdm transmission up to 80 km. In *2020 Optical Fiber Communications Conference and Exhibition (OFC)*, pages 1–3. IEEE, 2020

2. Ravi Raghunathan, G Ricard, Filippo Miatto, Isabelle Zaquine, and Romain Alléaume. Single qubit arbitrary unitary synthesis using photonic spectral encoding. In *Quantum Technology International Conference (QTech 2018)*, 2018

3. Romain Alléaume, Ivo P Degiovanni, Alan Mink, Thomas E Chapuran, Norbert Lutkenhaus, Momtchil Peev, Christopher J Chunnilall, Vincente Martin, Marco Lucamarini, Martin Ward, et al. Worldwide standardization activity for quantum key distribution. In *2014 IEEE Globecom Workshops*, pages 656–661. IEEE, 2014

4. Hao Qin, Rupesh Kumar, and Romain Alléaume. Saturation attack on continuous-variable quantum key distribution system. In *Emerging Technologies in Security and*

Defence; and Quantum Security II; and Unmanned Sensor Systems X, volume 8899, page 88990N. International Society for Optics and Photonics, 2013

5. Yannick Dumeige, Romain Alléaume, Philippe Grangier, François Treussart, and Jean-François Roch. Coupling of a single nitrogen vacancy colour centre in diamond, to a planar microcavity. In *2011 13th International Conference on Transparent Optical Networks*, pages 1–4, 2011

6. David Elkouss, Anthony Leverrier, Romain Alléaume, and Joseph J Boutros. Efficient reconciliation protocol for discrete-variable quantum key distribution. In *2009 IEEE International Symposium on Information Theory*, pages 1879–1883. IEEE, 2009

7. M Peev, Romain Alléaume, T Langer, Lutkenhaus N, Maurhart O., and Salvail L. The secoqc quantum key distribution network prototype: Principles, design and implementation. In *Globecom*. IEEE, 2007

8. Mehrdad Dianati and Romain Alléaume. Architecture of the secoqc quantum key distribution network. In *2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07)*, pages 13–13. IEEE, 2007

9. Mehrdad Dianati and Romain Alléaume. Architecture of the secoqc quantum key distribution network. In *2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07)*, pages 13–13. IEEE, 2007

10. Rex AC Medeiros, Romain Alléaume, Gérard Cohen, and Francisco M de Assis. Zero-error capacity of quantum channels and noiseless subsystems. In *2006 International Telecommunications Symposium*, pages 900–905. IEEE, 2006

11. Romain Alléaume, François Roueff, Oliver Maurhart, and N Lutkenhaus. Architecture, security and topology of a global quantum key distribution network. In *2006 Digest of the LEOS Summer Topical Meetings*, pages 38–39. IEEE, 2006

Papers published or initiated during the PhD

12. Romain Alléaume, Jean-François Roch, Darius Subacius, Anton Zavriyev, and Alexei Trifonov. Fiber-optics quantum cryptography with single photons. In *AIP Conference Proceedings*, volume 734, pages 287–290. American Institute of Physics, 2004

13. Alexei Trifonov, Anton Zavriyev, Darius Subacius, Romain Alléaume, and Jean-François Roch. Practical quantum cryptography. In *Quantum Information and Computation II*, volume 5436, pages 1–11. International Society for Optics and Photonics, 2004

14. Lian-Tuan Xiao, Romain Alléaume, Quyen Dinh Xuan, Francois Treussart, Bernard A Journet, and Jean-françois Roch. Measurement of photon distribution in attenuated diode laser pulses. In *Physics and Simulation of Optoelectronic Devices XI*, volume 4986, pages 463–468. International Society for Optics and Photonics, 2003

15. F Treussart, R Alléaume, V Le Floc?h, LT Xiao, J-F Roch, and J-M Courty. Photon statistics of a single photon source. In *Organic Nanophotonics*, pages 413–422. Springer, 2003

16. Francois Treussart, Romain Alléaume, Jean-Michel Courty, and Jean-Francois Roch. Emission properties of a single photon source. *Physica Scripta*, 2004(T112):95, 2004

Standards and Technical White Papers

1. Romain Alléaume. Quantum key distribution (qkd); device and communication channel parameters for qkd deployment - group specification qkd 012. 2019

2. Marco Lucamarini, Andrew Shields, 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, and Zhiliang Yuan. Implementation security of quantum cryptography. *ETSI Group Specification Document*, 2018

3. Romain Alléaume, M Riguidel, H Weinfurter, N Gisin, P Grangier, M Dianati, Mark Godfrey, G Ribordy, J Rarity, M Peev, et al. Secoqc white paper on quantum key distribution and cryptography. Technical report, 2007

Patents

1. Romain Alléaume. Communication with everlasting security from short-term-secure encrypted quantum communication, October 2016. International Patent WO2016110582A1

2. Romain Alléaume and Adrien Marie. Phase reference sharing schemes for continuous-variable quantum cryptography, May 2016. European Patent EP3244566

3. Romain Alléaume. Practical quantum cryptography with everlasting security, October 2015. European Patent 3043507

4. Romain Alléaume. Hybrid classical quantum cryptography, January 2015. European Patent 3043508

Contents

Chapter 1

Introduction

My research activity over the past fifteen years has largely been focused on quantum cryptography and in particular quantum key distribution (QKD) and its industrial development. This has given me the opportunity to tackle a large variety of subjects, ranging from foundamental scientific questions related to information security and quantum optics, to technological and engineering challenges associated with the development of a commercial QKD system. This "Habilitation à Diriger des Recherches" (HdR) manuscript intends to present an overview of this work and also to draw some perspectives for the future of quantum cryptography, with a focus on its practical applications.

1.1 From research to applications

I have chosen to position the focus of this manuscript at the *application frontier*, i.e. to take the interplay between quantum cryptography research and its applications as a guideline. This choice is largely driven by my own carrier path, where I have tried to contribute to science and technology both as a researcher, but also by creating the start-up company SeQureNet [Seq]. This choice is also based on the observation that, even though the promises of the second quantum revolution have started to become a reality, only a handful of quantum technologies have already reached a sufficiently high maturity level to serve real-world use cases. On the other hand, for most application envisaged so far, there still exists of a gap between the performances required to guarantee a quantum advantage and current technological capabilities.

This mismatch between technology and application requirements is sometimes eclipsed by media hype, in which the real and impressive progress on quantum technologies might be extrapolated towards overoptimistic predictions about applicability. Considering the development of quantum technology not as a one-way train towards dreamed applications, but instead embracing it as a complex dialectic between research in progress and emerging applications, probably strikes a better balance and provides a way to grasp and address more efficiently upfront challenges. This approach is schematically represented on figure 1.1, that depicts a two-way process associated with a research-application di-

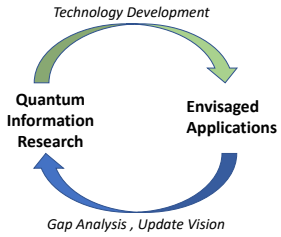

Figure 1.1: Dialectic interaction between research in quantum information and the targeted applications.

alectic. It also provides an interesting and application-oriented framework to analyze the current dynamics of quantum information technologies, including quantum computing, even though our focus will be here solely on quantum communications.

Despite not embracing mainstream trends and relay dazzling promisses about the "quantum future", I still want to claim that the critical vision we would like to articulate here is *optimistic*. It consists in accepting that the application frontier is a two-way process, based on the motivation to push technology towards higher maturity levels, but also driven by the compelling need to update our vision as we become better aware of some mismatch between technological capabilities and expected applications. As depicted on Figure 1.1, the dialectic interaction should be seen as two-sided opportunity: at research level, to improve our understanding of fundamental technological limits ; at application level, to update our expectations and redefine our vision. This dialectic vision also shapes the structure and content of this manuscript.

1.2 Quantum cryptography and its applications frontiers

The birth of quantum information science as an established research field, can be dated back to the mythic Physics of Computation Conference which was jointly organized by MIT and IBM, and held at the MIT Endicott House in 1981. A very interesting celebration conference [QC421] has recently been for the 40th anniversary of this event. In wonderful keynotes, founding fathers of the field Charles Bennett and Peter Shor recalled some of the outstanding achievements that have been reached in 40 years, and also pinpointed the growing influence that quantum information fundational ideas have had over the past decades.

Quantum cryptography and in particular QKD have definitely played a pioneering role in this journey. As a matter of fact, QKD in its simplest form requires only to prepare, transport and measure single qubit quantum information. It hence constitutes one of the simple route towards a measurable quantum cryptographic advantage. QKD is, as a consequence, one of the most mature quantum technologies and one of the first able to expand

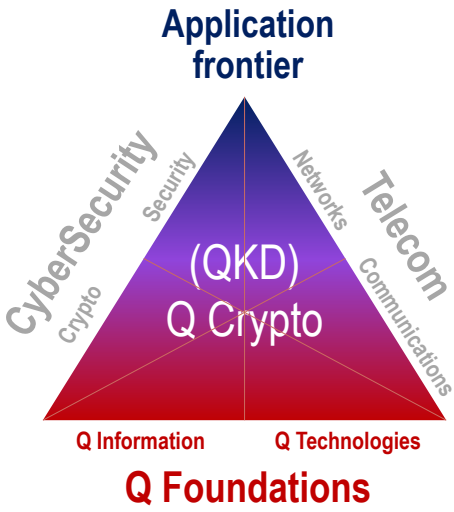

Figure 1.2: QKD is a pluri-disciplinar technology. It rests on a foundational quantum pillar and is becoming increasingly connected to the telecommunications and cyber-security industry pillars.

its application boundaries towards large-scale markets, such as telecom infrastructures or security applications. As illustrated in figure 1.2, these two major industry verticals also constitute natural industrial ecosystems in which QKD technology strive to integrate, but also to augment, in order to demonstrate its relevance from a societal and industrial standpoint. Playing a prominent role in federating the engineering efforts in quantum communications and cryptography towards integrated industrial ecosystems, QKD is therefore undoubtedly a key technology to understand the interplay between quantum foundations and applications.

Figure 1.2 provides a pictorial representation of this viewpoint, in the form of a triangle, that can also be seen as a bird's eye view of the content of this manuscript. We will begin with the basis of the triangle, with chapter 2 on quantum cryptography, where we will briefly position existing primitives in terms of service but also in terms of technological readiness. We will then address in chapter 3, and chapter 4 respectively, the two other sides of the triangle, and the challenges associated with the integration of quantum cryptography (and principally QKD), in the cybersecurity and telecom landspaces. Finally we will propose in chapter 5 a more personal analysis of some of the lessons learnt at the application frontier, based on the experience and insights gathered as a contributor to QKD technology. This actually leads us to formulate a critical analysis of QKD positioning and then, to propose a path and some new perspectives for quantum cryptography, both in terms of research program and applications.

1.3 Organization of the manuscript and main contributions

Let us now describe in more details, chapter by chapter, and section by section, the content of this manuscript, with pointers towards the related scientific contributions and references.

We propose in **Chapter 2** an overview of quantum cryptographic primitives, with a focus on functionalities that can be implemented with near-term technologies. This initial survey aims at positioning QKD with respect to the broader landscape of quantum cryptographic primitives. We try in particular to pinpoint the particular position held by QKD as being one of the most mature quantum technology to claim a quantum (cryptographic) advantage, therefore epitomizing real-world quantum cryptography performed at the application frontier.

Chapter 3 is dedicated to system engineering and networking aspects of QKD. It highlight the structuring role that QKD technology has played, and continues to play, towards the development of quantum communication research and technologies as a whole. After a generic presentation of QKD communication processes 3.1 and technologies 3.2, the chapter is organized around two main themes: QKD system engineering and QKD networking, vith a focus on continous-variable (CV)-QKD. The associated challenges have also been an important focus of the research that I have conducted at Telecom Paris over the period 2008-2014, in parallel with the effort lead within the start-up SeQureNet, that I co-founded in 2008, to bring the first CV-QKD system to market [Seq].

CV quantum communication engineering is presented in section 3.3. The associated research had been, for an important part, initiated by a first work on the classical post-processing side of QKD where we focused on the improvement of error-correction techniques for DV-QKD using LDPC codes [ELAB09], and later on, by the milestone result obtained by Anthony Leverrier on multi-dimensional reconciliation [LAB+08], on CV-QKD. Within the SEQURE collaborative project we then performed the first field demonstration combining CV-QKD with link encryptors, and tested the reliability of the CV quantum communication technology [JKJD+12]. This has contributed to trigger the decision to develop a commercial CV-QKD system, within SeQureNet. More recently, I have started again to work on CV quantum communication system design in the context of the transition from transmitted local oscillator to a local local oscillator (LLO) design [MA17]. Studying the trade-off inherent to this transition, - including a specific self-coherent design that we have patented [AM16] and that has later proven its experimental relevance [QL18] - opens interesting convergence between quantum and classical coherent communications, which has now become one of our primary research focus in the context of the QT Flagship project CIVIQ [AAWJ20].

Quantum networking is then presented in section 3.4. It was one of the first research challenge that I encountered and had to deal with as I was integrating the European project SECOQC and was starting to work at Telecom Paris, in 2005. In this stimulating context, I

have contributed to define and formalize the architecture of QKD networks, including the 3-layers architecture [ARML06] that has then become widely adopted [SFI+11, CZC+21, MNR+20]. In collaboration with my European colleagues, in particular at AIT Vienna, we also came up with the first suite of network protocols for a trusted node QKD networks, [DA07] that has then been demonstrated at metropolitan scale during the SECOQC demonstration Vienna in 2008 [PPA+09].
We also present and put in perspective our work on mixed QKD/WDM transmission [KQA15], in which we performed the first experimental demonstration that QKD could be deployed over an optical fibre in coexistence with intense WDM channels, whose launch power is typically around 0 dBm. Such "native strong coexistence capability" is made possible by the significant common mode rejection ratio that can be obtained with a balanced homodyne receiver. Also not yet sufficient for deployment over optical backbones, these results and the additional recent progress [EHP+19, KSDS19] position quantum coherent communications favorably in view of the integration of quantum communication over existing lit fiber network infrastructure.

Chapter 4 is dedicated to the interplay between QKD and security. After recalling its composable security definition 4.1, we discuss how QKD can be used and combined with other security primitives in order to provide security services, while keeping an edge over purely computational and classical constructions.

The question of enhancing real-world security applications using QKD 4.2 has been (and still is) at the heart of my research work, starting with the SECOQC white paper [ARW+07] that was later published, after an important revision work, in the special issue of the Theory of Computer Science journal, at the occasion of the 30th birthday of BB84 [ABB+14]. This part of my work has lead me to become increasingly interested by cryptography, and also increasingly aware of the dissensus that could exist between quantum and classical cryptographers, in relation with QKD. This raising of awareness has in return deeply influenced my research. In particular, it has motivated me to investigate the nature of the dissensus and to develop research positioned at the frontier between classical and quantum cryptography, and that may contribute to reconcile both visions.

The ability to build quantum cryptographic hardware and to certify its security properties appears as another central challenge addressed in section 4.3. In this perspective, the design, evaluation and certification of QKD implementation secure against high attack potential attackers appears as a concrete and ambitious objective, to which my research team has vigorously contributed, notably via our work on saturation attack on CV-QKD. In [QKA16], we studied the implementation security of CV-QKD and demonstrated that the non-linear response of coherent receivers, in case it is not monitored, could be used as an attack vector against CV-QKD and lead to a full security break. We coined this vulnerability "Saturation Attack". We then showed in [QKMA18] that this attack could be implemented with simple hardware and proposed a practical counter-measure. We also participate to the ETSI QKD-ISG efforts on QKD implementation security[LSA+18], and to the writing of the first QKD protection profile [ETS21]. Towards this end, we have recently

proposed and experimentally demonstrated how the Common Criteria methodology and attack ratings can be applied to conduct vulnerability analysis of QKD [KMQA21] paving the way towards security certification of real-world quantum cryptographic systems.

The final **Chapter 5** intends to conclude this manuscript by drawing some new perspectives towards real-world application of quantum cryptography. This chapter is built around original content as well as research in progress. We open this chapter, in section 5.1, with a critical analysis of quantum cryptography positioning. Building on our work on the use of QKD for cryptographic purposes [ARW$^+$07, ABB$^+$14] but also acknowledging the important dissensus between quantum and classical cryptography communities [PPS07, Sch18, NCS20, ANS20, NSA20], we try to identify the nature of the complex dialectic interaction between these communities and the grounds on which their vision of cryptography can differ. This leads us to suggest a revised positioning with a stronger complementarity with respect to classical cryptography, as well as and an engineering-driven approach targeted to provide a security gain in realistic contexts.

Section 5.2, then presents our ongoing work on quantum cryptography in an hybrid quantum-computational security model that combines the noisy storage assumption [KWW12] with an extra assumption, namely the short-term security of computational one-way functions [Unr15] . The advantage of this Quantum Computational Timelock (QCT) security model is to allow to build protocols with everlasting security (unreachable with computational schemes) with performance (rate-loss behavior) and functionality that go beyond what is possible with "standard" quantum cryptography. Building on some ideas first proposed at QCrypt 2015 [All15b]. We recently proposed [VA20] a key distribution protocol in the QCT security model whose security proof can be established- for the moment against restricted attacks - by a reduction to a quantum to classical randomness extractor [BFW13]. This leads to key distribution rates that could be boosted by a $O(d)$ factor when implemented over a d-dimensional encodings, opening a new path towards quantum key establishment in high-loss setting, but also in terms of practical security with reduced trust requirements at the receiving site. I have also filed three european patent demands in relation with this work, one of them leading to a granted international patent [All15a, All15c, All16].

We conclude in 5.3 with a final section that intends to propose a shift in the approach pursued by practical quantum cryptography towards a revised vision that we call real-world quantum cryptography (rwqc) by analogy with the distinctive approach, scientific and technological work as well as community building that has already occurred around real-world cryptography [RWC]. Rwqc emerges as a holistic approach characterized by a shift of priorities towards objectives such as practical security gain in real-world application contexts or the ambition to engineer cost-effective quantum cryptographic hardware whose security can be certified. We elaborate on these perspectives and on the concrete development of such a real-world quantum cryptography program and try also to capture the high-level vision that it could be based upon. This leads us to envisage "Slow Information" in which data locality and privacy could emerge as central concepts empowered

by provable security in relevant cyber-physical models as well as high-quality, certified, engineering.

Chapter 2

Charting the near-term quantum cryptographic landscape

Quantum cryptography can be defined as the ensemble of cryptographic tasks that are impossible to realize solely with classical means, and that are rendered possible thanks to the use of quantum information as a communication or processing resource.

From a conceptual viewpoint, the central challenge of quantum cryptography is hence to leverage quantum information principles in order to build cryptographic protocols that meet one of the two following objectives:

1. Reach a security level that cannot be obtained classically, in particular based on classical information processing and computational assumptions.

2. Realize functionalities that are not achievable solely with classical means.

Cryptographic protocols can essentially be built from a small set core building blocks, such as randomness generation, cryptographic hashing, key establishment, data encryption, as well as digital signature and commitment schemes. Such core building blocks are called cryptographic primitives and are logically the main focus of attention both for codebreakers and codemakers.

We aim to present here a schematic overview of existing quantum cryptographic primitives, with of focus on applications and hence primitives that can be implemented with near-term technologies. Towards this end we analyze for which cryptographic functionalities there exist constructions based on quantum resources that allow to obtain a specific "quantum cryptographic advantage", but also for which functionalities we cannot hope to obtain such an advantage. This overview will moreover allow us to position quantum key distribution - that will be the main primitive studied in this manuscript - in the broader landscape of quantum cryptographic applications.

2.1 Near-term vs long-term applications

A significant part of my research work has been focused on addressing questions that sit at the frontier between quantum information science and engineering. A common pattern is that the related quantum cryptographic applications could be build with existing technology, and demonstrated in the lab [KQA15, QKA16, QKMA18] but also in field demonstrations [JKJD+12, PPA+09].

Even thought the distinction between near-term and long-term applications is deemed to be at least partially subjective and will of course evolve with time, it seems interesting to identify some patterns correlating between the technological readiness quantum cryptographic primitives and their required resources:

- Near-term quantum cryptographic applications essentially rely on primitives using quantum phenomenon to provide secure functionalities for *classical data*. In particular, such primitives and protocols, as it is the case for QKD, do not require long-lived quantum memories.
- Some quantum cryptographic primitives on the other hand explicitly take *quantum information* as input or as output and require technologies that are yet an early-stage in terms of technological readiness, such as long-term quantum storage, or large-scale quantum computing.

Most of the remaining of this manuscript will be devoted to near-term quantum cryptographic applications, and in particular to its flagship primitive, QKD.

Operating quantum cryptography with more advanced technological resources, enabling quantum information storage and processing, however leads to very stimulating, and fundamental questions. It is also becoming a vibrant field of research. Let us hence evoke - even only briefly - some important classes of quantum cryptographic primitives that fall in this category. We also refer the interested reader to [BS16, WEH18] for a more elaborate account on related concepts.

- Quantum money, i.e. the ability to design unforgeable quantum coins (which hence requires long-term quantum storage) whose validity could be verified privately (by the bank) [Wie83]. An important question is to design a scheme allowing for publicly verifiable quantum money [AC12, Zha19].
- Generalization of cryptographic primitives, definition of appropriate security models and constructions, in a setting where quantum information is processed using a quantum computer. This can in particular relate the encryption of quantum information [BZ13, ABF+16].
- Private quantum computation [Fit17]. Considering that future large quantum computers will be mostly accessed through the cloud, there will be a pressing need to

allow for private quantum computation and to develop protocols to address the task of securely delegating quantum computation to an untrusted device while maintaining the privacy, and in some instances the integrity, of the computation. Following the seminal theoretical breakthrough leading to the first protocol for blind quantum computing scheme[BFK09], private quantum computation is a very active research field.

- Multi-party cryptographic protocols on quantum data, operated fully quantum network (often called quantum internet). Application can range from leader election to quantum versions of consensus protocols[WEH18].

2.2 Framing quantum cryptographic advantage

Thoughts and anticipations about quantum technologies are deeply influenced by our understanding of existing - and hence classical- information technologies. A common intuition, rooted in this classical tropism, assumes that the agenda of quantum cryptography consists in proposing a quantum versions all existing classical cryptographic primitives and also that such "quantum translation" could automatically translate into a cryptographic advantage.

This intuition however does not stand a closer scrutiny, on which we will elaborate more in chapter 4. As a matter of fact, quantum cryptographic primitives are often based on core classical resources and protocols. This interplay rules out the possibility of always obtaining a gain by "quantumizing" a cryptographic protocol, since it may result in constructions where the security limitations are classical in their nature.

In addition, as we consider near-term applications, we will not only aim at a theoretical cryptographic advantage, but at an advantage that can be translated in practice. The dialectic between theoretical and practical cryptographic advantage will indeed also be a central question, transverse to several aspects of our work.

Framing these questions requires to look more closely at several key characteristics of the primitive such as the security model, the underlying trust assumptions but also the required resources and their practical availability.

Security model The approach generally adopted in classical cryptography is to rely on *computational assumptions* to build cryptographic primitives [1]. This leads to very efficient, robust and ubiquituous constructions, that constitue an essential pillar of the security of our digital society and economy. Classical cryptographic constructions yet suffer from an inherent weakness: computational assumptions might be compromised at some point in

[1]Some cryptographic primitives such as the One Time Pad, are classical and information-theoretically secure (ITS). Yet, for brevity reasons, we will denote as"classical", computationally-secure cryptographic primitives, and refer to (classical or quantum) ITS primitives, when security is not grounded on computational assumptions

the future, due to advances in algorithmic or in computing power. In particular, in the context of secure communication with classical data, *harvesting attacks* sometimes described as " store now, attack later" are intrinsically always possible, since classical data can be copied at the physical layer, without restrictions. This jeopardizes the ability to guarantee long-term security with classical cryptography.

An essential advantage of quantum cryptography is hence to provide a practical route to realize some cryptographic functionalities with *information-theoretic security (ITS)*, thereby reducing, if not removing the security threats inherent to computational assumptions.

Beyond this fundamental opposition between computational and information-theoretic security, finer-grained variations on the security model can also be very interesting to consider, notably in conjunction with practical feasibility constraints. The underlying assumptions associated to this "fine-grained security models" can in particular be related to:

- *Quantum storage*: physical (technological) limitations on the quantum (but possibly also classical [CM97]) storage capabilities of the adversary, leading to the *quantum bounded-storage* [DFSS08] and the *quantum noisy-storage* [KWW12] models. In such model, information-theoretic security is sought, based on the assumption that the physical limitation holds.

- *Relativistic constraints*: communication limitations related to spatially distributed players and the impossibility to send a signal faster than light [Ken12].

- *Time-dependent definitions* and in particular the notion of *everlasting security*. A protocols enjoys the everlasting security property if it is secure against an attacker that is computationally-limited *only* during the protocol execution, and that is allowed to perform an unbounded amount of computation afterwards. Everlasting security is, from a practical standpoint, not much weaker than information-theoretic security, and yet this relaxation of the security model can lead to decisive gains, in terms of practicality. We will present our work exploring this direction, based on a quantum-computational hybrid security model, in chapter 5. Another very interesting example of time-related security definitions is the notion of revocable time-release encryption introduced by Unruh [Unr15].

Functionality and trust model Cryptographic primitives are naturally characterized by their functionality, such as random number generation, secret-key encryption, keyed hashing or bit commitment scheme. Trust model is another crucial characteristic, intrinsically related to the inner working of the functionality and however often less scrutinized.

For one part, the trust model is related to the trust relations between the different players of the cryptographic primitive, and is therefore associated with the structure of the functionality. For example, coin tossing is a 2-party cryptographic protocol, that only makes sense if the two parties do not trust each other. Quite differently, key establishment is a 3-party protocol, with two legitimate users, commonly called Alice and Bob trusting

each other and aiming to establish fresh new key material, secure against a third party, the attack attacker Eve that is hence untrusted.

Trust models are also related to *physical trust assumptions* that play a central role in the practical security of real-word cryptographic system implementation. Such assumptions indeed play a particular role in quantum cryptography. As a matter of fact, quantum cryptography is intrinsically based on a formalized description of the physical layer, that allows to use specific verification methods to assess and assess the validity of the model, along three main lines:

- Evaluate and experimentally test the implementations following a best-practice approach, in order to certify the security assurance of a quantum crypto-system. Such approach is in many aspect similar to the approach used to evaluate the implementation of security classical crypto-sytems such as smartcards, with the notable difference that the tolerable deviations between theoretical model actually system, can formally evaluated in the case of quantum crypto-systems for which the physical description of the ideal system is perfectly set.

- Rely on specific properties, of quantum correlation, such as entanglement or steering to conduct some "self-testing" of the quantum states shared by the legitimate players, for example by testing some Bell inequalities to certify entanglement. Such techniques are also known as *device-independent* techniques, and are totally specific to quantum information processing. In a cryptographic setting, device-independent techniques may allow to conduct some quantum cryptographic protocols without the need to trust the the physical implementation of the devices.

2.3 Functional overview of quantum cryptographic primitives

2.3.1 Local randomness generation

Generating random numbers is certainly one of the most foundational primitives in computer science, with applications in numerical simulations, lotteries or fundamental tests in physics. In the context of cryptography, randomness generation is a primitive that can be performed locally, by one player, and is for example needed to generate cryptographic keys. Its security is captured by the notion of *impredictability*: an attacker should not be able to guess (better than a random guess) the next bit of the random sequence, knowing the previous ones.

Under computational assumptions, related to the existence of secure one-way function and hardcore predicated, pseudo-random generators (PRNGs) can be constructed [KL14], and PRNGs. It might however be considered risky, from a security viewpoint, to rely on a computational assumption to generate random bits, since a computer is fundamentally a deterministic state machine, and the sequence of bit it can produce cannot be more random than the initial seed of the PRNG . Von Neumann somehow expressed this concern in his famous say "Anyone who considers arithmetical methods of producing random digits is,

of course, in a state of sin". Another striking illustration of the issue one can encounter with a PRNG, is that the algorithm might have been intentionally flawed to contain a backdoor, as it has been the case with Dual_EC_DRBG (Dual Elliptic Curve Deterministic Random Bit Generator) as revealed by Edward Snowden based on a leaked NSA memo [Lan14]. Such backdoor in a PRNG, that was part of a standardized cryptographic suite could in particular impact the security of cryptographic key generation, by making such keys predictable for the NSA .

There is therefore a compelling need to produce "true" random numbers, that could constitute a guaranteed source of entropy even in adversarial settings, and we know that such true random number generators (TRNGs) cannot just be digital, and must instead rely on some physical hardware able to generate some physical output that is sampled in order to obtain an entropy source. "Classical" TRNGs exist and are commercially available. They typically consist in high-dimensional and chaotic physical systems, such as ring oscillators or thermal noise in resistors.

Quantum random number generators (QRNGs) constitute a special kind of hardware-based TRNGs, where the physical systems that is measured, in a quantum system in some superposition of the measurement eigenstates [HCea17]. This leads to measurement outcomes that constitute a "natural" entropy source, that still need to be classically processed with a randomness extractor, in order to provide almost uniform randomness.

QNRGs come in two main flavors:

- *Prepare and measure QRNGs (PM-QRNGs)*, for which the quantum state preparation and measurement device need to be trusted. An interesting research question would consist in clarifying to which extend PM-QRNGs differ, from a security standpoint, from other hardware-based TRNGs. Such difference might stem if some specific vulnerability of chaos-based systems to injection attacks, able to strongly reduce their output entropy [MM09], could be proven to be generic.

- *Device-independent QRNGs (DI-QRNGs)*, Violation of a Bell inequality test, run between two distant parties, could not be faked by correlated classical data, and imply the statistical independence of the measurement results with respect to one another. Such fundamental quantum behavior can be used to produce random bits, in a device-independent fashion, i.e. without trusting the implementation details such as state preparation and measurement. In case loophole-free Bell test can be experimentally performed, which requires to close detection and locality loopholes, then fully device-independent randomness generation can be be provided (actually randomness expansion from a small seed [CK11]), as it has been the case for the first time in [PAM$^+$10], with ions (but only closing the detection loophole) and then in [GMR$^+$13] with a source of entangled photons.

2.3.2 Key establishment

Distributing cryptographic secret keys among a set of legitimate users is a central problem in cryptography. Before the advent of public-key cryptography in the 1970's, sharing a symmetric key between the sender and the receiver was a prerequisite to establish a secure channel, with the issue that the distribution of initial secret keys had to be performed outband, typically using secret couriers, making it difficult to manage over large networks, without a centralized and trusted operator. This issue, known as the *key establishment problem* has been a structural problem that has had a deep impact on the deployment and the practical operation of cryptography until the 1970's. The invention of public-key cryptography in 1976 [DH76] has litterally lead to a revolution of our digital society, enabling a whole new set of secure functionalities over open networks, and in particular digital signature and key establishment, even between users that do not initially share a secret, therefore offering a solution to the key establishment problem. More broadly public-key cryptography has provided the security foundations for the development of Internet.

Quantum key distribution (QKD), invented in 1984 by Charles Bennett and Gilles Brassard [BB14] based on some earlier ideas of Stephen Wiesner [Wie83] is a quantum cryptographic alternative solution to the secret key establishment problem. It is a 3-party primitives, with two trusted parties (Alice and Bob) and an eavesdropper, Eve. Rigorously speaking, QKD should be called quantum key agreement, or quantum key establishment, since the secret key shared at the end of the protocol is not decided upon solely by one of the player and then distributed to the other. However, the expression "quantum key distribution" and the acronym QKD are now firmly established.

Contrary to the computationally-secure secret-key and public-key schemes for key establishment, QKD is information-theoretically secure (ITS), i.e. secure irrespectively of the computing power that may be used by an attacker [May01, BBB$^+$06, SP00]. In particular QKD is secure even against an attacker equipped with a quantum computer, and yet can be operated with available technology. QKD hence offers a solution for ITS key establishment, while this primitive impossible to realize with classical means [2]

It is interesting to note that information-theoretically secure classical secret key agreement, by public discussion, over an untrusted channel is possible [Mau93], and that such work has played an important role in establishing the theoretical foundations of QKD security [BBCM95]. ITS classical secret key agreement however typically requires settings with additional assumptions, such as the wire-tap channel [Wyn75] or the satellite scenario [Mau93] that allow to guarantee that the amount of information accessible to Eve remains bounded to a level below with the mutual information between Alice and Bob. In this perspectives, the striking advantage of QKD is to use fundamental quantum properties, and in particular measurement-disturbance trade-off, to upper the information leaked to Eve, therefore alleviating the need for additional assumptions.

[2] Whether practical QKD can serve real-world applications, with an effective advantage with respect to classical alternatives, will be evoked in more depth in the next chapters.

2.3.3 Secure multi-party computation between untrusted parties

Secure multi-party computation (MPC) protocols enable a set of parties to interact and compute a joint function on their private inputs while revealing nothing but the output of the computation. As opposed to cryptographic protocols for secure communication, the parties in a MPC protocol a priori do not trust each others and may act according to different adversarial models such as *honest but curious* or *malicious*. MPC enables organizations to analyze big data collaboratively without requiring them to reveal any private information. As data is increasingly located in cloud premises, the potential of applications for MPC is considerable, ranging from for private information processing to threshold cryptography.

Oblivious Transfer (OT) is another abstract MPC primitive, that can be used as a building block for any arbitrary secure multiparty computation protocol (including bit commitment (BC)).

OT can be realized from computational assumptions, and in particular the existence trapdoor one-way functions as shown by Rabin in 1981 [Rab05] . It is however impossible to realize OT with information-theoretic security[Bea96]. A natural and important question for quantum cryptography is therefore whether OT can be realized with information-theoretic in a quantum setting.

Oblivious Transfer can be captured by two protocols, the one introduced by Rabin [Rab05] and **1-out-of-2-OT**, that has been shown to be equivalent to Rabin OT [Cré87] and that we shall describe here.
The principle of 1-out-of-2-OT, between two parties Alice and Bob that do not trust each other, is the following:

- Alice chooses as input two bits b_0 and b_1.
- Bob chooses a selection bit c and gets as output the bit b_c.

A protocol realizing OT is said to be secure if none of the parties learn any more information than what she is supposed to learn according to the protocol definition (for example a 1-out-of-2-OT would be insecure, if A could learn bit c or if B could both bits b_0 and b_1).

Following the first breakthrough result in quantum cryptography, with the BB84 QKD protocol, a long series of work has studied which other MPC cryptographic primitives are possible in the quantum world.

However, the subsequent results were negative as Mayers and also Lo and Chau proved in 1997 the impossibility of secure ideal quantum bit commitment and oblivious transfer and consequently of any type of two-party secure computation [May97, Lo97, LC97], with information-theoretic-security. The intuition behind this no-go result is that entanglement can be always be used to establish cheating strategies that cannot be detected by an honest player.

Under additional physical limitations, secure OT is however possible and this is in particular the case if Bob has a bounded [DFSS08] or a noisy quantum memory [KWW12], but also based on relativistic constraints [KTHW13, PGea18].

Another important 2-party primitive is *coin flipping over the telephone* (that we will simply denote as coin flipping), which was first proposed by Blum [Blu83] and has since found numerous applications in two-party secure computation. Even though the results of Mayers and of Lo and Chau exclude the possibility of perfect quantum coin flipping, i.e., where the resulting coin is perfectly unbiased, it still remained open whether one can construct a quantum protocol where no player could bias the coin with probability 1.

Aharonov et al. [ATSVY00] indeed provided a quantum coin flipping protocol where no dishonest player could bias the coin with probability higher than 0.9143. A series of work then tried to investigate how low the cheating probability of a dishonest player could be, in a quantum setting. Kitaev established a $1/2$ lower bound for the product Alice and Bob cheating probabilities, therefore leading to a $\frac{1}{\sqrt{2}}$ lower bound in the case where Alice and Bob cheating strategies are symmetric. Again a series of theoretical advances, and the construction of an optimal weak coin flipping protocol by Mochon [Moc07], culminated into a quantum (strong) coin flipping protocol, with almost optimal cheating probability, $\frac{1}{\sqrt{2}} + \epsilon$ [CK09].

Table 2.1: Overview of near-term quantum cryptographic primitives.

	Functionality	Security Model & Trust assumptions	Feasibility & Practicality: Performance vs Requirements
RNG	QRNG	ITS, trusted implementation	High maturity: TRL ≥ 8, QRNG on chip, Gbit/s rates, first certifications [HCea17].
	DI-QRNG	ITS, untrusted quantum hardware	First demos: require loophole-free Bell tests, very low rates [PAM$^+$10].
KE	QKD	ITS, trusted implementation	High maturity: TRL ≥ 8, Mbit/s rates at 50 km, 1b/s at distances ≥ 300 km, chip-level integration of components [XMZ$^+$20].
	MDI-QKD	ITS, trusted emitter, untrusted receiver	TRL ≥ 6, kbit/s rates at 50 km [XMZ$^+$20].
	DI-QKD	ITS, untrusted quantum hardware	Theoretical advances towards feasibility [SBV$^+$20].
	DI-QKD	Bounded storage, untrusted quantum hw	Improves loss and error-tolerance w.r.t ITS [PMLA13].
MPC	OT, BC	ITS	Impossible [May97]
	OT, BC	Bounded Storage (BS) Noisy Storage (NS) Relativistic	OT, BC feasible under BS and NS models [KWW12] and under relativistic constraints [PGea18].
	Coin Flipping	ITS	Almost optimal cheating probability of $\frac{1}{\sqrt{2}} + \epsilon$ for strong coin flipping [CK09].
	Secure Identification	BS or NS	Password-based identification with minimal information leakage [Sch10]

Chapter 3

Quantum communication engineering

QKD is one of the most mature quantum technologies [LT19]. Its development is intrinsically related to the ability of enabling security applications with security levels (notably information-theoretic-security) unachievable classically. This "cryptographic facet" of QKD has been contextualized in the previous chapter and will be the focus of the next chapter.

In this chapter, we want to focus on the "communication facet" of QKD and on the driving role that quantum key distribution is playing on the development of quantum communication research and technologies. Addressing some of the associated quantum communication challenges has been one of the important objectives of my research work, with associated contributions ranging from QKD system engineering [LAB+08, JKJD+12, MA17] to Quantum communication networking [ARDL09, PPA+09] , including the integration of QKD over existing classical WDM optical networks [KQA15, AAWJ20], that we will now review and put in context in this chapter.

3.1 QKD communication processes and channels

A QKD system is for a large part an optical communication system that bear important similarities with classical optical communication systems. In the ETSI QKD Group Specification 012 [All19b], we have described the main communication resources involved in a QKD system. We have in particular classified the three main logical communication channels, according to the related logical communication processes, as described in Table 3.1. This breakdown of a QKD system into 3 communications processes happens to be useful to structure the description of quantum communication challenges and also to position our work on QKD system design and development.

Table 3.1: QKD System Communication Processes and Channels

Channel Name	Communication Process Description	Remark
Quantum Channel	Alice encodes classical information on quantum states and sends those quantum states on the quantum channel to Bob	The quantum states should not be distinguishable and hence need to form a non-orthogonal set.
Synchronization Channel	Alice prepares classical analog optical signals (needed for reference sharing purposes) and sends those signals on the Synchronization channel to Bob.	The synchronization channel is in general implemented over the same physical channel as the quantum channel, yet this is not compulsory, and another physical channel might be used.
Distillation Channel	Alice and Bob exchange classical messages between Alice and Bob, to perform Sifting (agree on the raw data to be retained for subsequent classical post-processing) and Classical post-processing.	The physical interface used for Distillation (or Post-processing) channel, can be independent from the one used for the quantum channel.

3.2 DV and CV Quantum communication technologies

Quantum communication technologies can be categorized according to the dimensionality of the Hilbert space supporting the quantum signals.

- Discrete variable (DV) schemes, where information is encoded over a finite-dimensional Hilbert space. In the context of quantum communications, this corresponds to schemes where information is encoded in finite dimension d, and detected using a measurement able to discriminate orthogonal qudit states. Such measurement is in general implemented using, a mode-sorting scheme (for example, depending of the nature of the encoding: a polarizing beamsplitter, an OAM sorter or a wavelength-division demultiplexer), followed by single-photon detectors (SPDs). Several prominent practical DV-QKD systems rely on phase-encoding over time-bin qubits ($d =$

2)[FLD+17, BBR+18].

- Continuous variable (CV) schemes, where information is encoded over an infinite-dimensional Hilbert space. In the context of quantum communications, this corresponds to schemes where information is encoded over the quadratures of one mode of the electromagnetic field. Quantum measurements on such a system can be performed using coherent receivers: homodyne and heterodyne (also-called dual-homodyne) detectors [DL15]

Our work on QKD system engineering has been mainly focused on CV-QKD. We propose a brief CV/DV comparison, that is interesting as both quantum technologies have relative merits and drawbacks, as illustrated in Table 3.2: DV-QKD systems enjoy a stronger tolerance to optical losses, while CV-QKD are particularly interesting on shorter distances, due to their engineering convergence with classical coherent communications as well as their native coexistence capability with WDM classical signals [KQA15]. DV and CV encodings should in any case not be opposed. They constitute a precious toolbox for quantum communications and for quantum information processing and can moreover be advantageously combined for some applications [ANNVLF15].

Table 3.2: DV and CV-QKD technology: elements of comparison

DV-QKD	CV-QKD
Long reachable distance achievable with current detectors Typically 150 km- 200 km can be reached (1 bit/s limit around 300 km)	More sensitive to loss Distance limit demonstrated: 25 km in 2007 [LBGP+07], 80 km in 2013 [JKJL+13a] Cf subsection 3.3.2, 150 km in 2020 [ZCP+20]
DV-QKD key rate is not very sensitive to reconciliation efficiency	CV-QKD has more complex post processing and is very sensitive to reconciliation efficiency. Need for specific highly efficient error correction codes. Cf subsection 3.3.2
Single photon detectors need to be cooled (-30°C for APDs, 4K for SNSPDs)	Coherent receivers can be operated at room temperature
Single photon detectors are sensitive to stray light.WDM integration requires high filtering	Coherent detector act as selective spectral filters well fit for WDM integration, Cf section 3.4.2.
No need of phase reference (phase randomization is actually better for security)	Need of a shared phase reference between Alice and Bob, Cf subsection 3.3.1

3.3 CV-QKD System Engineering

3.3.1 Quantum coherent communication

In [AM16], and in the subsequent patent [MA17], we have addressed a central issue in CV-QKD system design, namely to jointly operate CV quantum communication and phase reference sharing with the objective to improve either on the performance or on the hardware requirement, and therefore cost, with respect to early work on this emerging topic [QLP+15, SBC+15, HHL+15], that is now dominating the research agenda in CV-QKD system design.

Phase reference sharing is a specific challenge for quantum coherent communication protocols. As a matter of fact, the receiver must perform a phase-sensitive detection using an optical beam usually called "local oscillator" whose phase drift with respect to the emitter must be controlled, or estimated, and corrected. The problem of sharing a reference frame is specific in the sense that reference frame information constitutes *unspeakable information*, that can only be shared through physical carriers exchanged between emitter and receiver. On the other hand, it is important to emphasize that although quantum mechanics gives a precise framework to formulate the question of reference frame sharing, in relation with quantum metrology [BRS07], this question can be solved "classically", using macroscopic signals to exchange reference frame information. The type of questions related to phase reference sharing is not whether it is possible, but whether it can be achieved given resource constraints, dictated by the hardware resources and by the characteristics of the channel, such as losses and noise.

The Transmitted Local Oscillator design. In most implementations of CV-QKD performed before 2015 [HLW+15, HFW+13, JKJL+13b, QHQL07], the phase reference is directly transmitted from Alice to Bob through the optical channel as a bright optical pulse with each quantum signal pulse and is used as the LO pulse at reception. Such implementation is detailed in Fig. 3.1 and is referred to as the Transmitted LO (TLO) design. The main advantage of this scheme is the guarantee, by design, of a stable relative phase between quantum signal and LO at reception by producing both of them from a single laser L_A placed at Alice's side. Despite it is the most implemented GMCS protocol, limitations of this design have been pointed out in [QLP+15, SBC+15, HHL+15]. Security weaknesses of such implementations have however been demonstrated in practice by manipulating the LO intensity [FGG07, MSJ+14, JKJD13] or wavelength [HWY+13a] on the quantum channel. Furthermore, such protocols rely on the use of a bright LO at reception. For long distance or high speed (where the pulse duration is short), the requirements in terms of launch power at emission creates practical issues. This will in particular limit the possibility of using the TLO design on shared optical fibers at long distance and high-rate operation, i.e. situations where the requirements on LO power at emission would be extremely large.

The Local Local Oscillator method. In order to lift the limitations of CV-QKD implementations relying on the TLO design, a new CV-QKD method relying on a "local local

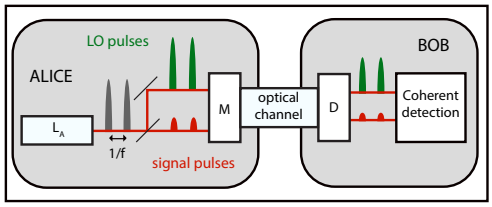

Figure 3.1: *(color) Transmitted local oscillator (TLO) design. In the TLO design, the phase reference (green pulse) and the quantum signal (red pulse) are derived from the same optical pulse and sent from Alice to Bob using multiplexing/demultiplexing (M/D) techniques.*

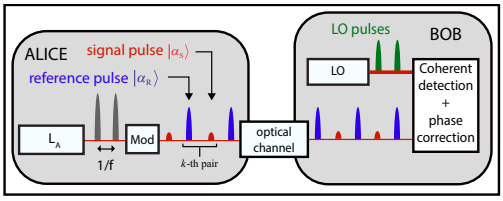

Figure 3.2: *(color) Local local oscillator (LLO) sequential design. In the LLO-sequential design, Alice sequentially sends weak quantum signal (red pulse) and bright phase reference (blue pulse) pulses. At reception, Bob performs consecutive coherent detections of each pulse received using is own LO pulses (green pulse).*

oscillator" (LLO) has been independently introduced in [QLP+15, SBC+15, HHL+15]. This method, implementing the Gaussian modulated coherent state protocol, consists in using a second laser at Bob's side in order to produce local LO pulses for coherent detections. One crucial advantage of implementing CV-QKD in a LLO configuration is to close, by design, any potential security loophole linked to the possibility of manipulating the LO as it propagates on the public optical channel between Alice and Bob. Implementing LLO CV-QKD allows on the other hand to ensure by design that the LO is fully trusted, and in particular that the LO amplitude (that requires careful calibration) cannot be manipulated. Another important advantage of LLO CV-QKD stems from the fact that in this configuration, repetition rate and distance do not affect the LO intensity at detection. A LO power sufficient to ensure high electronic to shot noise ratio may thus be obtained, independently of the propagation distance.

Implementing CV-QKD in the LLO configuration however comes with new experimental challenges. The main issue in LLO-based CV-QKD is to be able to perform CV-QKD despite the potentially important drift of the relative phase between Alice's emitter laser L_A and Bob's local oscillator laser L_B, see Fig. 3.2. The relative phase at reception is, in the case of LLO-based CV-QKD, the relative phase between the two free-running lasers L_A and L_B. As such, Bob's raw measurement outcomes are *a priori* decorrelated from Alice's quadratures and a phase correction process has to be performed in order to allow secret key generation. The goal of the phase reference sharing in the context of LLO CV-QKD is then to ensure a low enough phase noise so that the excess noise is significantly below the threshold imposed by security proofs [DL15].

Our Contribution in [AM16, MA17]: we have analyzed some limitations in the LLO sequential method implemented in [QLP+15, SBC+15, HHL+15], where time-multiplexing between quantum signals pulses and reference pulses was used in order to jointly perform phase recovery and quantum communication. We have then introduced new ele-

Design	Trusted LO	Tolerable phase noise	Hardware requirements
Transmitted LO (Fig. 3.1)	No	$\Delta\nu/f \sim 10$	Stable interferometric set-up
LLO-sequential (Fig. 3.2)	Yes	$V_{\text{drift}} \sim 10^{-1}$ (60dB AM) $V_{\text{drift}} \sim 10^{-3}$ (30dB AM)	High AM dynamics

Table 3.3: Summary of the advantages and drawbacks of Transmitted LO and LLO-sequentional CV-QKD designs (cf Figure 3.1 and 3.2).

ments in the standard noise model of CV-QKD analysis, considering new practical constraints imposed by the simultaneous quantum signal and phase reference transmission of LLO-based CV-QKD. In particular, we show that the amplitude modulator dynamics is a key parameter in order to compare performance of realistic implementations of LLO-based CV-QKD. Based on this comprehensive model, we show that there exist fundamental and practical limitations in the phase noise tolerance of the design introduced in [QLP+15, SBC+15, HHL+15], that we designate as LLO-sequential.

In order to go beyond this phase noise limit, we have introduced the idea of self-coherence in phase reference sharing for CV-QKD implementations based on a local local oscillator. Self-coherent designs consist in ensuring the phase coherence between pairs of

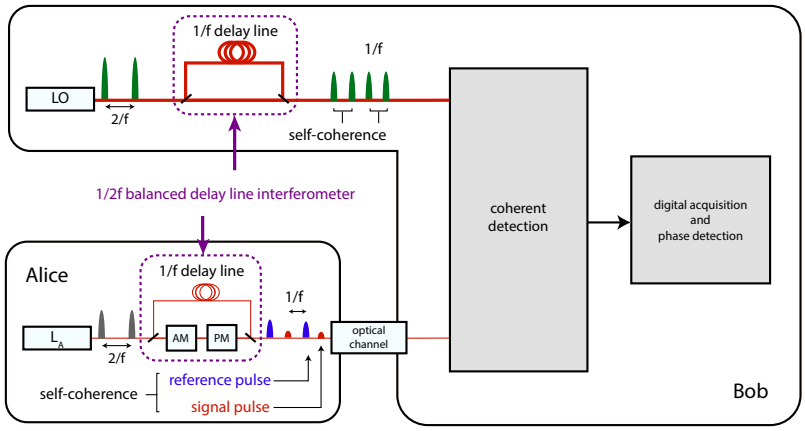

Figure 3.3: *(color) LLO-delayline design. Alice sends consecutive phase coherent signal/reference pulses pairs to Bob based on a balanced delay line interferometer. On his side, Bob uses his own laser as the LO for coherent detections using the same delay line technique to produce phase coherent LO pulses. Phase estimation and phase correction are digitally performed after measurement acquisition.*

quantum signal and phase reference pulses by deriving both of them from the same optical wavefront at emission. This allows to perform relative phase recovery schemes with better sensitivity than in the LLO-sequential design. In particular, we have proposed a design, called LLO-delayline, implementing a self-coherent phase sharing design. It ensures the self-coherence using a balanced delay line interferometer split between emitter and receiver sides as depicted on figure 3.3. We have analyzed how self-coherence is obtained and studied the performance reachable with this design, demonstrating that they exhibit a much stronger resilience to high phase noise than the LLO-sequential design under realistic experimental parameters. While previous experimental proposals of LLO CV-QKD are limited to slowly varying reference frames regimes (ie. based on very stable lasers or high repetition rates), our newly introduced design allows phase reference sharing resilient to high phase noise regimes, using the idea of self-coherence.

A second self-coherent design, referred to as LLO-displacement, relies on an original multiplexing allowing to transmit both the quantum signal and the reference pulse within each optical pulse. The simultaneous transmission of quantum signal and phase reference can be seen as an original cryptographic primitive, considered in [Qi16], that can be used with different modulation schemes. In particular, this allows to optimize the resources − in terms of required hardware and repetition rate − in LLO-based CV-QKD experiments. We have studied the theoretical performance of such design and exhibit its limitations, in terms of phase noise tolerance. An important advantage of our LLO-displacement design is however its experimental simplicity, since no specific hardware devices are required. Interestingly this design has been experimentally validated and further developed into the first simultaneous quantum and classical communication scheme proposed by Qi and Lim [QL18].

3.3.2 Classical post-processing

Key distillation, and more generally the classical post-processing operations that follow the quantum communication (and sifting) phase, can be fully implemented over a classical channel, possibly independent from the physical channel on which quantum communications take place [All19b].

The design and optimization of key distillation is essentially a classical problem. It consists in core operations such as error correction and privacy amplification, that are not specific to QKD, and have been first proposed by Maurer et al., in the context of information–theoretic secret key agreement by public discussion [Mau93, BBCM95].

Practical QKD classical post-processing however leads to specific regimes, and constraints, in particular on the error correction phase. As a matter of fact, even though Shannon's coding theorem indicates the existence capacity achieving codes, the rate R of practical error correcting codes, with a finite number of signals and effective decoding scheme, typically bears some penalty with respect to Shannon's capacity C , that we can designate by the efficiency $\beta \equiv R/C < 1$. The practical constraints and the impact of non-ideal error-correction greatly vary between CV and DV-QKD. In the case of CV-QKD, the

requirements associated with error-correction are particularly high, for two main reasons.

- First because CV-QKD quantum communication is characterized by a very low signal to noise ratio (SNR), with noise variance above 1 shot noise unit while the signal variance is typically much weaker, in particular at long distance.
- Second because the volume of raw key, to be error-corrected, is not decreased by losses and remains directly proportional to the number of signals emitted by Alice.

Error correction typically can hence constitute a bottleneck for modern CV-QKD system performance. While Gaussian protocols can provide the highest key rates and already enjoy the strongest proofs, [DL15], error correction is especially challenging in that case. Early implementations used sliced reconciliation to map infinite-dimensional modulation signals to a discrete alphabet, leading however to reconciliation protocols that were highly inefficient (small β) at low SNR. In [LAB+08], we proposed a method based on eigth-dimensional reconciliation, allowing to efficiently map ($\beta > 95\%$), without post-selection, CV-QKD signals to a high-dimensional binary alphabet, onto which specific LDPC codes can be applied. This technique has allowed a very significant leap in performance, from a reach of about 25 km in [LBGP+07], to 80 km in [JKJL+13a], as illustrated on figure 3.4

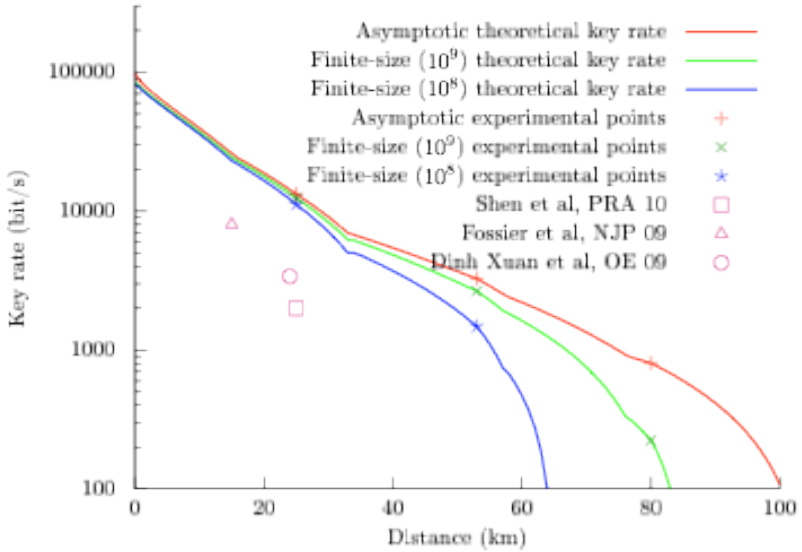

Figure 3.4: Key rate versus distance of the CV-QKD experiment [JKJL+13a]. This illustrates the performance leap obtained in particular by significantly improving the error-correction efficiency β at long distance (low SNR), using multidimensional reconciliation from [LAB+08]

State-of-the art implementations for CV-QKD error-correction, based on LDPC and implemented over a GPU, currently reach a maximum throughput below 100 Mbit/s [LZL+20]. With the increase of clock rate from MHz to GHz and the convergence with

DSP-based coherent communications, high-speed modern CV-QKD implementations may however require to process and error-correct raw key at Gbaud rates, which is hence currently not feasible or highly cumbersome. This situation will certainly call for further advances either in error-correction algorithms, post-processing hardware, CV-QKD protocols, and possibly a combination of them. In this perspective, recent advances on establishing the security of CV-QKD with a discrete modulation [GGDL19, LUL19] appear as a promising direction towards high-speed CV-QKD with real-time post-processing.

3.3.3 Engineering a high TRL system

Technology Readiness Level (TRL) TRLs measure the maturity level of a technology throughout its research, development and deployment phase progression. TRLs are based on a scale from 1 to 9, with 9 being the most mature technology.

Figure 3.5 displays the European TRL scale. TRLs plays a central role in the transition from research prototypes (TRL 1-4) to industrial systems (TRL 7-9). It also certainly plays a central role in European Commission Call for Projects!

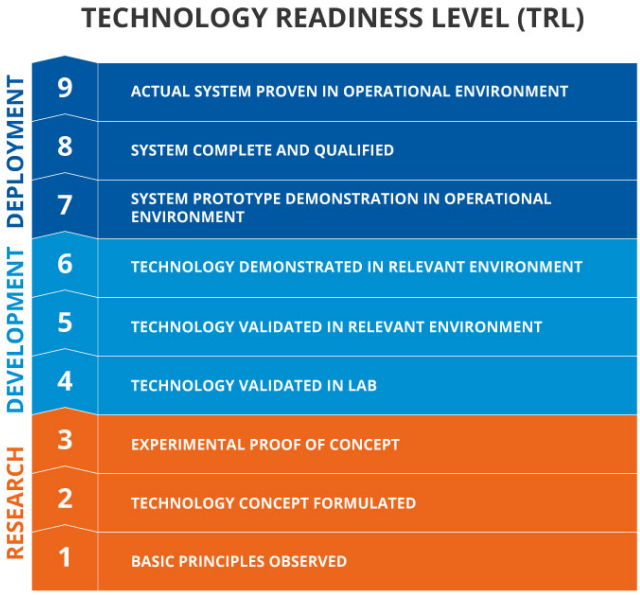

Figure 3.5: Technology Readiness Levels scale, used in Horizon 2020 program.

QKD is one of the first quantum technology that has been able to climb the TRL ladder, reaching TRL 7-9 about a decade ago for DV-QKD systems [IDQ21]. Concerning CV-QKD technology, SeQureNet, spin-off of Telecom Paris(Tech), that I have co-founded in 2008, has actively contributed to push forward the industrialization of the technology during the period 2010-2014. We report here on a some salient aspects of this work in the next two

paragraphs, before considering today's landscape and challenges in the final paragraph.

System integration One stringent requirement to evolve from a laboratory system to a field demonstration is the ability to operate the system with higher reliability, combined with the ability to move the system and make sure it meets field requirements, notably in terms of packaging, operating conditions and stability.

Regarding the developments performed by SeQureNet and initially Telecom ParisTech, they inherited from 10 years of work, performed at Institut d'Optique and Thales Research and Technology, following the invention of CV-QKD by Frederic Grosshans and Philippe Grangier [GG02]. Its first experimental demonstration [GVAW+03] has been followed by steady improvements, culminating in the development of an autonomous CV-QKD system in the context of SECOQC demonstration [PPA+09], typically reaching TRL5.

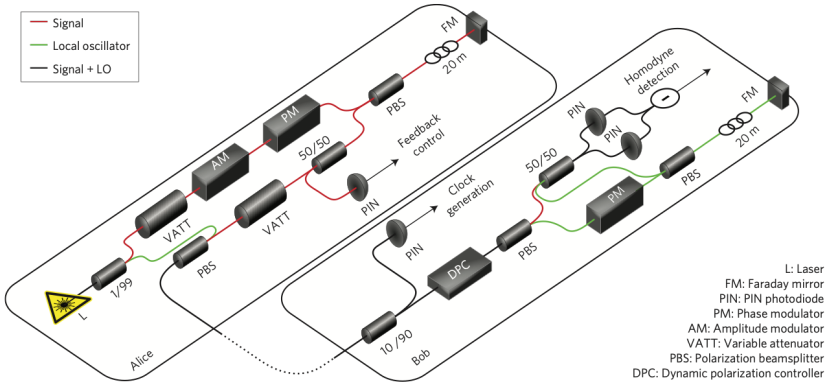

Figure 3.6: Optical design of the Cygnus CV-QKD system

SeQureNet has developed, and commercialized for the first time globally in 2013, a CV-QKD system named Cygnus (cf. Figure 3.6). Cygnus was designed to allow field tests and integration experimentation by academic for industry players interested in testing and further developing CV-QKD technology.

The starting point was the CV-QKD system used for the SECOQC demonstration, during the PhD thesis of Jerome Lodewyck, in collaboration between IOGS (Philippe Grangier) and TRT (Thierry Debuisschert). Several improvements have been performed to bring the system to TRL7:

- At the hardware level: minor modifications of the optical design have been operated, with the removal of one amplitude modulator (on Alice side). The system architec-

ture is depicted on figure 3.6. Special efforts have been invested to improve the SNR and stability of clock recovery signals (Alice-Bob synchronization). The system repetition rate has been set to 1 MHz, compatible with the rate of high-clearance (20 dB) custom shot-noise limited homodyne detection developed at IOGS [LBGP+07].

- The main modifications, and the core work needed to increase the stability and performance of the CV-QKD system lie on the software side. The software stack has been fully rewritten, with new feedback control loops, improved procedures for parameter estimation and original (inventive) algorithms for phase stabilisation, synchronization. Additional efforts were related to a better separation of functionalities, and a clean management of scheduling. This lead to a more stable and more evolutionary system.

- New algorithms, for reconciliation have been written, based on the work described in 3.3.2. They rely on efficient LDPC codes, implemented on GPU and fast privacy amplification algorithm.

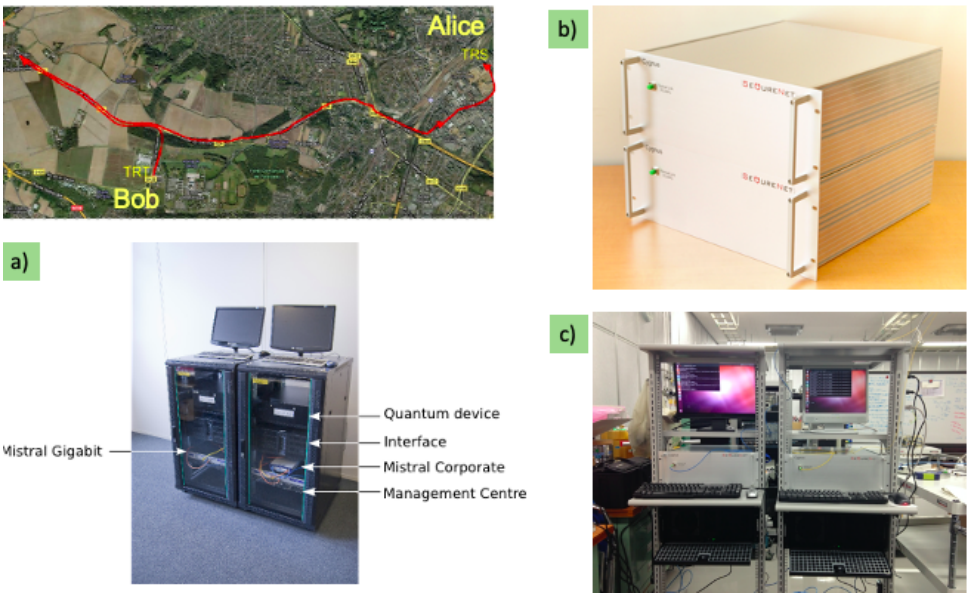

Figure 3.7: a) Map of the 18 km field-test combining CV-QKD with encryptors [JKJD+12] b) Cygnus: first commercial CV-QKD system, released by SeQureNet in 2013 c) Cygnus deployment within the Tokyo QKD network (2014).

Field deployments QKD is the first quantum communication technology to have reached a maturity level sufficient to allow field deployments. This requires to meet an ensemble of requirements related to stability, noise robustness, integration and interfacing, allowing to climb from TRL4-5 to TRL larger than 7.
The work conducted at Telecom Paris in the context of a French ANR project SEQURE al-

lowed to perform the first long-term (several weeks) field demonstration of CV-QKD interfaced with Layer 3 encryptors, [JKJD+12] . Increased software stability has been achieved by suppressing memory overflow issues that were previously limiting autonomous system operation. On Figure 3.7 a), we can see the map of the 17.7 km field demonstration, performed in 2011, linking Thales R & T (Palaiseau) to Thales Raytheon Systems (Massy), together with a picture of the two integrated systems, combining CV-QKD devices and Mistral encryptors from Thales.

As detailed in the previous paragraph on System integration, the work accomplished by our spin-off SeQureNet addressed additional challenges, related in particular to error-correction and system integration. This has lead to the release of the first commercial CV-QKD system in 2013, based on a transmitted local oscillator (TLO) design. This system, called Cygnus, integrated in 19" racks, is depicted on Figure 3.7 b), it has been successfully commercialized and deployed, as illustrated on Figure 3.7 c), with the integration of Cygnus CV-QKD systems in the Tokyo QKD network.

3.4 Quantum communication networking

The challenge of "networked quantum information" also often designated as "quantum networks", is becoming central to quantum technologies, starting with quantum communications, but also with the vision of connecting quantum sensors and quantum computers in the future. This is illustrated by recent recent program targetting the development of Quantum Interconnects (QuIC) [HQI21] enabling the transmission of quantum information between classical and quantum machines, using heterogeneous quantum platforms. At larger scales, the development of a Quantum Internet connecting spatially distributed quantum computers and sensors and opens radically new perspectives in terms of information processing and constitutes a federative objective [WEH18].

In line with the angle that we chosen manuscript and in coherence with our research work, we will focus on QKD networking. We will first review some important questions, related to the architectural design and the topology of QKD networks, and detail how we have contributed to some of the early works on these topics [ARML06, ARDL09, SPD+10] . We will then focus on one central question for the feasibility of quantum networks: the ability to deploy quantum communications in coexistence with classical communications, on existing fiber network infrastructure, and how it may influence future technology development [KQA15, AAWJ20]. Finally, we will explore some future challenges in quantum networking and discuss the role of QKD networking in this more global picture.

3.4.1 QKD networks

The deployment of large-scale QKD networks, such the infrastructure gradually deployed in China (cf. Figure 3.8) over the past 5 years [CZC+21] , certainly constitute one of the most striking illustration of the progress achieved by quantum technlogies, and their ability to revolutionize the future of information technologies.

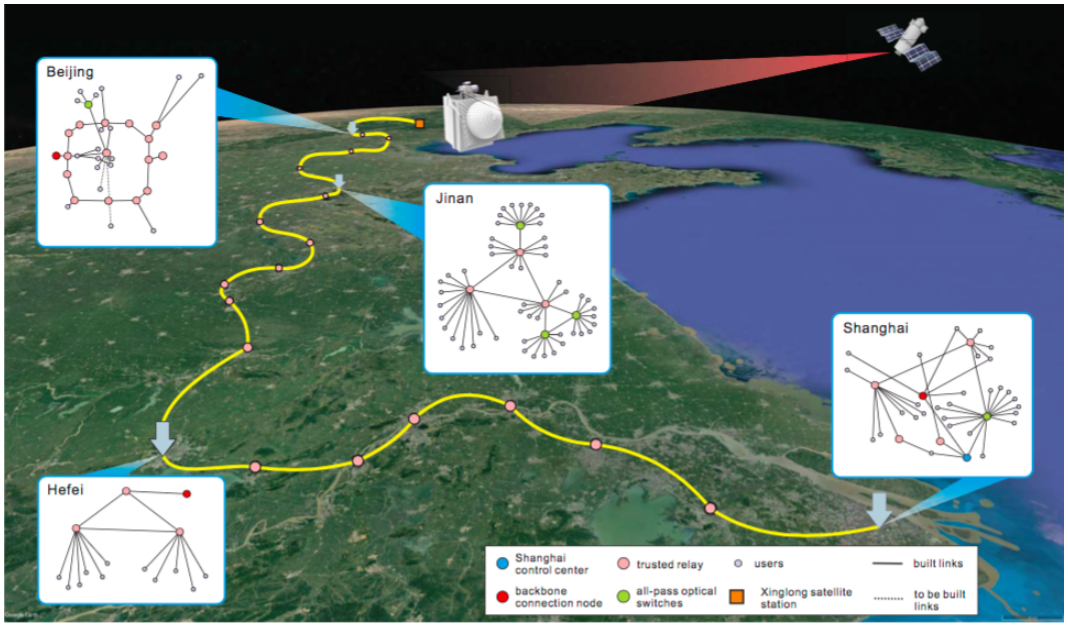

Figure 3.8: Quantum Key Distribution network in China [CZC+21], with a terrestrial part composed of a 2000 km quantum backbone, connecting several metropolitan QKD networks. It is complemented by a spatial segment, that has been illusrated by the Micius satellite demonstration demonstration [YLL+20]

Architecture of quantum networks

The European project Secoqc has constituted one of my first professional undertaking, following my PhD. I was in charge of the Secoqc "NETWORK Work-Package" and thereby started to investigate how classical networks operate, in order to understand what reasonable architecture could be proposed for QKD networks. This work lead to a series of works and talks, in collaboration, notably, with colleagues at the Austrian Institute of Technology that were coordinating the Secoqc project.

A central outcome of this work has consisted in proposing, for the first time, a logically layered architecture for QKD networks, with three different layers:

- The QKD layer, that is also a physical layer where optical QKD quantum channels are implemented, on a point-to-point basis, between QKD endpoints, placed in QKD (trusted) nodes.
- The Secrets layer, that is to say a classical communication network connecting trusted nodes in which QKD-generated keys are stored. This layer enables network-wide key forwarding between connected trusted node based on one-time-pad encryption and can therefore ensure a global management of secret keys.
- The Application layer, in which global keys are transferred (from the secrets layer) and used by applications such as symmetric encryption, symmetric authentication, possibly within more complex network security protocols such as IPSec [MNR+20].

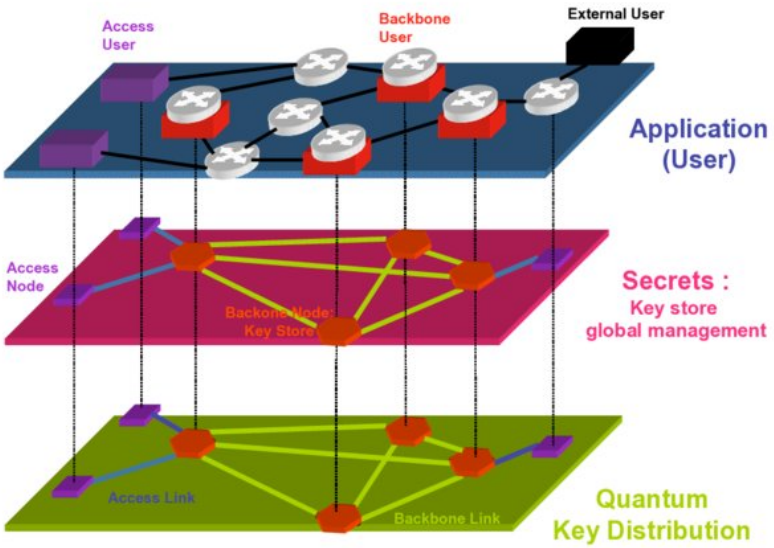

Figure 3.9: 3 Layers architecture for a QKD network based on trusted nodes. This logical architecture proposed for the first time in [ARML06] has then also been adopted by most subsequent large QKD networks projects in Japan, Korea and China.

This architecture allows to decouple secret key management from optical network management and quantum key distribution and from the use of the symmetric keys in secure applications. On a cryptographic level, it can be used to provide long-distance key establishment with information-theoretic security, by daisy-chaining OTP encryptions with one-time-pad keys renewed by QKD. The trusted node QKD network architecture [ARML06] together with an original suite of network protocols [DA07], that we have proposed in the framework of the Secoqc project, have been demonstrated at metropolitan scale in Vienna in 2008 [PPA+09]. Interestingly, we can also notice that this work has also strongly influenced the architectural design adopted in subsequent QKD network deployments. In particular, a similar 3-layer approach has been adopted in most of the subsequent QKD network deployments [SFI+11, CZC+21, MNR+20].

Topological design

Beyond its logical description and architecture, the topological design of a QKD network (and more generally, quantum communication infrastructure) is a multi-factorial and constrained problem, that needs to take into account at least three dimensions:

- The targeted service, in particular for a QKD network, the ability to establish an ITS cryptographic key between any two distant nodes.
- The structure of the demand, i.e. the spatial and time distribution of the requested

traffic, but also the associated value of the service to the final user.

- The cost structure, that can be roughly divided into the initial investment needed to install and deploy the network (capital expenditure, CAPEX), as well as the marginal operational costs associated with running the services (operational expenditure, OPEX).

In the case of a QKD network, as it is in general the case in telecommunication networks, CAPEX is expected to be dominant. It will correspond to the cost of the fiber infrastructure, but also of the trusted node infrastructure. In both case, availability and compatibility with existing infrastructure, will play a central role. We address in more detail the question of quantum and classical coexistence, and in particular the ability to share existing fiber infrastructure, in 3.4.2 .

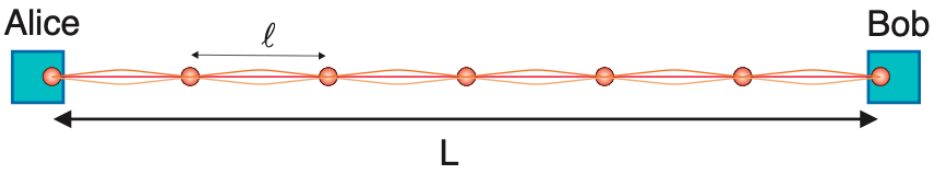

Figure 3.10: Toy model of a 1D QKD chain linking two QKD users, Alice and Bob over a distance L (considered much longer than D_{max}, the maximum span of a QKD link). Intermediate QKD nodes, spaced by a distance ℓ serve as trusted relays, while multiple QKD links can be deployed in parallel to meet the demand.

In [ARDL09], we have conducted one of the earliest study on the topological design of a QKD network, investigating in particular the impact of the specific rate versus distance profile of QKD, $R(l)$, on the global cost minimization of different QKD network architectures and models, starting with a toy model depicted in Figure 3.10. This enables to observe the emergence of an optimal distance at a which trusted node would need to be placed, on a linear chain, but also to study the transition, in 2D models, between topological design with one level of hierarchy (QKD backbone) as in for high traffic demand (or lower cost of trusted node infrastructure), versus non-hierarchical architecture composed of a collection of 1D chains as in Figure 3.10. Although not yet instantiated with real figures, the models and results obtained in this article illustrate the importance of infrastructure cost in the general economical equation associated with quantum communication networks.

Mitigating trusted node security

Because of the span limitation os QKD links, a QKD network able to offer long-distance connections must rely on trusted nodes (or possibly on a GEO satellite, that would be able to offer a wide geographical covering from entangled photon pairs). Relying on trusted node is however often considered with reluctance by the cybersecurity community. More

specifically, public-key cryptography has allowed, fifty years ago to perform secure communications in an end-to-end fashion, i.e. without requiring to trust an intermediate third party, however with some practical limitations. Hence from this perspective, a security technology requiring to introduce trusted node may be considered a step backward.

This objection against trusted QKD networks is structural and cannot be easily mitigated. However, a closer scrutiny at the typology of secure networks, shows that there can be important variations in terms of underlying key management and trust structure. In particular, some high-security communication and data storage infrastructure, are managed principally with symmetric cryptography, and rely on trusted nodes. This can typically be the case for military, but also critical infrastructures with a centralized trusted operator. The use of QKD can hence be relevant in order to strengthen the security of key management procedures in such networks, that typically correspond to the use-cases targeted by the current EuroQCI initiative towards the deployment of a European Quantum Communication Infrastructure [EC19].

In [SPD+10] we have focused on trusted repeater networks and have studied the case when part of the nodes are not to be trusted and could be arbitrarily malicious. We have shown how to ensure that two distant users of the network can share identical and private keys after key generation over the network, on which QKD links connect direct neighbors, assuming that classical messages can be transported reliably over the network. We show that path-diversity can be used to tolerate l-bounded adversary, i.e. that corrupt at most l nodes. In particular, we have shown that secret keys can be generated through l disjoint paths in a private and authentic way against $(l-1)$ bounded adversaries.

3.4.2 Quantum and classical communication coexistence

Most of the effort on QKD system design and most of the experimental demonstrations have so far been realized on dark fiber. This however restricts the deployability of QKD to a limited number of scenarios where the barriers of availability and price for reserving a dedicated dark fiber for QKD could both be overcome. Wavelength Division Multiplexing (WDM) compatibility of QKD would thus imply a significant improvement for QKD in terms of cost-effectiveness and compatibility with existing optical infrastructures. However, WDM coexistence of QKD with intense classical channels raises some new challenges because of the additional noise induced onto the quantum channel. This noise can be due to insufficient isolation between the classical and quantum channels, which can be managed by more severe isolation. On the other hand, non-linear effects and in particular spontaneous Raman scattering leads to wide-spectrum (over 200 nm) of spurious noise photons, some of which being inevitably spectrally matched with the quantum channel. Coping with Raman noise induced by classical channels is a major challenge for QKD systems and especially for discrete variable QKD (DV-QKD) that rely on single photon detectors that are not spectrally selective: Raman scattering spectrum leads to in-band noise photons that cannot be efficiently removed by wavelength filters without adding significant extra losses.

Early work Pioneering work on QKD in WDM environment has been performed with DV-QKD systems, in coarse-WDM [Tow97] as well as later in dense-WDM configurations [PTC+09, CTP+09], however over distances below 25 km. Several DV-QKD experiments have then tried to extend the distance for mixed QKD/WDM. In [EWL+10], 4 classical channels where multiplexed with a DV-QKD system and 50 km operation was demonstrated. However, the input power of the classical channels was attenuated to the smallest possible power compatible with the sensitivity limit of the optical receiver (-26 dBm). Attenuating the classical channel launch power was also used in [PDC+12] where the impressive distance of 90 km was demonstrated, however with an input power limited down to -18.5 dBm and in addition the use of temporal filtering techniques. Temporal and spectral filtering techniques have also been optimized in [PDL+14] to allow the first demonstration of DV-QKD in coexistence with one 0 dBm classical channel, at 25 km.

Continuous Variable QKD (CV-QKD) As analyzed in [KQA15], the coherent detection used in CV-QKD to measure the field quadratures acts as a natural and extremely selective filter whose acceptance is equal to the bandwidth of the coherent detector, i.e. typically ranging between 1 and a few hundreds of MHz. As a consequence, CV-QKD can operate in a regime where it filters out spurious light down to a single spatio-temporal mode. This feature allows us to achieve results that could not have been obtained so far with DV-QKD, namely the coexistence of a fully operational CV-QKD system over metropolitan distance with an intense dense-wavelength-mutiplexed classical channel of several dBm.

In [KQA15] we have experimentally validated the capacity of CV-QKD to co-propagate with intense WDM signals. Our experimental test-bed consisted in a CV-QKD link (operated at 1531.12 nm) multiplexed with one DWDM classical channel whose wavelength is set at 1550.12nm. We could check, as displayed on Fig.3.11/left, the linear dependence of Raman-induced noise with launch power, and test CV-QKD operation at 25, 50 and 75 km. We also observe for example that up to 14 mW (11.5 dBm) of launch power can be tolerated by CV-QKD in the forward configuration, at 25 km.

CV-QKD can be deployed in coexistence with classical channels of unprecedented power levels thanks to the mode selection property of its coherent detection. This gives CV-QKD an advantage for the integration into different optical network architectures and in particular access networks. Figure 3.11/right displays a comparison between DV-QKD and CV-QKD in terms of tolerable classical channel power. As it can be seen, CV-QKD can be integrated into different high power passive optical networks such as for example Gigabit PON, 10G-PON and WDM/TDM PON. On the other hand, integration of DV-QKD in such optical networks requires either some modifications in the architecture or further advances in the noise reduction techniques applicable to DV-QKD.

Towards QKD/WDM coexistence over optical backbone links The ability to deploy QKD over optical backbones or over inter-datacenter links could be a game-changer for the development of the technology, significantly reducing QKD deployment cost overhead and most importantly opening radically larger and security-relevant market segments.

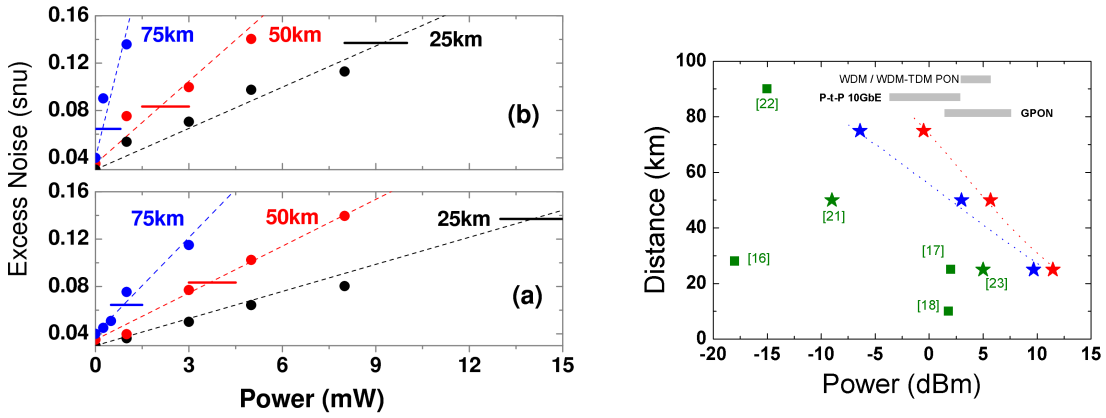

Figure 3.11: **(Left)**: **Excess noise measurements vs launch power in forward (a) and backward (b) channel configuration**. Black, red and blue data points are the excess noise evaluated at Alice for fiber length of 25km, 50km and 75km, for different classical channel power. Dashed lines indicate the expected excess noise curve and solid horizontal lines are null key threshold for CV-QKD, for the respective channel distance.
(Right): Tolerable classical channel power vs Reachable distance: Performance of QKD in the context of coexistence with classical optical channels. Red and blue colors represents our results with a CV-QKD system, in forward and backward classical channel configuration, while previous works with DV-QKD systems are in Green. Stars: experiments conducted in the C-band (DWDM). Squares: experiments conducted in CWDM. The dotted red and blue lines are the forward and backward simulation curve for the null key rate in the current experiment. Gray bands show transmitter input power range in different standardized optical networks. Figure taken from [KQA15], see original article for the number-reference correspondance.

This objective however comes with very stringent requirements:
1) Cover a distance equivalent to the typical optical fiber span, i.e. around 80 km ;
2) QKD operation with positive key rates in coexistence with several WDM classical channels (up to 100 in backbone) each of nominal (0 dBm) launch power, hence requiring ultra low WDM-induced noise ;
3) QKD integration should ideally have a minimal impact over standard WDM link information transmission capacity.

Although these requirements have not yet been fulfilled in a single experimental demonstration, significant steps have been recently made. In [EHP+19], CV-QKD co-propagation jointly transmitted with 100 WDM channels over which a datarate of 18.3 Tbit/s was being sent, over a realistic set-up. This impressive demonstration meets criteria 2) and 3), however was demonstrated only over 10 km. Fig. 3.12 compares this figure with earlier demonstrations. At OFC 2019, Kleis et. al. [KSDS19] reported on an experimental demonstration of mixed CV-QKD /WDM with classical signals placed in the S-band.

This has allowed them to multiplex up to 28 classical channels at 0 dBm each (approx. 14 dBm of total power) in coexistence with CV-QKD, i.e a notable progress towards criteria 1) and 2). Finally, we notice that [MWZ+18] has made decisive steps in meeting criteria 1-2-3) all along, by demonstrating the integration of DV-QKD, in coexistence with 21 dBm of classical signals, carrying 3.6 Tbs data-rate, over 66 km. This record performance however relies on the use of large-core fibers and cannot therefore be directly applied within existing networks.

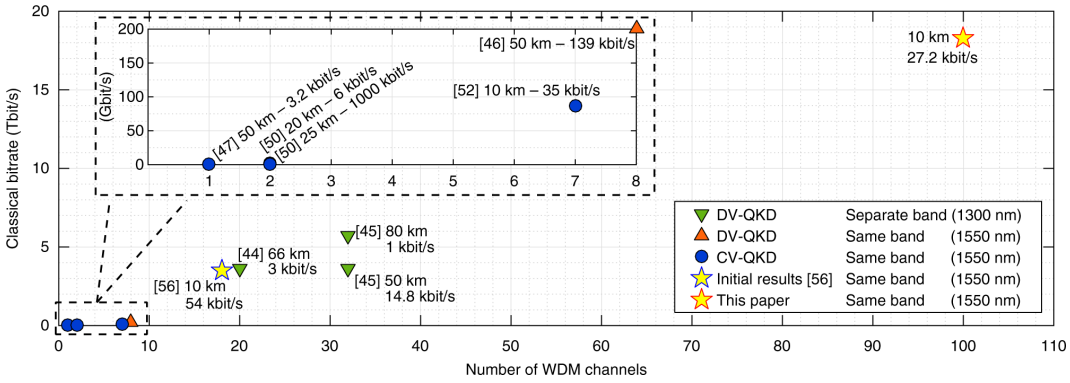

Figure 3.12: Figure taken from [EHP+19] and comparing the total classical bitrate, the number of wavelength division multiplexing channels and the total data-rate of classical channels. It illustrates the abililty to operate CV-QKD in mixed WDM environment close to the backbone regime, i.e with 100 classical channels and Terabit/s classical capacity. However the demonstrated distance was only 10 km, and the launch power of each classical channel is approx. -7 dBm. See original article for details, and the number-reference correspondance.

Chapter 4

QKD security: from theory to practice

4.1 QKD Security definition

As for any cryptographic protocol, reasoning about the security of QKD first requires to define its security criteria. An ideal secure key needs to satisfy two properties. The first one is *correctness*, i.e; that the key bits strings in possession of Alice and Bob need to be identical. The second one is *secrecy* with respect to Eve, i.e. that given the (classical and or quantum) knowledge acquired by Eve, the key bits should appear as uniformly distributed.

We can define K_A and K_B (with the same length m) to be the key bit strings obtained by Alice and Bob, respectively. The secret key can be correlated to a quantum state ρ_E held by Eve. The joint state ρ_{ABE} can be written as the following classical-classical-quantum (c-c-q) state:

$$\rho_{ABE} = \sum_{(k_A,k_B)} Pr(k_A,k_B)|k_A\rangle\langle k_A| \otimes |k_B\rangle\langle k_B| \otimes \rho_E \tag{4.1}$$

where $k_A, k_B \in \{0,1\}^m$ are the bit values.

Conversely, an ideal key state held by Alice and Bob is described by

$$\rho_{ABE}^{ideal} = 2^{-m} \sum_{(k)} |k\rangle_A\langle k_|| \otimes |k\rangle_B\langle k_|| \otimes \rho_E \tag{4.2}$$

where $k_A = k_B = k$ implies that Alice and Bob hold the same string, and where ρ_E is independent of k, i.e., Eve has no information on the key string variable K.

Due to practical statistical issues, such as the finite data size and non-ideal error correction, Alice and Bob cannot aim to obtain an ideal key with certainty from a practical QKD protocol. It is however reasonable to allow the key to have a small failure probability for its correctness and secrecy, and to extend the security definition accordingly.

A QKD protocol is defined [BOHL$^+$05a, RK05] to be ϵ_{cor}-correct if the probability distribution $Pr(k_A,k_B)$ of the final state ρ_{ABE} in Eq. 4.1 satisfies $Pr(k_A \neq k_B) \leq \epsilon_{cor}$. It

is defined to be ϵ_{sec}-secret if the state ρ_{ABE} is close in trace distance to the single-party private state ρ_{AE}^{ideal}, i.e more precisely if $min_{\rho_E}\frac{1}{2}(1-p_{abort})||\rho_{AE}-\rho_{AE}^{ideal}||_1 \leq \epsilon_{sec}$, where p_{abort} is the probability that the protocol aborts and $\rho_{AE}^{ideal} = 2^{-m}\sum_{(k)}|k\rangle_A\langle k|\otimes\rho_E$ denotes a bipartite quantum state where Alice holds a uniform string, perfect decoupled from Eve.

Hence, for some ϵ_{cor} and ϵ_{sec}, we say that the QKD protocol is ϵ -secure with $\epsilon = \epsilon_{cor} + \epsilon_{sec}$ if it is ϵ_{cor}-correct and ϵ_{sec}-secret . A strong feature of this security definition, based on trace-distance metric, is that it is composable, even against an eavesdropper E holding a quantum memory [BOHL$^+$05a, RK05].

It is interesting to note that the above-mentioned security definition was for a large part developed by Renato Renner, and co-authors, during his PhD work [Ren05]. One important goal has been to address the issue of proposing a composable security definition, criteria that was not met by previous security definitions relying on mutual information as a quantifier for Eve information, because the possibility to unlock a large quantity of mutual information with a small leakage of secret information [KRBM07]

4.2 Using QKD for cryptographic purposes

A significant part of my work, in particular in the context of European collaborative initiative (Secoqc, EuroQCI) or groups (ETSI QKD ISG) has been to question the theoretical and practical cryptographic advantage that can be achieved with QKD. This has lead me to act as editor for the Secoqc cryptography white paper[ABB$^+$14], co-author of the ETSI implementation security white paper[LSA$^+$18], and more recently to work on the question of security gain in the context of EuroQCI study[MA20].

The appealing feature of quantum key distribution (QKD), from a cryptographic viewpoint, is the ability to establish keys with information-theoretic security (ITS). QKD however does not provide a standalone security service in its own: the secret keys established by QKD are in general then used by a subsequent cryptographic application for which the requirements, the context of use and the security properties can vary.

It is therefore important, particularly in the perspective of integrating QKD in a large quantum communication infrastructure [EC19], to analyze how QKD can be combined with other cryptographic primitives and to clarify important trade-offs, in particular between security and performance. After setting some important definitions, we analyze which secure communication constructions relying on QKD can be deployed with a clear security-gain with respect to existing computational cryptographic schemes.

4.2.1 Definitions

Quantum cryptography departs from classical cryptography essentially from a security standpoint, and not from a functional standpoint. Concerning QKD, it provides a specific route to realize the authenticated key encryption (AKE) primitive. To capture the security gain that QKD may bring, it is essential to introduce definitions that allow to establish a

comparison between classical and quantum cryptographic approaches, and in particular to consider two different security notions related to AKE:

- Single-shot security: the security achieved a the level of a single key establishment session.

- Key dependency: the vulnerability of a key, established in a given AKE session, with respect the compromise of another key, established in a future session (forward security) or past session (backward security).

Security levels for single-shot key establishment

We consider the different levels of security for AKE (mostly the confidentiality of the key, but possibly its integrity and authenticity), when considering an attacker whose attack surface is, by definition, limited to a single key exchange. In order to capture the cryptographic advantage that may be attained by QKD, it is relevant to distinguish between three security levels, information-theoretic security (ITS), being the highest.

- Information-theoretic security (ITS): a AKE is information-theoretically secure if it is secure irrespectively of the computational power that may be used by an attacker. A synonym of ITS is unconditionally secure. The second highest level of security in this context is the so-called everlasting security.

- Everlasting security: An AKE scheme has the everlasting security property if it is secure against adversaries that have unlimited computational power after the protocol execution. This implies that computational attacks may be launched against the AKE scheme, but only during the execution of the protocol, which strongly limits the corresponding threat. The lowest and more generic security level is computational security. This is the case for most classical cryptographic primitives.

- Computational security: the security of the AKE scheme is based on a computational hardness assumption. Solving the computationally hard problem during or after the execution of the AKE protocol may reveal the established keys.

When several cryptographic primitives are composed within a given protocol, the resulting protocol can only be as secure as its weakest component. This consideration applies, for example, to the relation between AKE protocol and encryption. If any of the two protocols is computationally secure, then the overall protocol can only be computationally secure. Moreover, if we want to enjoy the everlasting security property for a composite AKE + encryption protocol, we need to combine an everlasting secure AKE scheme with an ITS encryption scheme. Finally, if we aim to build a composite protocol with ITS security, then all the building blocks must be ITS as well.

Key dependency

Single-shot security refers to the level of security that can be reached by a given AKE cryptographic construction, at the level of a single session. Key dependency, on the other hand, considers a more general scenario where many session keys have been established, and considers the impact that the leakage of a given key may have on the security of another one. The two central concepts are forward secrecy and post-compromise security that designate respectively the impact that information leakage about a given key may have either on past session key (forward security) or on future ones (post-compromise security). Figure 4.1 illustrates schematically these two concepts.

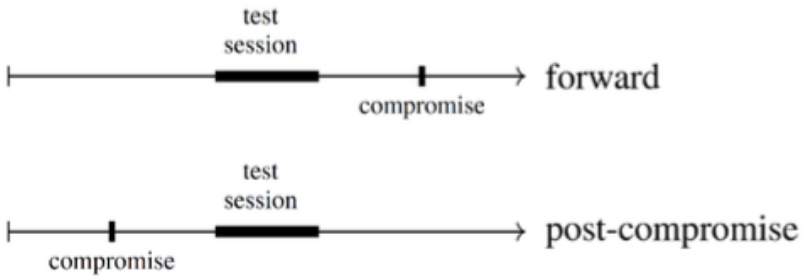

Figure 4.1: Attack scenarios considered by forward and post-compromise secrecy; "test" refers to the session under attack. Forward secrecy protects sessions against later compromise; Post- compromise security protects sessions against earlier compromise [CGCG16].

Forward secrecy A central concept is the notion of forward secrecy.The term "forward secrecy" however does not have a unique meaning across the literature. In the case of authenticated key establishment (AKE), forward-security designates AKE protocols in which the compromise of a key does not lead to compromise keys of previously completed sessions [BG20]. In order to clarify discussion and comparison between QKD and computational AKE schemes, we need to make a distinction between absolute and computational forward secrecy:

- Absolute forward-secrecy: Even if a session is compromised, the only way to have access to the previous sessions is to break their single-shot security. Moreover, the compromise of the session does not help at all for this purpose (i.e. the one-shot security of a given session is independent on the knowledge of the following ones).
- Computational forward-secrecy: gaining information about past sessions from the compromised current session key is a task that requires to break a computational problem.

- No forward-secrecy: the AKE scheme does not provide at all any backward protection.

Post-compromise security We also want to analyze how a leakage of information about a key the could affect the subsequent AKE sessions and which kind of security levels can be considered. We will be referring to this end to the general concept of post- compromise security (PCS) [CGCG16], that designates the property of an AKE scheme such that the compromise of a given secret key does not lead to the compromise of secret keys established in future sessions. It will be again important, in view of future comparison, to further distinguish between different form of post-compromise security, for AKE schemes. To this end we consider a compromised AKE session, and another subsequent session, called test session. We aim to qualify the security dependency of the test session, with respect to the compromised session.
Continuous eavesdropping assumption: We aim to qualify the security dependency of a (future) test session, with respect to the compromised session. To that end, we assume that an attacker is always (continuously) conducting a (passive or active) eavesdropping of *all* communications between the AKE parties (Alice and Bob). If the eavesdropping was not continuous, then, a trivial strategy to restore security after a compromise, would simply consists in continuously initiating new AKE sessions (using previously established keys for authentication): such strategy would lead to new secure shared keys for the session on which the attacker fails to eavesdrop.

Depending on the active of passive nature of the eavesdropping, we can then distinguish 3 levels of post-compromise security:

- Full Post-Compromise Security: in which a *continuous active* attack (either on the classical, or quantum channel, depending on the AKE protocol setting) is required to maintain compromise

- Partial Post-Compromise Security: : in which an *active, but episodic* attack is required to maintain compromise.

- Basic Post-Compromise Security: in which a *passive* attack is sufficient to maintain compromise.

4.2.2 Comparison of the security for different AKE schemes

Now that we have introduced the necessary definitions, we can compare the security of different Authenticated Key Exchange constructions, in terms of single-shot security and key dependency, and in particular compare the security of QKD-based AKE with alternative computational schemes relying on symmetric-key or public-key cryptography.

QKD-based AKE

The single-shot security of QKD-based AKE depends on the authentication scheme used for authenticating the classical channel. ITS authentication schemes based on pre-shared secret and universal hashing [CW79, Sti94] can be combined with QKD to build an ITS AKE. Using pre-shared secret can however be challenging, notably over large networks. In this case, public-key authentication provides an interesting alternative, that can be used to build everlasting secure QKD-based AKE. In addition, it is not necessary to use computational secure authentication for all the key exchange sessions: once the QKD protocol has output some secret key, a portion of this secret can subsequently be used to perform subsequent authentication rounds, with ITS, guaranteeing the following statement: "if authentication is unbroken during the first round of QKD, even if it is only computationally secure, then subsequent rounds of QKD will be information-theoretically secure" [SML09].

In addition to ITS (or everlasting) single-shot security, one of the strong features of QKD-based AKE is to offer absolute forward-secrecy and full post- compromise security. As a matter of fact, QKD generates (usually based on an integrated QRNG) session keys that are information-theoretically independent from each other, i.e. with maximum new entropy at each session. This provides the highest levels of security regarding the key dependency, and in particular absolute forward-secrecy. Regarding post-compromise security, one shall consider the sequential production of session keys with QKD. In such case, the secret material needed at each QKD round to authenticate the classical channel stems from a previous QKD round [ABB$^+$14]. A post-compromise man-in-the middle attack is therefore only possible only if all subsequent sessions, after the compromise and until the session are also broken in real time, i.e. setting extremely stringent requirements on the attacker.

Classical computationally secure symmetric-key-based AKE

Symmetric schemes as the block cipher AES can be used to guarantee the confidentiality of a message, but also to guarantee integrity and authenticity, with the Message Authentication Codes (MACs). Combining both functionalities can be employed also to build an AKE primitive, that will exhibit computational single-shot security. Most symmetric-key-based AKE schemes rely on shared long-term secrets, called master keys, and are vulnerable to the leakage of such long-term secrets. This means that they in general do not provide forward-security (while some standard public-key schemes can). It is however possible to add key-derivation mechanisms, to improve on this weakness, as proposed for example with a recent work [ACF20]. We should note however, only computational forward-secrecy can be achieved in this case, which hence strictly departs from the absolute forward-secrecy AKE schemes that can be achieved using QKD.

Another drawback of symmetric schemes, in terms of key dependency, is that they in general do not offer post-compromise security. As a matter of fact all future sessions keys are deterministically derived from previous ones. Hence, once the attacker has compromised at least one session in the past, he can completely retrieve all the secrets of the

following sessions.

Classical computationally secure public-key-based AKE

Public-key-based AKE is especially needed to operate large and open networks with many users. In such context, the distribution of pre-shared secrets is cumbersome as the number of keys scales badly (quadratically) with the size of the network. In such situation the use of a public-key authentication scheme is extraordinarily convenient to provide distributed trust when combined with certificate authorities (CAs) in a public key infrastructure (PKI). In terms of the security properties, public-key based AKE schemes can provide computational single-shot security based however on weaker computational assumptions than symmetric-key cryptography, such as the existence of trapdoor one-way functions (TOWFs). Conversely, public-key AKE can be implemented with ephemeral key strategy, allowing the session keys to be independent and therefore offering absolute forward-secrecy and full post-compromise security.

4.2.3 Using QKD for Secure Communications

Establishing a secure communication between two or more parties is a central security service that is a primitive for many other security services. The security functionalities associated with secure communications comprise one of the three fundamental security properties (and very often all of them): confidentiality, integrity and authenticity. Two main schemes are particularly useful: an AKE scheme and an authenticated encryption (AE) scheme. We have already analyzed constructions for AKE schemes in the previous subsection. We now want to make a step further, analyzing constructions for AE schemes and their combination with AKE schemes, in order to construct secure communication schemes. In the previous subsection, we went through the three main core cryptographic mechanisms that can be used to build AKE scheme: QKD, symmetric crypto, public-key crypto, complemented by appropriate authentication mechanisms.

Regarding Authenticated Encryption, we need to both choose the encryption scheme and the type of authentication that we want to provide. The possible security levels for encryption in this context are ITS or computational. In general the security level for authentication matches the security of encryption but we will also consider everlasting secure AKE schemes, combining public-key authentication with ITS encryption. Lastly, we are not going to consider public key encryption to protect the messages, since, even if we trust trapdoors one-way functions (TOWF), it is always computationally much more efficient to use a symmetric encryption scheme combined with a public-key AKE. Finally, we will improperly designate as "AES", all computationally secure symmetric encryption schemes.

Main Secure Communication Constructions

This leads us to short-list and compare the security properties of six of the main Secure Communication constructions that can be envisaged. They consist in combining a key establishment scheme, an encryption scheme and an authentication mechanism (that will be used to authenticate key establishment and encryption).

1. QKD + OTP encryption + ITS authentication.
   The highest level of security achievable, both in terms of individual security and key dependency, is obtained combining QKD with One-Time Pad (OTP) and an ITS authentication (both for authenticate the QKD classical channel and the encrypted message). In this way the communication can guarantee ITS confidentiality, but also ITS integrity and authenticity. Moreover, thanks to QKD, it provides absolute forward-secrecy and full post-compromise security. Initialization of this scheme is based on distributing pre-shared symmetric secret keys.

2. QKD + OTP encryption + computational authentication
   Relaxing the ITS assumption for the authentication scheme enables more flexibility in key management and initialization, that can rely on pre-shared secrets as well as public-key schemes. Such computational authentication combined with QKD still enables to perform key establishment with everlasting security. Such keys can then be used to construct authenticated encryption schemes with OTP. In this case we can construct Secure Communication with everlasting security for confidentiality, authenticity and integrity, and in addition guarantee absolute forward-secrecy and full post-compromise security.

3. QKD + AES encryption + comp. authentication
   OTP is not the only encryption scheme that can benefit from QKD. Another interesting approach is to combine QKD with a symmetric encryption scheme such as the AES block cipher. This leads to a secure communication scheme whose communication rate is not limited by QKD relatively low key rates. Conversely, the global security level is however then only computational. The security provided by AES encryption is considered quite high.There are currently exist known attack on AES256 whose complexity significantly departs from exhaustive search, which can be implemented by a quantum attacker using Grover search with 128 bits of complexity [BNPS19]. The main interest of combining QKD with AES encryption, besides everlasting security, resides in the key dependency properties. QKD-based AKE provides keys with absolute forward-secrecy and full post-compromise security, which can hence be used to strengthen the security of the SC scheme with respect to key key leakage.

4. (TRNG + AES)-AKE+ AES encryption + computational authentication One possible solution is to use a fresh source of entropy to generate the keys, such as a TRNG, combined with a computational symmetric encryption scheme (key derivation and key

transport mechanism). In this configuration the key establishment (TRNG+AES) can provide computational forward-secrecy, but only basic post- compromise-security. The only reasonable choice is then combining this AKE configuration with a fast computationally secure symmetric encryption scheme such as AES, supported by a computational authentication scheme. The security level of the SC scheme is therefore computational.

5. AES-based AKE + AES encryption
   As an alternative to 4), simpler to implement, the fresh source of entropy (TRNG) can be replaced by a pseudo-random number generator (PRNG) and rely on the use of pre-shared secrets. By doing so, we define a deterministic key derivation function (KDF) [Kra10] that can be used to expand, with computational security, a pre-shared key, in many other shared keys. This approach however lacks of key independence: without the injection of new entropy, a key leakage can affect the security of both past and future communications. More precisely, it offers only basic post-compromise security and computational forward-secrecy.

6. Public key AKE + AES + computational authentication
   One last possibility, is a scenario where public key AKE schemes to start the session, supported by a public-key infrastructure (PKI) to perform flexible public-key-authentication for both the key exchanged and the symmetric encryption. The resulting SC schemes provides computationally secure confidentiality, integrity and authenticity. Lastly, using the ephemeral keys strategy, the authenticated AKE can offer absolute forward-secrecy and full post-compromise security. The initialization in this construction is always asymmetric.

Analysis of security gain

A QKD-based secure communication schemes is said to offer a security gain if it provides the correct functionality (secure communications) with a set of security properties that cannot be obtained with computational crypto primitives only. Security gain is crucial in the sense that it appears as necessary condition for a scheme to be of practical interest. When analyzing the relevance of QKD-based secure communications schemes (SC) listed above, the choice of encryption algorithm appears as central design choice. This leads to consider two main group of constructions, among the 6 constructions listed above i.e.

- Constructions 1. or 2. i.e. ITS Secure Communications relying on QKD combined with OTP (One Time Pad) Encryption.

- Constructions 3., i.e. Computational Symmetric Encryption combined with QKD, that we will often denote as QKD+AES option (knowing that we will generically denote as AES any symmetric encryption algorithm based on a computationally secure one-way-function).

It is interesting to compare these two schemes, from the perspective of security gain, but also performance (data rate) and trust assumptions, and foreseen applications.

ITS Secure Communications
From a security gain viewpoint, the choice of QKD+OTP is the strongest option: it allows to build Information-Theoretically-Secure (ITS) SC, which is unachievable classically and hence leads to a clear security gain. It however also comes with the constraint that the SC rate is limited to the QKD rate (i.e.today below Mbit/s per quantum communication mode, with existing technology). This option will be well adapted to use-cases related to data with long-term-security requirements and for which relatively low data- rates is acceptable.

Computational encryption combined with QKD (QKD+AES)
The advantage of computationally secure SC (i.e; QKD+AES) , with respect to QKD+OTP is that it can be performed with high data rates (e.g. with 100 Gbit/s AES encryptors). However, the situation, in terms of security gain, is less favorable and depends also on the network typology and trust:

- **over a point-to-point link** In that case, the fact that QKD AKE offers full post-compromise security, and that no trusted node are needed, implies a security gain. QKD+AES hence appears as an interesting way to strengthen the security of P2P secure communication links, in particular as a defense in depth, possibly in combination with PQC. This is in line with the recently proposed protocol by Paterson et. al. [DHP20].

- **over a large network with trusted nodes** In the case of a large network with trusted nodes, combining QKD with AES for secure communications does not bring a security gain with respect to the use of symmetric encryption and key derivation that can be achieved to perform SC with the same security (computational security of AES) in an end-to-end fashion (i.e. without trusted nodes) and also without QKD, and hence also at a significantly lower cost.

4.2.4 Conclusion

To which extent secure communication schemes based on QKD can bring some advantages with respect to schemes relying solely on computational cryptography? To answer this question, we have conducted an analysis based on security properties - that we have carefully defined, and that also takes trust assumptions into account. The central conclusion of this analysis is that schemes combining QKD with OTP encryption should be considered in priority, in the context of large QKD networks with trusted nodes, in order to provide a security gain.

We can moreover think of security services providing a security gain based on QKD+OTP and implementable with existing or near-term technology, in particular:

- High-security key transport and more generally high-security key management, possibly over a large network, with trusted nodes. In such use-case, QKD+OTP can be thought as a special (ITS and automatized) form of trusted courier. Such ultra-secure communication scheme could typically be used to perform out-of-band key establishment in order to strengthen key management in high-security contexts.

- Long-term secure storage, that can be implemented by combining a distributed storage infrastructure, with QKD+OTP in order to perform proactive secret sharing over a ITS SC communication network. Some data such as genome data, health data or tax data may require long-term (50+ years) confidentiality and integrity protection, which cannot be provided by current cryptography and secure storage techniques. Proactive secret sharing decomposes the secret into n shares in such a way that a threshold number k ? n of shares is required to reconstruct the secret while any smaller number of shares reveals no information about the secret. The shares are renewed on a regular basis in order to prevent attacks by mobile adversaries who may be able to learn more and more shares over time. QKD combined with One-Time-Pad encryption offers a solution to perform share renewal, with information-theoretic security, hence offering a clear security gain over classical secure storage techniques, and can be implemented in practice [BBD+17, MGA+20] with existing technology.

Conversely, an important (negative) conclusion of the analysis is that Secure Communications based on QKD combined with AES encryption, does not provide security gain when deployed over large network requiring intermediate trusted nodes.

4.3 Practical security of QKD

Even though the term "unconditional security", synonym of information-theoretically, is often used to characterize the security of QKD, one must be careful with the precise meaning of this expression. As noted in [GRTZ02a], several underlying assumptions must be fulfilled for QKD security proofs to be valid.

- [Quantum Mechanics] Quantum Mechanics is valid. The security of QKD is intrinsically based on properties derived from quantum mechanics axioms, such as the fact that non-orthogonal quantum states, onto which information is encoded in QKD, cannot be distinguished perfectly.

- [No leakage] There is no information leakage from the security enclaves in which Alice and Bob QKD systems are placed and operate.

- [Trusted implementation] The implementation of Alice and Bob QKD devices is conform to the model used in the security proof while the underlying trust assumptions are verified.

However, as we consider practical QKD implementations, such assumptions may not always be valid. In particular we also to provide security assurance against attackers that may actively challenge such assumptions. Most attacks on QKD implementations, also designated as "quantum hacking" indeed consist in active attacks aiming to break either the [No leakage] or the [Trusted implementation] assumptions, or both. We will first propose in 4.3.1, a rapid overview of the work conducted on implementation attacks against QKD. We will then present our series of work on quantum hacking, related to saturation attack against CV-QKD, starting with the attack principle and the theoretical study of two attack paths [QKA16, QKMA18].

We will then present our work on the experimental vulnerability assessment of QKD systems, introducing the notion of attack ratings [KMQA21]. This work more generally connects to the challenge of certifying QKD implementations and to the ongoing international effort on that matter (to which we participate within the ETSI QKD-ISG [LSA+18]) towards the definition of standardized vulnerability analysis and security evaluation for QKD and the certification of quantum crypto-systems presenting strong guarantees against quantum hacking.

4.3.1 Quantum hacking

Theoretical security proofs [Ren08, SBPC+09, LCT14] constitute a strong conceptual framework to capture the security properties of QKD protocols, based on a model and assumptions, as listed in the previous section. QKD implementations may, however, not fully comply with the model used in the security proof, leading to security vulnerabilities and the possibility to launch side-channel attacks [XMZ+20].

In discrete-variable (DV) QKD, single photon detector (SPD) is the most vulnerable device that suffers from different kinds of side channel attacks. Attacks such as time shift [QFLM07, ZFQ+08], after gate [WLW+11], blinding [Mak09], spatial mode mismatch [SCB+15] attacks and etc. can all break DV-QKD securities. Among which blinding attack is considered as the most powerful attack, where Eve inserts an intense light to actively control Bob's single photon detector. Such kind of attack has been experimentally verified on commercial QKD systems [LWW+10] and implemented as a full-field eavesdropping demonstration [GLLL+11]. Various countermeasures have been proposed against detector-based attacks, however only the measurement-device-independent (MDI) QKD [LCQ12] can perfectly defeat these attacks.

Continuous-variable QKD (CV-QKD) [WPGP+12], is another promising approach to perform quantum key distribution. It relies on continuous modulation of the light field quadratures and measurements with coherent detection (homodyne or heterodyne detectors) instead of SPDs in DV-QKD system. Benefiting to coherent detection, CV-QKD can be fully implemented with off-the-shelf optical communication components [LBGP+07, FDD+09, JKJL+13a]. Moreover, the local oscillator (LO) in the coherent detection acts as a "built-in" filter to efficiently remove any noise photons in different modes, which enable CV-QKD to be co-existed with intense classical channels over optical net-

works [KQA15] and to be possibly implemented in day light free space environments. Unfortunately, these elements have potential vulnerabilities in CV-QKD implementations that can be used by Eve to break security. For example LO manipulation is a long standing security problem where Eve can modify LO pulse in different ways [JKJL$^+$13a, MSJ$^+$14] and steal secret keys without being discovered. This issue has been recently solved by generating locally LO (LLO) signal at Bob side[QLP$^+$15, SBC$^+$15, HHL$^+$15, MA17]. Regarding to homodyne detection (HD), either wavelength dependent properties of the beam-splitter [MSJL13, HWY$^+$13b, HKJJ$^+$14] or amplifier electronics saturation [QKA13b, QKA16] can be independently taken advantage by Eve to launch attacks to break security.

Saturation attack against CV-QKD

While most implementation attacks against CV-QKD target LO manipulation in the TLO setting, we have proposed in [QKA16] and further studied in [QKMA18] the so-called saturation attack against CV-QKD, that consists in biasing the excess noise estimation by actively inducing the saturation of the homodyne detectors.

The modus operandi of this attack is twofold. Eve launches the intercept and resend (IR) attack [LDGP$^+$07] such that she gains encoding information about the states sent by Alice. However, a full IR attack induces 2 shot noise unit (SNU) of excess noise in Alice & Bob measurements and hence reveals the presence of Eve. Exploiting the non-linear behavior of a homodyne detector, in a way that Eve resends newly prepared signals to induce electronics saturation on the homodyne detector, she can reduce 2 SNU of excess noise below the null key threshold - where all generated keys are believed to be secure. Since excess noise level is favorable to secure key generation, Alice and Bob then proceed to error correction and privacy amplification. After listening to the classical post processing communication between Alice and Bob, Eve can gain complete information about the final key without revealing her presence. Importantly, the saturation attack only targets on the HD which means even the recent proposed LLO CV-QKD scheme is not immune to this attack if no countermeasure is considered.

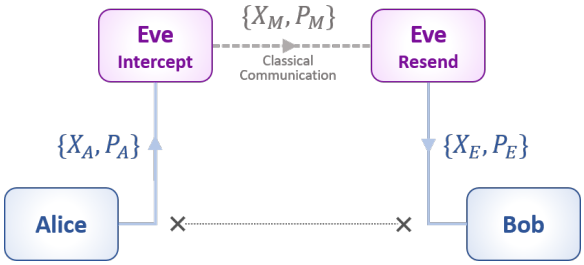

Figure 4.2: Scheme for saturation attack. Eve$_{intercept}$ intercepts Alice's Gaussian modulated signal of quadratures $\{X_A, P_A\}$ and shares her measurement results $\{X_M, P_M\}$ through the classical channel to Eve$_{resend}$. The resent and displaced signal of quadrature $\{X_E, P_E\}$ is measured by Bob homodyne detector.

The actual realization of the saturation attack comprises of two steps: intercepting Alice's signal and resending a newly prepared signal to Bob with displacement Δ and gain G. We can consider that two cooperating eavesdroppers are involved in the attack: Eve$_{intercept}$, located near Alice intercepts the signals of quadratures $\{X_A, P_A\}$ and classically communicates the measurement results $\{X_M, P_M\}$ to Eve$_{resend}$- located near to Bob as shown in Figure 4.2. Due to the technical restrictions imposed by the laboratory equipment, we experimentally demonstrate only the resend step of the attack and model the impact of the measurement associated with the intercept step. $\{X_M, P_M\}$ is deduced from $\{X_A, P_A\}$ by simulating a heterodyne measurement, i.e. 3 dB loss factor and also the addition of a random Gaussian noise of variance 2 shot noise [LDGP$^+$07].

Efficient countermeasures against the saturation are known. As detailed in [KJJ15] active monitoring of the linearity of Bob's coherent detection can provide a robust countermeasure against saturation attack. This countermeasure, however, requires dedicated hardware (additional amplitude modulator at Bob side). We have proposed in [QKMA18] another countermeasure against the saturation attack, that can be implemented without using additional hardware: it relies on the pre-characterization of the detector linearity range, and consists in post-selecting measurement data, based on the fact that these quadrature measurements fall, within high confidence, in the linearity range of the detector. This countermeasure, that relies purely on software, has the advantage of being implementable at a small marginal cost.

Experimental implementation of the saturation attack

The work done in [QKA16, QKMA18] demonstrates that the non-linearity of the coherent receiver can in principle be exploited to obtain a complete break of a QKD security protocol, in certain parameter regimes.

We have recently pushed the analysis one step further in [KMQA21] and studied in practice some of the experimental routes that could be used to launch the saturation attack in practice. This has lead us to consider two implementation paths for the saturation attack, namely a coherent and and incoherent attack strategy.

Coherent attack strategy This implementation strategy for the saturation attack consists in coherently displacing the signals sent by Alice, in order to drive Bob's receiver into saturation. We have experimentally tested this attack in [KMQA21], using a set-up built around a Sagnac interferometer where a laser, coherent with the QKD signals, is mixed on a highly unbalanced variable beamsplitter. This setup, displayed on Figure 4.4 allows to maintain a high phase stability thanks to the Sagnac loop and to perform a controlled displacement by varying the beamsplitter transmittance. As depicted on Figure 4.3, this setup has allowed us to coherently displace the QKD signals, and to drive the homodyne reception into saturation, for high displacement values.

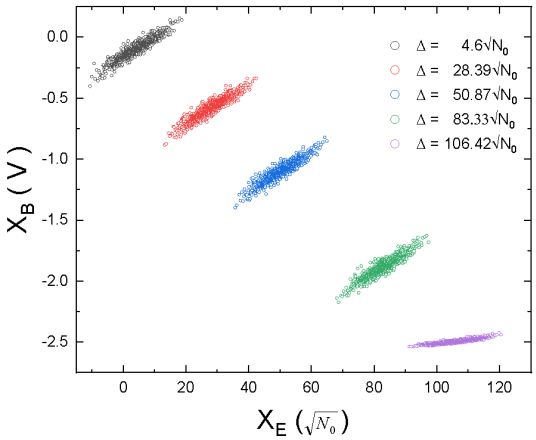

Figure 4.3: Response of homodyne output due to a coherent displacement. Input signal sent by Eve, with quadrature variance $Var(X_E) = 22N_0$ with 5 different displacement values Δ and saturation at $106.42\sqrt{N_0}$ (magenta). Displacement shifts Bob's quadrature measurement X_B (expressed here in volts). Large displacement value can lead to saturation (that occurs when X_B reaches -2.5Volts).

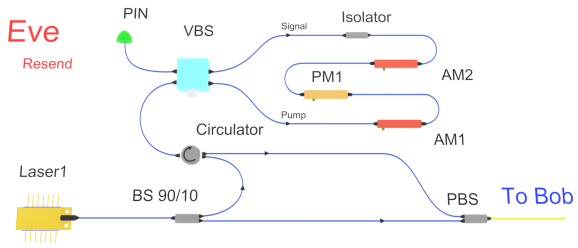

Figure 4.4: Experimental setup for generating displaced coherent state. AM: Amplitude Modulator, PM: Phase Modulator, BS: BeamSplitter. In the Sagnac loop, Gaussian modulated signals are prepared using the AM and PM modulators and are then displaced at the Variable Beam Splitter (VBS), based on a coherent interference between pump. Displaced signals is then sent to Bob along with local oscillator.

Incoherent attack strategy The incoherent attack strategy consists in sending an intense incoherent laser pulse sent along with the resent coherent state.This strategy is experimentally much simpler, and relies on incoherent laser pulse injection.

Saturating the homodyne detector with external laser pulse indeed presents several operational advantages over the coherent strategy. In particular, active phase drift compensation is not required. Saturation attack with incoherent strategy can achieve comparatively a much better performance in terms of quadrature stability and noise. Provided

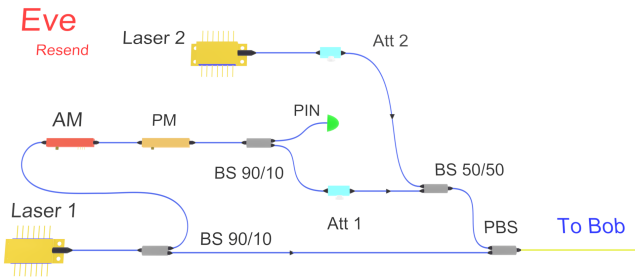

Figure 4.5: Setup for incoherent coherent attack strategy, relying on pulse injection from an external incoherent laser to induce saturation. AM: Amplitude Modulator, PM: phase Modulator, BS: BeamSplitter, PBS: Polarization BeamSplitter, Att: Variable Attenuator.

the channel loss is not too small (low channel loss make it more difficult for Eve to succeed in the intercept-resend attack), then incoherent attack strategy set-up displayed on Figure 4.5 can be successfully used to obtain a full break of QKD security: Alice and Bob estimate that secure key can be distilled, at a positive key rate and see no change in the estimated loss ($T_{sat} = T$) , however the attacker has some knowledge about the key and hence QKD security is broken.

The results of the experimental implementation of incoherent strategy for saturation attack are displayed on Figure 4.6(a). The equivalent excess noise at the input is estimated from the variance of saturated homodyne output experimental data, for different transmission distances. It can be seen that, taking finite size effects into account, excess noise bellow the null key threshold can be achieved, for distances above 35 km, while keeping $T_{sat} = T$ which is the signature that Eve can launch a successful intercept-resend attack and remain untraceable.. On the other hand, for distance below 35 km, the success condition $T_{sat} = T$ cannot be fulfilled, and the attack cannot be launched without being possibly spotted by Alice and Bob.

4.3.2 Towards security certification

The maturity of the field of quantum communication is reflected in the recent development of impressive QKD networks, such as the one deployed in China [CZC+21], spanning thousands of kilometres and linking four metropolitan areas. In 2019, the European Commission has moreover launched the EuroQCI initiative aimed at deploying a pan-European quantum communication infrastructure in the next 10 years, connecting strategic public sites [LT19]. However, in order to take the final step towards a trusted global quantum infrastructure, the ability to evaluate and certify the implementation security of practical QKD implementation has become one of the most pressing challenges.

A standardized approach for security certification of quantum cryptographic devices

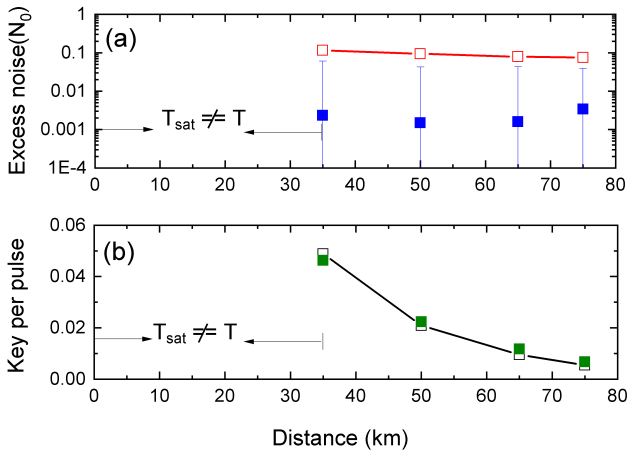

Figure 4.6: Results:- attack with incoherent light. **(a)** excess noise at Alice. Red squares indicate the null key noise threshold and blue squares the estimated values of ξ_{sat}. **(b)** Key rate per pulse, estimated under collective attacks. Black squares are simulated values of final key per pulse while Green squares are from the experiment. Error bars are one standard deviation of fluctuations among ten smaller data block of size 10^7.

will moreover be a key driver to increase, in not enable their commercial use in the context of highly regulated security-related markets such as telecom, health and critical infrastructures.

Security certification of QKD undoubtedly constitutes a complex task, requiring the collaboration of experts from different fields ranging from IT security, quantum engineering and theory. Over the last few years, several international standardization organizations have however been actively working towards this goal, under the unified Common Criteria framework : ISO/IEC JCT 1/SC 27 has been focusing on the security requirements , security evaluation, testing and specification of point-to-point QKD modules [ISO20]. In parallel, within the ETSI QKD ISG, we have contributed to identify and categorize the known implementation attacks against QKD in a 2018 white paper [LSA+18]. This work is now moving to a second level, the QKD ISG is now collective working on an important milestone: writing the first QKD Protection Profile [ETS21], i.e. a document that will be to provide a framework to analyze the implementation security of a QKD implementation, but also a standardized approach for the evaluation and the security certification of QKD systems.

QKD Attack rating In a recent work, [KMQA21], we have proposed some concrete steps towards this goal and have shown how to conduct QKD vulnerability assessment in practice , based on a sound methodology inherited from Common Criteria. Taking a running

CV-QKD system as a reference platform, we have experimentally tested and rated the two different attack paths, namely the coherent and incoherent saturation attack mentioned above.

The Common Criteria [CEM17], offer a comprehensive methodology and metrics to rate possible attacks against the QKD security assets. This methodology generally considers both the likelihood that a threat agent may successfully perform the attack and the magnitude of the impact that this attack has on the assets. In our rating procedure we have focused on the likelihood of an attack, evaluating the total effort required to successfully mount the attack, called the **Attack Potential**: the higher the Attack Potential, the lower the chances of the attack being performed are.

	Attack Potential					**Rating**	**Experimental Results**
Coherent Attack	Exp 6	KoT 3	WoO 10	Equ 7	**AP** **26**	**Beyond High**	✓ Noise experimentallly characterized × Attack not feasible under noise model
Incoherent Attack	Exp 3	KoT 3	WoO 4	Equ 4	**AP** **14**	**Moderate**	✓ Attack experimentally demonstrated

Table 4.1: Summary of the analysis on the two attacks to the homodyne detection. We have reported the values for each factor of the Attack Potential, namely: Exp. stands for Expertise, KoT for Knowledge of the TOE, WoO for Window of Opportunity and Equ for Equipment. The factors chosen for the analysis are from Common Criteria [CEM17].

The rating procedure consists in attributing a numeric value to the Attack Potential, the sum of them is the actual Attack Potential. In the Common Criteria framework, rating is performed by considering the following factors: a) Expertise, b) Knowledge of the TOE, c) Window of opportunity, d) Equipment, e) Elapsed time.

In the context of the attack on a lab systems, the Elapsed time factor (that typically designates the time elapsed between the release of a given product version, and the release of hardware of software security patches) is difficult to evaluate and was hence not considered. We have on the other hand evaluated all the other four factors. order to rate the two attacks paths for the saturation attack against CV-QKD Concerning the knowledge of the TOE we have assume that the hacker Eve tries to obtain as much information as possible about the Target of Evaluation (TOE) design, i.e. Eve has a good knowledge about the specifications of the main components of the QKD system. Some important details might however be system-specific or protected by a non-disclosure agreement between the vendor and the owner of the QKD system. For this reason, for both attacks, the Knowledge factor for the TOE factor is evaluated as *restricted*.

Both attack paths rely on the intercept-resend strategy and can in principle be launched in real time. However, such online implementations of the attacks require to evaluate the optimal value of the displacement Δ and of the gain G (see methods): this can be obtained by manually tuning Eve's setup and measure the excess noise due to displacement. Assuming a frequent trusted evaluation of the channel loss, this tuning might be quite challenging, especially in the case of the coherent attack, where the tuning precision is inevitably limited by the accuracy of the phase locking. As a result, for the coherent attack the Windows of Opportunity can be chosen as *difficult*, while *moderate* for the incoherent attack. Another important difference between the two attack paths is related to the requirements in terms of equipment and expertise. As previously explained, the coherent attack requires Eve to resend coherent displaced signal while being successfully phase locked with Alice and Bob. To achieve this, Eve needs to be an *expert* in coherent optical communications, able to control noise at the quantum level and to have access to *bespoke* equipment. On the other hand, the incoherent attack only requires Eve to send an incoherent signal, without worrying about being phase locked with Alice and Bob: this is reflected in a simplified setup (Equipment *specialized*) and in a lower level of required technical expertise for Eve (Expertise *proficient*). Based on correspondance between the different factors and their numerical value (see [KMQA21] for details) we obtain an Attack Potential of 26 and 14 for coherent and incoherent attack respectively. As expected, the coherent attack is rated as *beyond high*, while the incoherent attack is only rated as *moderate*.

These results illustrate the importance of rating attacks in order to prioritize the implementation of countermeasures and to steer the design and engineering of practical QKD systems towards the highest possible security standards, paving the way to their security certification.

Chapter 5

Perspectives

As detailed in chapter 4, QKD can offer, *in principle*, a distinctive security advantage over classical techniques, particularly in contexts where long-term protection is required. Moreover, as exposed in chapter 3, tremendous progress have achieved on the technology side with the development of QKD systems that exhibit increased performances and their field deployment over optical networks.

Yet the question of he usefulness of QKD to serve real-world use cases *in practice* is still considered a controversial question: On the one hand, the importance of pushing further the integration and use of QKD technology is strongly supported by the quantum research and the emerging quantum industry community. The support to the development of QKD technology is also important on the institutional side, with strategic investments from leading scientific countries over the past years in QKD technology and quantum communication infrastructures (including China, Korea, Japan, UK, Germany) . On the other hand, the importance of pushing the development of quantum cryptography towards the application side has often been considered with skepticism by notable representatives of the cybersecurity community [PPS07, Sch18, NCS20, ANS20, NSA20].

This divergence of views, between the quantum and classical cryptography practitioners is obviously not uniform over the two communities. Remarkable advances involving fruitful collaborations between quantum and classical cryptographers are indeed occurring at an increasing rate [BS16, Sas18, PAB+20]. However, we also believe that this disagreement has some structural causes and has moreover lead to some gap between the communities that may hinder progress towards a better mutual understanding. We also believe that this gap can be reduced, if not fully closed, by updating vision and research programs, and that this reconciliation can play a significant role in the future progress of practical quantum cryptography. The objective of this chapter is to try to take one step back and analyze the reasons of such diverging views and to identify some grounds on which they could be reconciled.

After a first section in which we try to analyze and better understand the complex dialectic behind the classical versus quantum cryptographic discord, we then propose some directions to overcome the identified challenges. One of these directions consists in con-

sidering security models strictly stronger than what can be achieved with computational cryptography, and yet weaker than QKD standard security model. We have started to explore this direction already a few years ago by considering hybrid security models and are now reaching some tangible results with the so-called quantum-computational timelock security model and key establishment construction [VA20]. We will present this work in a second section. We will then elaborate in a third section on the perspectives towards the development of real-world quantum cryptography. This will lead us to link the question of security gain evoked in chapter 4 with the identification of promising application domains for quantum cryptography. In a sense we will revisit the childish but also invigorating question: "what is quantum cryptography good for?" and to try to formulate some elements of answers. This will also lead us to propose some perspectives for future research and technology development, rooted in an updated vision of quantum and classical cryptography respective positioning.

5.1 Critical assessment of quantum cryptography positioning

As emphasized in the introduction and illustrated in the different chapters of document, the work achieved in order to push QKD towards its application frontiers has a double outcome:

1. Major breakthroughs: at technological level, in topics such as quantum communication components and systems, quantum networking but also at fundamental level, in topics such as quantum information theory, security models and proofs.

2. A better understanding of the technological, but also fundamental reasons for a gap between envisaged applications, and what technology can actually deliver.

After having mostly focused on the first aspect so far, we want to make seize the opportunity of this Habilitation thesis to also investigate the second aspect that is probably less frequently tackled, and address the following key questions: *Why has QKD technology not yet been as successful, in terms of applications and impact, as many of us were expected 20 years ago?* This question will lead us to consider how we should update our vision and revise our targets both in terms of technology and applications in order to tackle more efficiently the outstanding challenges.

5.1.1 Classical and quantum cryptography: a complex dialectic

A structural and fertile dispute

The dialogue between quantum and classical cryptography, is by essence, and since the inception of quantum cryptography, driven by a dispute on the foundations of cryptographic security: can we let is rest on computational hardness assumptions, or should we claim to provide stronger guarantees, and rely on information-theoretic security ?

This questioning is at the heart of the groundbreaking BB84 paper, that appeared in the Proceeding of the ICCSSP conference held in Bangalore in 1984 [BB84], after having been rejecting from major cryptography conferences. There, Charles Bennet and Gilles Brassard, make clear that quantum cryptography objective is to challenge conventional cryptography relying on computational security:
«*Conventional cryptosystems such as ENIGMA, DES, or even RSA, are based on a mixture of guess work and mathematics. Information theory shows that traditional secret-key cryptosystem cannot be totally secure unless the key, used once only, is at least as long as the cleartext. On the other hand, the theory of computational complexity is not yet well enough understood to prove the computational security of public-key cryptosystems. In this paper we use a radically different foundation for cryptography, viz. the uncertainty principle of quantum physics. In conventional information theory and cryptography it is taken for granted that digital communications in principle can always be passively monitored or copied, even by someone ignorant of their meaning.* »

This radical challenge to conventional cryptography, has been extremely stimulating and fertile and has played a fundamental role in the fantastic development of in quantum information and quantum technologies, over 40 years, if we date it back to the birth of quantum information science a to the mythic Physics of Computation Conference in 1981 [QC421]. The dispute between quantum and classical cryptography must somehow be seen as a reciprocal challenge, which is all the more fascinating that it is often misunderstood:

- As Bennett and Brassard have clearly expressed, the program of quantum cryptography is to challenge the security fondations of classical cryptography, and to develop cryptographic protocols based on information-theoretic security, for some of the core cryptographic services needed in our digital society such as key establishment mechanism or multi-party computation.

- Reciprocally, classical cryptography constitutes a challenge on the practical side for quantum cryptography. As a matter of fact, it is important to realize, as detailed in chapter 2, that essentially all quantum cryptographic primitives can also be obtained with classical means, under computational assumptions. In this sense, classical cryptography constitutes a direct benchmark for quantum cryptography, in terms of security versus resource requirements and performances, for all quantum-enabled security services.

Systematic opposition can have detrimental effects

The structural dispute between classical and quantum cryptography has been extremely stimulating. It has in particular lead to outstanding developments on the quantum cryptography side, both in terms of fundamental concepts and in terms of technology. However, this competition may also turn into a systematic opposition, which can hamper the mutual understanding between the classical and quantum crypto communities, and thus

the collaborations at this nonetheless essential frontier. We try to analyze here some of the reasons that may have triggered or fueled such a dynamic of systematic opposition, and point at its detrimental consequences.

Some damaging confusions

The reciprocal challenges that classical and quantum challenges address to each other, may lead to simplistic answers triggered by the temptation to assert that the absolute truth is held by one side only. Such positions, in case they manage to spread, can the source of important and damaging confusions. We pinpoint some examples of influential assertion that are yet based on confusions, illustrating also that they may arise from both sides.

«All cryptography primitives will become quantum-based » The belief that cryptography is bound to become fully quantum might be influenced by the vision of technology and innovation as a creative destruction process [Per95], where successful technologies have to disrupt and replace older ones, in order to develop. It is not our subject here to question Schumpeter's theory, but to note that the creative destruction vision does not apply to quantum cryptography, and in general to other branches of quantum technology such as quantum computing or sensing. As a matter of fact, even though all these quantum technologies can imply profound paradigm shifts, they don't imply the "destruction" or their classical counterpart.

If we focus now on cryptography, it is important to realize that several public-key functionalities (where a very large number of users may publicly engage in parallel in a protocol, such as for example public-key encryption or verification of a digital signature) play a fundamental role in our digital word and yet that they *cannot* be obtained with quantum means with information-theoretic security. Confusion however often arises with respect to this latter aspect. For example, some (otherwise quite interesting) work on information-theoretically-secure classical message authentication schemes using quantum means has been coined as "Quantum Digital Signature" [AA15], even though it does not verify the properties of a digital signature, and in particular public verification.

«The quantum threat on cryptography implies the need for QKD » Another important source of confusion, and of discord between the classical and quantum cryptography community, is related to the different directions that can be considered and enforced in order to guarantee that cryptography would still remain safe against futuristic attackers in possession of (large) quantum computers. As a matter of fact, the discovery of a polynomial-time factoring algorithm by Peter Shor in 1994 [Sho94], implies that such quantum computers could in principle be used to factor large numbers exponentially faster than classical machines, threatening a large fraction of public-key cryptography and therefore of a fundamental pillar for Internet security. Early claims from the quantum cryptography community might have been biased towards the conclusion that computational cryptography as a whole was threatened, promoting quantum cryptography, and in particular QKD as the preferred solution, in order to avoid a "cryptocaplyse".

This first level of confusion has been rapidly settled, notably via active interactions between the Quantum cryptography [Bra16] and Post-Quantum Cryptography (PQC) [Ber09] communities, with an agreement on both sides regarding the importance of proposing new solutions to address the quantum threat. However, an important aspect of the question is still often neglected by the quantum cryptography community: while Shor algorithm certainly weakens the security foundations of public-key cryptography, its impact on symmetric-key cryptography is much less dramatic [Ber09]. This hence opens the possibility to use fully-symmetric solutions, (i.e. come back to some pre-1970 cryptography solutions) in order to build quantum-safe security infrastructures. This also implies that symmetric solutions constitute the real contender and should be the reference point when designing quantum-based security infrastructures. This point, recently voiced by ANSSI [ANS20] however remains largely overlooked by the quantum cryptography community. It constitutes, on the other hand, a central motivation for our work on hybrid quantum computational security models (cf next section).

«QKD systems cannot be made practical » Some PQC supporters may also turn out to be QKD skeptics, thereby pointing at practical limitations of QKD technology as a reason to disregard its use in real-world use cases [NSA20, NCS20, ANS20] . As explained in chapters 3 and 4, QKD does have performance limitations, and has to face some new challenges on the implementation security side. However, these challenges are addressed with energy and method [LSA+18, XMZ+20, PAB+20, CZC+21, LT19]. Real-world deployment, performance enhancement, drastic cost reduction and certification of QKD therefore all constitute tangible and reachable milestones for the years to come. There however hence seems to be a blatant contradiction in the position mentioned above: how could one consider realistic the fact that large quantum computers could be built within 10 to 15 years, and yet that building affordable and secure QKD systems over the course of the next 5 to 10 years would be technologically out of reach?

Antagonistic positions

The most serious risk, in relation with the dynamic of opposition that we have evoked and the confusing positions that are sometimes largely relayed, would be install some form of long-term antagonism between the classical and cryptography community.

After having worked on these questions for some time [ARW+07, ABB+14, LSA+18] and as expressed publicly at several occasions already [All17, All19a], my impression is that this dissensus has reached problematic levels. More precisely, the debate seems to have at least partially crystallized into antagonistic positions:

- Driven by the idealistic goal of developing "a cryptography based solely on the laws of physics" [CCD+15], but also by the practical confusions that we have pointed above, a fraction of quantum cryptography community tend to believe that quantum cryptography could and indeed should, on the long run, replace classical cryptography.

- Irritated by such implicit superiority claims doubled by approximate positions, some opinion leaders of classical cryptography have developed an antagonistic rhetoric with respect to quantum cryptography and QKD in particular [Ber18, Sch18, NCS20, NSA20]. They rightly point at some confusions and over-claims concerning the application scope of quantum cryptography, but also tend in the same movement and yet on erroneous grounds - often based on outdated information such as the supposedly lack of authentication, or the impossibility to guarantee implementation security [NCS20, NSA20] - to deny any practical application of QKD, if not to dismiss the interest of the whole quantum cryptography field.

5.1.2 Bridging the divides by resetting priorities

A long-term opposition between classical and quantum cryptography would have negative consequences, hindering interactions and joint research work. It must hence be contained and even, if possible, ended. Acknowledging the synergy between classical and quantum cryptography can constitute an important step on that direction that however also need be complemented by a shift in the vision and methods.

Take advantage of synergies and acknowledge complementarity

One central reason to aim at stronger cooperations between classical and quantum cryptography communities is based on the fact that both subjects are anyway intimately linked: they share common theoretical foundations, but also common challenges and application domains. Understanding how to operate cryptography in a quantum world is for instance a central challenge both for PQC and for quantum cryptography. If we consider quantum cryptographic primitives, including QKD (as explained in chapter 4) most of them need to be combined with other classical primitives, and therefore must be studied jointly. Finally, cryptographic formalism, definitions and proof techniques that have been gradually put on firm foundations [Gol09] constitute an invaluable framework that quantum cryptography may aim to augment, but certainly not to ignore and redefine.

The strong ties between classical and quantum cryptography form an outstanding basis for joint undertakings in science and technology and it clearly appears that isolating both subjects from on another would be elusive. In that respect, one of the main message developed in chapter 4:

Quantum Cryptography cannot replace Classical Cryptography, but is complementary.

probably still requires to be more convincingly and broadly conveyed and acknowledged. Variations around this message have already been clearly articulated [PPS07, ABB$^+$14, ANS20]. This message however enters in conflict with some of the confusing assertions mentioned previously and that remain influential. Such misconceptions have indeed not fully disappeared, with detrimental effects: push the communities further appart and undermine confidence. Further efforts to broadcast this message and to make it more widely acknowledged hence remains important.

Reconsider the objective of «Absolute security»

As illustrated by figure 1.2 and in more depth within chapters 3 and 4, QKD technology has a dual nature and the dynamics of the field is driven by parallel objectives:

1. QKD is a communication technology and its development shall be based on engineering work improving the performance versus cost trade-offs so that it can meet a demand as large as possible.

2. QKD is also a cybersecurity technology, often characterized by the promise to offer "absolute security" [MMMP99, LMC05]

The pursuit of these two objectives has been incredibly stimulating and has lead to remarkable progress on the conceptual and technological sides. However, since the competencies needed to address these challenges are generally held by different engineers and scientists, tackling jointly the practicality and security aspects of QKD represents a formidable challenge. As a consequence these questions are, to a large extent, addressed separately or sequentially.

This dissociated approach of the security and practicality of QKD has so far essentially allowed to escape a central contradiction, however clearly identified in [GRTZ02b]: *Absolute security implies infinite costs, which in turns implies zero practical interest*, which means that the two objectives listed above are fundamentally incompatible.

This leads to a central dilemma and the need to actually make a choice between conflicting objectives to solve this dilemma. The nature of this choice has already been identified a decade ago, by Valerio Scarani and Christian Kurtsiefer in their "black paper on quantum cryptography" [SC14] and clearly expressed, in the quote below:

«This leads us to guess that the field, similar to non-quantum modern cryptography, is going to split in two directions: those who pursue practical devices may have to moderate their security claims; those who pursue ultimate security may have to suspend their claims of usefulness.»[SC14].

Scarani and Kurtsiefer exhort the QKD community to open their eyes on the divergence between two distinct objectives, but also on the price to pay for such a clarification. Concerning practical QKD, which constitutes our main focus, this clarification most certainly require to acknowledge the need to *relativise absolute security claims* and to redefine on more practical grounds the type of security guarantee that real-world QKD systems are able to bring in practice.

Such clarification, despite its symbolic cost, can foster QKD progress in terms of engineering and implementation security. As a practical and concrete approach, we have recently illustrated how the use of Common Criteria vulnerability analysis methodology, based on attack ratings allows to guide system design and to establish a lower bound on QKD practical security [KMQA21].

Aim at provable security under more realistic models

As we write these lines, the vast majority of the QKD community remains reluctant to fully acknowledge the dilemma pointed by [SC14] and to give up the absolute security claim, even for practical QKD. An important reason for that certainly lies in the simplicity and in the symbolic power of targeting absolute security, without any assumptions. However, even at the most abstract level, this claim might be difficult to ground on a solid correspondance with the physical world and the physical implementation of QKD, as illustrated by the recent ad absurdum refutation by Bernstein invoking the holographic principle [Ber09]. It is also interesting to note the recent answer by Renner and Renes [RR20] invoking fault-tolerant quantum computation as a justification - arguably far from practical - for the validity of QKD absolute security model.

Beyond these difficulties, there is also a central reason to cherish the absolute security model: it has provided and still provides a powerful framework that has allowed to make key conceptual progress and develop fantastic research that has lead to a composable security definition and proof of QKD [Ren05], capitalizing on a remarkable series of work spanning over more than 10 years [BBCM95, SP00, May01, BBB$^+$06, BOHL$^+$05b].

We propose to consider more "realistic" security model as a way to better capture and define security properties that could then be enforced in practice, with high assurance. This will typically rely on trading the objective of ultimate security (with no or strictly minimal assumptions) to security models with additional assumptions. Such evolution should however not be a leap into the unknown. Formal proofs, based on a precise security model certainly constitute one of the most precious asset of quantum cryptography. Moving towards new security models for quantum cryptography, car only be envisaged if *provable security*†i.e. the ability to derive security claims from rigorous logical reasoning, is kept as an intangible principle for quantum cryptography.

Diversifying with respect to one main security model also present the risk to end up with models, protocols and security claims that become very complex, at that may be difficult if not impossible to to compare. We can note this phenomenon currently exists in modern cryptography, that rely on computational assumptions that are in general not directly comparable. However, complexity theory and the use of restricted models [Sho97], and reduction-based reasoning coupled with generic unifying approaches [MPZ20] constitute powerful tools to compare security models. It seems important to aim at such comparative analysis, also in quantum cryptography. Studying the possible reductions between different existing quantum cryptographic protocol has howerver often been left aside so far, which contributes to some of the confusion that we pointed at in the previous subsection. For example the reduction of Quantum Digital Signatures [AA15] to QKD followed by information-theoretic authentication [Sti94] is often ignored. In the same spirit, we have realized that despite the very large literature on Quantum Secure Direction Communication (QSDC) [DLL03], the protocol properties have only been informally defined. We are currently working on a paper [SAL22] aiming at providing a property-based comparison between QSDC and QKD combined with One-Time-Pad encryption.

5.2 Quantum cryptography in a hybrid security model

5.2.1 Extended security models in quantum cryptography

As presented in Chapter 2 the use of quantum ressources 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 plann 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. The development of theoretical quantum cryptography however allowed to establish that some cryptographic functionalities such as secure multi-party computation [May97, LC98] or position-based cryptography [LL11] are impossible to realize in a quantum world against an unbounded attacker, due to no-go theorems.

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. Before presenting our work on a new security model [All15b] in the following of this section, we present here an overview of the work related to the interplay between adopting weaker security model than unconditional security, and obtaining additional quantum cryptographic primitives with extended functionalities or properties.

Assumptions on the storage capabilities of the adversary 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.

In the *bounded-quantum storage model*, introduced by Damgard, Fehr, Salvail and Schaffner [DFSS08] one assumes that the adversary can only store a limited amount of qubits. This model is inspired by the classical bounded storage model, [CM97], 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 [WST08], 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 and 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 [KWW12], while en-

tanglement sampling technique allows to to extend the validity of the noisy storage to the case where the time-limited bound applies to the quantum capacity [DFW14].

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$^+$14] and has been experimentally demonstrated [LHA$^+$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 [LL15]. However such constructions resort to random coding arguments for which practical implementation with structured measurement is not possible.

Everlasting security based on shot-term computational security assumption A 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 trusted signature cards.

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.

5.2.2 Quantum Computational Timelock Security Model

Model Assumptions We proposed in 2015 [All15b] 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:

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 ciphertext 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 $\mathcal{N}_t : \rho \to \mathcal{N}_t(\rho)$. The assumption related to noisy storage and decoherence is characterized by:

$$\forall t > t_{coh}, \forall \rho \qquad \frac{1}{2}\left|\left|\mathcal{N}_t(\rho) - \frac{\mathbb{I}_d}{d}\right|\right|_1 = o\left(\frac{1}{d}\right) \tag{5.1}$$

It is interesting to note that these two categories of assumptions, namely short-term computational security [Unr15] and noisy quantum storage [KWW12], have so far already been considered in quantum cryptography, yet only disjointly.

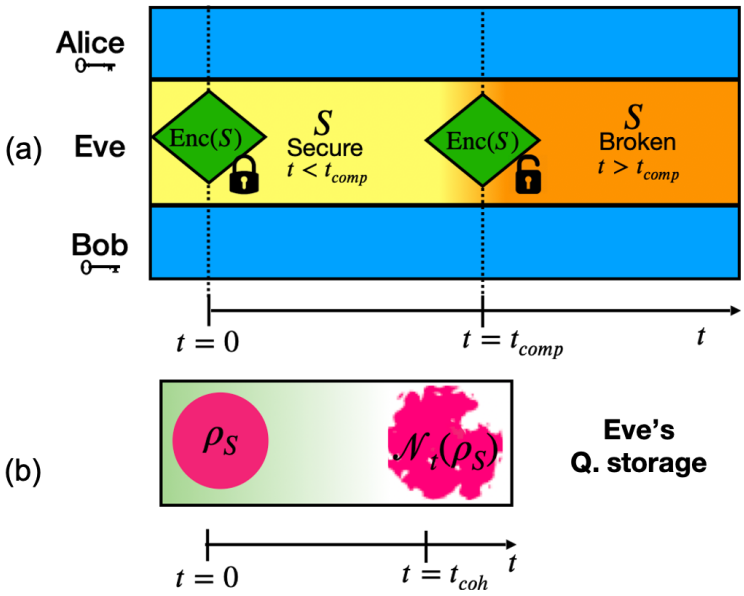

Figure 5.1: QCT security model: Assumption (a): Short-term secure encryption during time t_{comp}, during which Alice and Bob can exchange an ephemeral classical secret S. Assumption (b): Time-limited quantum memory, with coherence time $t_{coh} << t_{comp}$

.

Validity of QCT security model It is also important to discuss about the validity of the model, and in particular about its central assumption: $t_{coh} \ll t_{comp}$.

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, we reviewed in [VA20] 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.

Rationale of the Quantum Computational Timelock 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 limits the power of the attacker with respect to the quantum channel, but where trust assumptions 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.

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 subsection) the resulting protocol cannot be unconditional 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.

- Improvement of the performance envelope, with respect to QKD and more broadly to repeaterless quantum secret capacity fundamental bounds [PLOB17]. This im-

provement 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.

5.2.3 MUB-QCT key establishment protocol

In [VA20] we have proposed and studied a key agreement protocol that we called **MUB-Quantum Computational Timelock** (MUB-QCT), where a single bit x is encoded on n 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) and a set of pair-wise independent permutations.

MUB-QCT Encoding and Decoding (one channel use)

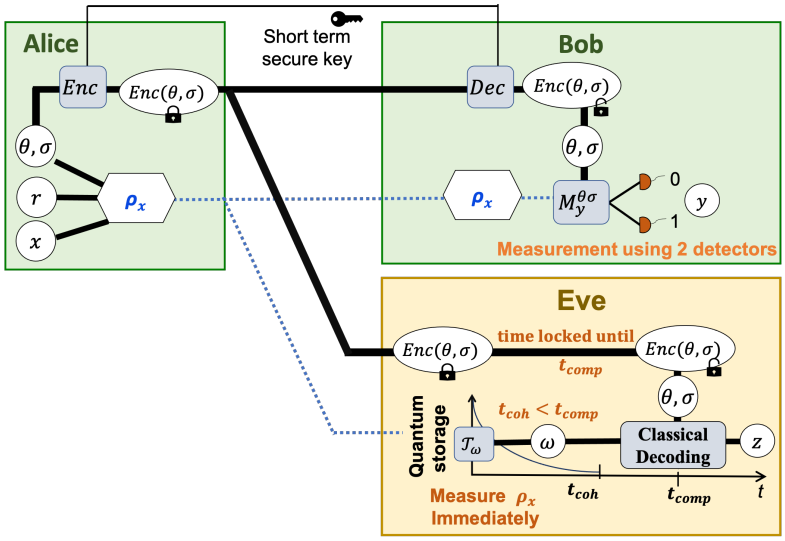

Figure 5.2: One channel use of MUB-QCT leads to a classical wire-tap scheme w.r.t. bit x:
(a) Low-noise binary classical communication channel $x \to y$ between Alice and Bob.
(b) Noisy binary communication channel $x \to z$ between Alice and Eve. Due to QCT assumptions, Eve is forced to measure ρ_x immediately at reception, and to later decode z using her measurement result ω and post-measurement information S.

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 $x^n := (x_1, \ldots, x_n)$, $x^n \in \mathcal{X}^n$.

We shall call $A = A_1 A_2$ 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 $\{|i_{xr}\rangle\}_{x\in\{0,1\},r\in[d/2]}$.

An essential element of MUB-QCT protocol will consist in randomizing on of the basis states of A using two 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.

Encoding at Alice

- *Setting a computational timelock:* 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 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 $x \in \{0,1\}$, 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

$$|\psi_{x,r}^{\theta,\sigma}\rangle = P_\sigma U_\theta |i_{x,r}\rangle \tag{5.2}$$

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

$$M_y^{\theta\sigma} = \sum_{\theta,\sigma} (P_\sigma U_\theta)^\dagger (\sum_{r=1}^{d/2} |i_{y,r}\rangle\langle i_{y,r}|)(P_\sigma U_\theta)^\dagger) \tag{5.3}$$

1-MUB-QCT Key Establishment Protocol (Single copy case)

Protocol 1 *1-MUB-QCT Key Establishment*

Setting: *: Single-copy encoding overa d-dimensional Hilbert space A, noisy and lossless quantum channel, n channel use.*

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.*
   - *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 p_e. If 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.*

Remark: the generalization to the case of a lossy quantum channel could be addressed relatively simply, by adding a sifting phase,.

Security analysis

Eavesdropping model We consider the worst-case scenario where Eve has full access to the channel input, as depicted on Figure 5.2. This is similar to the strong locking scenario as considered in [GHK+14]).

Hence from Eve's viewpoint, that does not know r, nor $S = (\theta, \sigma)$, the quantum state at channel input can be described by a density matrix ρ_x with

$$\rho_x = \frac{1}{|\theta||\sigma|} \sum_{\theta\sigma} P_\sigma U_\theta \Big(\frac{2}{d} \sum_{r=1}^{d/2} |i_{x,r}\rangle\langle i_{x,r}| \Big) (P_\sigma U_\theta)^\dagger \tag{5.4}$$

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 $z \in \{0, 1\}$.

Proposition 1 (Strategy II is optimal) *If Eve follows the strategy I, her success probability to guess the bit x correctly can be upper bounded given the decoherence model described in Equation (5.1), as $P^{\mathrm{I}}_{guess}(X|E) \leq \frac{1}{2} + o\Big(\frac{1}{d}\Big)$. If Eve follows strategy II, one simple strategy is to perform a measurement in a random MUB, followed by post-measurement decoding. This achieves success probability at least $\frac{1}{2} + \Omega\Big(\frac{1}{d}\Big)$. We can prove a matching upper bound, indicating that this is essentially the optimal strategy, by considering the measurement in a fixed basis (Eve has no preferable measurement basis since the full set of MUBs forms 2-design). Based on the work of Berta et. al., on Quantum to Classical Randomness Extractors [BFW13] we can establish that such generic strategy II, reduces to applying a strong QC-extractor to ρ_x. Taking the parameters of the 1-MUB-QCT protocol into account, this proves that $P^{\mathrm{II}}_{guess}(X|Z) \leq \frac{1}{2} + \Omega\Big(\frac{1}{d}\Big)$ and consequently that the optimal eavesdropping strategy is II.*

Performance Analysis Since the MUB-QCT protocol defines an effective wire-tap scenario, the key rate in the asymptotic limit for the MUB-QCT protocol, can be derived using following Csiszár and Körner formula [CK78]:

$$\begin{aligned} R &\geq I(X;Y) - I(X;Z) \geq H_{min}(X|Z) - H(X|Y) \\ &\geq -\log_2 \Big(\frac{1}{2} + \frac{1}{d} \Big) - h_2(p_e) \end{aligned} \tag{5.5}$$

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 [CBKG02], 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 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 5.3.

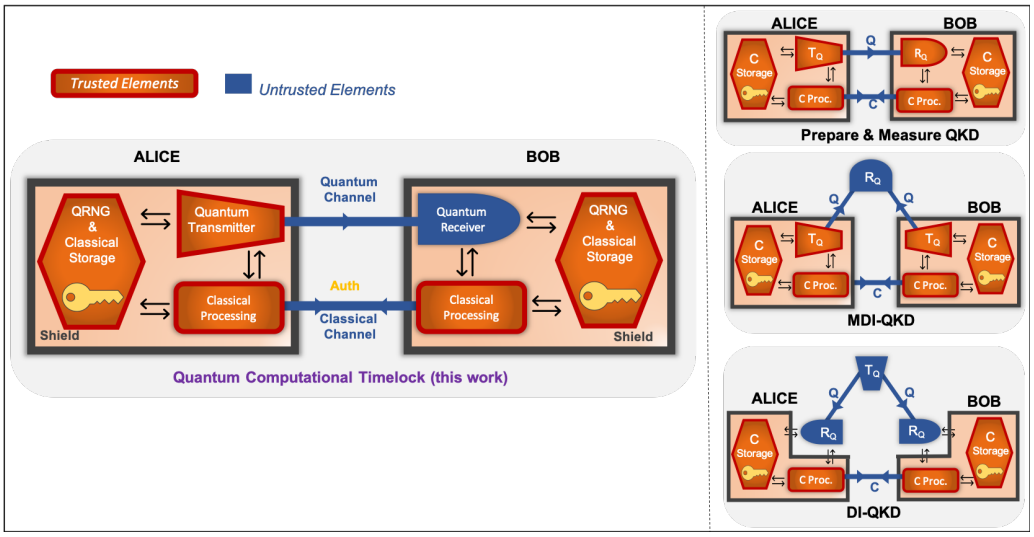

Figure 5.3: MUB-QCT trust requirements compared with those of standard QKD, MDI-QKD and DI-QKD. MUB-QCT enjoys some MDI-type security features. This characteristic can have an important practical impact by allowing to relax key engineering constraints.

m-MUB-QCT with multiple quantum state copies

The 1-MUB-QCT protocol considered the quantum communication of a single qudit state $P_\sigma U_\theta |i_{x,r}\rangle$ 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 $P_\sigma U_\theta |i_{x,r}\rangle$ 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 $\sim m$.

Security analysis of m-MUB-QCT against restricted attacks

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 $m > 1$.

We can however perform security analysis against restricted attacks, by considering two relaxations:

- *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).
- *Non-adaptative attacks*. This corresponds to assuming that Eve cannot update her attack strategy adaptively, over the m copies.

Under these restrictions, we can show that the optimal strategy corresponds to ***Proactive MUB measurement:*** in which Eve proactively measures each of the m copies in a different MUB and performs post-measurement decoding when learning θ and σ . Using the fact that the set of permutation operations commutes with MUB basis change, 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 information increases linearly with m as $I^{\mathrm{Pro}}(X;Z)_m = \mathcal{O}\left(\frac{m}{d}\right)$. This implies Eve cannot guess x perfectly when significantly less than d copies of the state $|\psi_{x,r}^{\theta,\sigma}\rangle$ are sent by Alice.

Performance Analysis

The proactive MUB measurement strategy 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 shown in Figure 5.4. Analyzing the plot in Figure 5.4, we observe three distinct regimes, *Constant rate regime*: short distance, where the secret key rate is constant and commensurate; *Single copy regime*: where the key rate is similar to the single copy case, scaling as the transmissivity T; *Cutoff regime*: long distances, where detector dark count rates dominate, sharply limiting the secret key rate.

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

5.2.4 QCT: Challenges and Future work

The Quantum Computational Timelock framework constitute a promising route towards real-world quantum cryptography (RWQC) with extended performance and functionalities. In particular, our newly proposed MUB-QCT protocol enables everlasting security

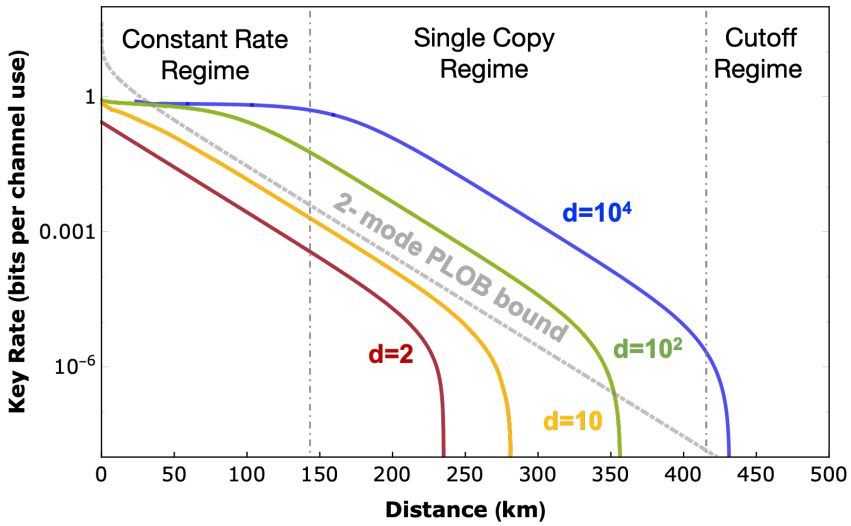

Figure 5.4: Key rate per channel use as a function of distance, for m-MUB-QCT protocol against proactive MUB measurement strategy. The key rate at a given distance iss maximized over the photon number m. The parameters assumed in the plots are: Loss 0.2dB/Km; $P_{dark} = 10^{-6}$; efficiency of detectors $\eta = 25\%$; visibility $V = 98\%$. Since MUB-QCT can be implemented with 2 detection modes (2-single photon detectors) we also plot 2-modes PLOB bound [PLOB17] as a benchmark..

key establishment with reduced trust requirements at reception side, and with rates and reach significantly outperforming those of QKD.These theoretical results need to be consolidated but also experimentally tested and validated so that the relevance of the QCT approach for RWQC can be assessed.

This leads to interesting new challenges for quantum cryptography in hybrid quantum computational security models. On the theory side, a central challenge, that we have started to investigate, consists in proving the security of m-MUB-QCT against general attacks. We conjecture that secure key rate can be obtained with up to $m \sim O(\sqrt{d})$ against general attacks, guaranteeing significant performance improvement in practically achievable multimode regime, even though lower than in the restricted analysis presented on Figure 5.4. Another fascinating challenge, that we also intend to tackle, is related to the design of repeater schemes in the QCT security model.

Building MUB-QCT demonstrators will require to prepare, modulate and detect high-dimensional quantum encodings. Finding efficient and robust implementation schemes and performing experimental demonstrations will hence be very important in order to establish the practicality of the QCT approach. Multiple quantum systems demonstrated so far in the context of high-dimensional QKD constitute interesting reference points indicating the in-principle feasibility of MUB-QCT: they include temporal-spectral [NWS+13, AKBH07], orbital angular momentum (OAM) [SBF+17, MMLO+15] as well as spatial mode [DBD+17] encodings. In terms of dimensionality, existing time or spectral

encoding HD-QKD techniques indicate the possibility to operate with d as large as 10^3 but also to envisage even much larger alphabet with existing or near-term technologies by leveraging the specificities of the QCT framework.

5.3 Towards real-world quantum cryptography

5.3.1 A holistic and engineering-driven approach

The divergence between cryptography considered either through the computer science lens or from the standpoint of real-world applications, is somehow already well acknowledged in modern cryptography and exemplified by the existence of different IACR conferences such as `Crypto` [Cry] or `Real-World Crypto` (RWC) [RWC], with distinct scope and positioning and yet tight links. We posit that such a distinction is now becoming increasingly relevant in the context of practical quantum cryptography, and that it is timely to consider the birth of an additional scientific and engineering community in order to develop `Real-World Quantum Crypto` (RWQC).

This leads to the question of the objectives that RWQC should pursue. In particular, if absolute security is not its horizon, can we define an alternative project, allowing to demonstrate a clear security advantage over classical crypto, and yet better suited to practical contexts than abstract quantum cryptography? We answer positively to this question. In particular, we believe that it is possible to address some if the core challenges of QKD, at the application frontier, by trading the quest of absolute security for practical security gains. In this perspective, RWQC emerges as a holistic approach characterized by a shift of priorities towards objectives that integrate a dialectic dimension, balancing the ambition to design cryptographic systems beyond classical reach with engineering constraints and cost-benefit analysis. With the ambition of providing a cryptographic advantage in the real-world,; RWQC can be articulated around two main guiding principles, at logical and physical levels.

Enable security gain for real-world use cases Considering well-defined security models, the objective is to propose end-to-end security services relying on quantum cryptographic protocols that can provide a clear security gain with respect to classical cryptography.

The notion of end-to-end security is very important, and yet often overlooked. It indeed conditions the logical rationale of the choice of cryptographic primitives and their combination. An emblematic question is related to the use QKD as a key renewal technique for AES encryption. As we have seen in section 4.2, QKD enables some security gain, over classical cryptography alone, in terms of post-compromise security. However, the implicit use of AES encryption for secure communications implies that we consider a security model where AES is long-term secure. This also implies that the overall security gain that can be achieved by combining QKD key renewal with AES encryption is marginal

with respect to what can be achieved purely classical solutions based on symmetric cryptography, as argued in [ANS20].

We however want to point out that there exist use-cases where the use of QKD can present strict security gain over classical cryptography (in that case PQC) alone. Such use-cases have in common the fact that QKD is used to securely transport (with OTP encryption) some *scarce and strategic high-security data only*, such as long-term secrets (health data, governmental secrets) or some high-level cryptographic keys.

- An emblematic example is the use of QKD for long-term-secure storage, based on proactive secret sharing, as initially proposed by J. Buchmann and his team [BBD+17], and recently demonstrated in Japan as well as in the OpenQKD project, to secure the storage of long-lived data such as medical records. We however note that QKD performance (key rates) is not yet sufficient to envisage long-term secure storage for large datasets [MGA+20].

- A promising direction consists in combining QKD and PQC in order to obtain clear gains from the combination, as in the recently proposed Muckle protocol [Exc20] where a hybrid key exchange protocol is specified and studied, that presents high reliability with respect to the failure of any of its (PQC and QKD) cryptographic components, but also a performance gain with respect to using PQC alone.

- Another interesting direction is to use QKD in the context of information-theoretic private information retrieval, where the challenge is to guarantee the privacy for data retrieved from shared database [KL21].

- Finally, another promising framework to demonstrate in practice a quantum cryptographic advantage consists in considering the combination of quantum cryptography with quantum sensing, for example in the context of secure time transfer [DSW+20].

Engineer secure and cost-effective quantum hardware Adopting security by design methodologies, the objective will be to build quantum cryptographic systems with a controlled engineering complexity - and therefore controlled cost - for which high security assurance levels can be reached.

The fact that quantum processes can be a source of cryptographic advantage in practice is in a sense obvious, for fundamental reasons related to the unique ability to describe security schemes occurring at the physical layer with the quantum formalism. It can indeed not only provide a complete description of the hardware, but also quantify how information can be exchaged, including bounds on information leakage. What however also represents an unsettled debate, and certainly a frontier for research on cryptographic hardware is to understand how can we transition from formal statements on information-theoretic security, to the engineering of systems with verifiable security properties, notably in terms of information leakage?

These challenges are at the heart of the current international effort towards the definition of standardized methods for security evaluation and certification of QKD [ISO20], [ETS21], as well as QRNG [QRa], to which we actively participate in parallel with the wider reflexion on the vulnerability analysis methodology and on the interplay between theoretical and practical security developed in [KMQA21] and on the central role that engineering complexity should be given. On a more fundamental level, these questions also strongly resonate with device-independent and semi device-independent cryptography. We note that the use of short-term secure computational assumption opens a promising direction to make DI-QKD more practical. [MDCAF20]

5.3.2 Renewed perspectives

Involvement of new stakeholders Structured around engineering-driven objectives, RWQC will require the commitment of new stakeholders, in particular engineers and scientists from the real-world cryptography (RWC) and the cryptographic hardware and embedded systems (CHES) communities. We are convinced that the combination of these expertises with the ones of practical quantum cryptographers and quantum information theoreticians will allow to make decisive progress both a foundational and technological levels.

Provable security for cyber-physical systems In resonance with the current work on QKD and QRNG implementation security, but also Physical Unclonable Functions (PUFs), the interplay between quantum technologies and cyber-physical system security appear to us as a fascinating and largely unexplored field of research .

Quantum cryptographic techniques make in principle possible some very strong forms of security by design, built around some physical and logical reduction to clear-cut processes such as the quantum measurement of an elementary quantum system, or device-independent characterization of measured correlations. In this perspective, security models and the interplay between logical and physical trust assumptions will play a central role, as outlined in 5.2.1 and 5.2.2.

Slow Information I would like to conclude this chapter and this manuscript, by promoting an alternative way to look at quantum cryptography and its applications, through the concept and the metaphor of "Slow Information". This concept is inspired by the "Slow Food" movement [Pet13], founded in 1989 that promotes local, sustainable and quality foods, with the ambition to be simultaneously protected from and included into the global food system. This movement has grown into a global scale over the years [slo], around the central idea that slowness is a key ingredient to differentiate from the food industry and its deficiencies, and to coexist with it.

If we accept the relevance of drawing a parallelism between Food and Data, we can then argue that the Slow Food principles provide interesting perspectives for our digital

and data-driven society, and envisage that quantum cryptography could play a decisive role in building a "Slow information" islands around a few principles that we can sketch:

- Similarly to the focus on "slowness"' in a era of fast-food and fast-paced industrialization of food production, the shift towards "Slow Information" and quantum cryptography would (and could) only target *a small fraction* of the classical data exchanged over modern networks, and *only over restricted geographical areas*, due signal-to-noise as well as trust contraints.

- Slow Information operates over network infrastructures whose physical layer can be fully characterized using quantum information tools. It targets application use-cases where a quantum cryptographic advantage can be reached, which implies relatively small data sets, for which long-term security is needed. This also conversely imply that Slow Information islands should expect to be operated very differently from modern classical networks, in which the physical layer constraints can be essentially abstracted and virtualized.

- Slow Information and the role of quantum networks would however not come as a replacement or in opposition to classical secure networks. They would rely on quantum cryptography, combined with computational cryptography, to protect highly confidential information presenting long-term security needs, with security levels unachievable classically. Based in particular around long-term-secure storage, such quantum networks extend our ability to manage confidential data without resorting to complete physical isolation.

- Slow information shall be based on precise trust assumptions notably with regard to tamper-proof security perimeters and quantum cryptographic systems implementations, that will need to be certified. It shall also be based on well-defined security models and provable security. We are here again tempted to draw a parallelism with the Slow Food movement and its promotion of high-quality products that rely on a cultural heritage whose protection and certification is required, with labels such as protected designation of origin, PDO, or protected geographical indication, PGI.

Bibliography

[AA15] Ryan Amiri and Erika Andersson. Unconditionally secure quantum signatures. *Entropy*, 17(8):5635–5659, 2015.

[AA21] Raphaël Aymeric and Romain Alléaume. Covert continuous variable quantum key distribution. *In Preparation*, 2021.

[AAWJ20] Romain Alléaume, Raphaël Aymeric, Cédric Ware, and Yves Jaouën. Technology trends for mixed qkd/wdm transmission up to 80 km. In *2020 Optical Fiber Communications Conference and Exhibition (OFC)*, pages 1–3. IEEE, 2020.

[ABB+14] Romain Alléaume, Cyril Branciard, Jan Bouda, Thierry Debuisschert, Mehrdad Dianati, Nicolas Gisin, Mark Godfrey, Philippe Grangier, Thomas Länger, Norbert Lütkenhaus, et al. Using quantum key distribution for cryptographic purposes: a survey. *Theoretical Computer Science*, 560:62–81, 2014.

[ABF+16] Gorjan Alagic, Anne Broadbent, Bill Fefferman, Tommaso Gagliardoni, Christian Schaffner, and Michael St Jules. Computational security of quantum encryption. In *International Conference on Information Theoretic Security*, pages 47–71. Springer, 2016.

[AC12] Scott Aaronson and Paul Christiano. Quantum money from hidden subspaces. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 41–60, 2012.

[ACF20] Gildas Avoine, Sébastien Canard, and Loïc Ferreira. Symmetric-key authenticated key exchange (sake) with perfect forward secrecy. In *Cryptographers' Track at the RSA Conference*, pages 199–224. Springer, 2020.

[ADM+14] Romain Alléaume, Ivo P Degiovanni, Alan Mink, Thomas E Chapuran, Norbert Lutkenhaus, Momtchil Peev, Christopher J Chunnilall, Vincente Martin, Marco Lucamarini, Martin Ward, et al. Worldwide standardization activity for quantum key distribution. In *2014 IEEE Globecom Workshops*, pages 656–661. IEEE, 2014.

[AKBH07] Irfan Ali-Khan, Curtis J Broadbent, and John C Howell. Large-alphabet quantum key distribution using energy-time entangled bipartite states. *Physical review letters*, 98(6):060503, 2007.

[All15a] Romain Alléaume. Hybrid classical quantum cryptography, January 2015. European Patent 3043508.

[All15b] 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.

[All15c] Romain Alléaume. Practical quantum cryptography with everlasting security, October 2015. European Patent 3043507.

[All16] Romain Alléaume. Communication with everlasting security from short-term-secure encrypted quantum communication, October 2016. International Patent WO2016110582A1.

[All17] Romain Alléaume. Can we accelerate quantum cryptography commercial take-off? In *Central European Workshop on Quantum Optics*, 2017.

[All19a] Romain Alléaume. Développement industriel de la cryptographie quantique: Défis et opportunités. In *French Photonic Days, Bordeaux:" La photonique, nouvelle ère du quantique"*, 2019.

[All19b] Romain Alléaume. Quantum key distribution (qkd); device and communication channel parameters for qkd deployment - group specification qkd 012. 2019.

[AM16] Romain Alléaume and Adrien Marie. Phase reference sharing schemes for continuous-variable quantum cryptography, May 2016. European Patent EP3244566.

[ANNVLF15] Ulrik L Andersen, Jonas S Neergaard-Nielsen, Peter Van Loock, and Akira Furusawa. Hybrid discrete-and continuous-variable quantum information. *Nature Physics*, 11(9):713–719, 2015.

[ANS20] ANSSI. Should quantum key distribution be used for secure communications?, 2020.

[ARDL09] Romain Alleaume, François Roueff, Eleni Diamanti, and N Lütkenhaus. Topological optimization of quantum key distribution networks. *New Journal of Physics*, 11(7):075002, 2009.

[ARML06] Romain Alléaume, François Roueff, Oliver Maurhart, and N Lutkenhaus. Architecture, security and topology of a global quantum key distribution network. In *2006 Digest of the LEOS Summer Topical Meetings*, pages 38–39. IEEE, 2006.

[ARS+04] Romain Alléaume, Jean-François Roch, Darius Subacius, Anton Zavriyev, and Alexei Trifonov. Fiber-optics quantum cryptography with single photons. In *AIP Conference Proceedings*, volume 734, pages 287–290. American Institute of Physics, 2004.

[ARW+07] Romain Alléaume, M Riguidel, H Weinfurter, N Gisin, P Grangier, M Dianati, Mark Godfrey, G Ribordy, J Rarity, M Peev, et al. Secoqc white paper on quantum key distribution and cryptography. Technical report, 2007.

[ATCR04] Romain Alléaume, Francois Treussart, Jean-Michel Courty, and Jean-Francois Roch. Photon statistics characterization of a single-photon source. *New Journal of physics*, 6(1):85, 2004.

[ATM+04] R Alléaume, F Treussart, G Messin, Y Dumeige, J-F Roch, A Beveratos, R Brouri-Tualle, J-P Poizat, and P Grangier. Experimental open-air quantum key distribution with a single-photon source. *New Journal of physics*, 6(1):92, 2004.

[ATSVY00] Dorit Aharonov, Amnon Ta-Shma, Umesh V Vazirani, and Andrew C Yao. Quantum bit escrow. In *Proceedings of the thirty-second annual ACM symposium on Theory of computing*, pages 705–714, 2000.

[BAL11] Aurélien Bocquet, Romain Alléaume, and Anthony Leverrier. Optimal eavesdropping on quantum key distribution without quantum memory. *Journal of Physics A: Mathematical and Theoretical*, 45(2):025305, 2011.

[BB84] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings IEEE International Conference on Computers, Systems and Signal Proceedings*, number 0, pages 175–179, 1984.

[BB14] Charles H Bennett and Gilles Brassard. Quantum cryptography: public key distribution and coin tossing. *Theor. Comput. Sci.*, 560(12):7–11, 2014.

[BBB+06] Eli Biham, Michel Boyer, P Oscar Boykin, Tal Mor, and Vwani Roychowdhury. A proof of the security of quantum key distribution. *Journal of cryptology*, 19(4):381–439, 2006.

[BBCM95] Charles H Bennett, Gilles Brassard, Claude Crépeau, and Ueli M Maurer. Generalized privacy amplification. *IEEE Transactions on Information Theory*, 41(6):1915–1923, 1995.

[BBD+17] Johannes Braun, Johannes Buchmann, Denise Demirel, Matthias Geihs, Mikio Fujiwara, Shiho Moriai, Masahide Sasaki, and Atsushi Waseda. Lincos: A storage system providing long-term integrity, authenticity, and confidentiality. In *Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security*, pages 461–468, 2017.

[BBR+18] Alberto Boaron, Gianluca Boso, Davide Rusca, Cédric Vulliez, Claire Autebert, Misael Caloz, Matthieu Perrenoud, Gaëtan Gras, Félix Bussières, Ming-Jun Li, et al. Secure quantum key distribution over 421 km of optical fiber. *Physical review letters*, 121(19):190502, 2018.

[Bea96] Donald Beaver. Correlated pseudorandomness and the complexity of private computations. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 479–488, 1996.

[Ber09] Daniel J Bernstein. Introduction to post-quantum cryptography. In *Post-quantum cryptography*, pages 1–14. Springer, 2009.

[Ber18] Daniel J Bernstein. Is the security of quantum cryptography guaranteed by the laws of physics? *arXiv preprint arXiv:1803.04520*, 2018.

[BFK09] Anne Broadbent, Joseph Fitzsimons, and Elham Kashefi. Universal blind quantum computation. In *2009 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 517–526. IEEE, 2009.

[BFW13] Mario Berta, Omar Fawzi, and Stephanie Wehner. Quantum to classical randomness extractors. *IEEE Transactions on Information Theory*, 60(2):1168–1192, 2013.

[BG20] Colin Boyd and Kai Gellert. A modern view on forward security. *The Computer Journal*, 2020.

[Blu83] Manuel Blum. Coin flipping by telephone a protocol for solving impossible problems. *ACM SIGACT News*, 15(1):23–27, 1983.

[BNPS19] Xavier Bonnetain, María Naya-Plasencia, and André Schrottenloher. Quantum security analysis of aes. *IACR Transactions on Symmetric Cryptology*, 2019(2):55–93, 2019.

[BOHL+05a] Michael Ben-Or, Michał Horodecki, Debbie W Leung, Dominic Mayers, and Jonathan Oppenheim. The universal composable security of quantum key distribution. In *Theory of Cryptography Conference*, pages 386–406. Springer, 2005.

[BOHL+05b] Michael Ben-Or, MichaÇ Horodecki, DebbieW. Leung, Dominic Mayers, and Jonathan Oppenheim. The universal composable security of quantum key distribution. In Joe Kilian, editor, *Lecture Notes in Computer Science*, volume 3378, pages 386–406–. Springer Berlin Heidelberg, 2005.

[Bra16] Gilles Brassard. Cryptography in a quantum world. In *International Conference on Current Trends in Theory and Practice of Informatics*, pages 3–16. Springer, 2016.

[BRS07] Stephen D. Bartlett, Terry Rudolph, and Robert W. Spekkens. Reference frames, superselection rules, and quantum information. *Rev. Mod. Phys.*, 79:555–609, 2007.

[BS16] Anne Broadbent and Christian Schaffner. Quantum cryptography beyond quantum key distribution. *Designs, Codes and Cryptography*, 78(1):351–382, 2016.

[BZ13] Dan Boneh and Mark Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In *Annual Cryptology Conference*, pages 361–379. Springer, 2013.

[CBKG02] 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.

[CCD+15] Matthew Campagna, Lidong Chen, Özgür Dagdelen, Jintai Ding, Jennifer K. Fernick, Nicolas Gisin, Donald Hayford, Thomas Jennewein, Norbert Lütkenhaus, Michele Mosca, Brian Neill, Mark Pecen, Ray Perlner, Grégoire Ribordy, John M. Schanck, Douglas Stebila, Nino Walenta, William Whyte, and Zhenfei Zhang. Quantum safe cryptography and security: An introduction, benefits, enablers and challengers. Technical report, ETSI (European Telecommunications Standards Institute), June 2015.

[CEM17] Common Methodology for Information Technology Security Evaluation, Version 3.1, Revision 5, 2017.

[CGCG16] Katriel Cohn-Gordon, Cas Cremers, and Luke Garratt. On post-compromise security. In *2016 IEEE 29th Computer Security Foundations Symposium (CSF)*, pages 164–178. IEEE, 2016.

[CK78] Imre Csiszár and Janos Korner. Broadcast channels with confidential messages. *IEEE transactions on information theory*, 24(3):339–348, 1978.

[CK09] André Chailloux and Iordanis Kerenidis. Optimal quantum strong coin flipping. In *2009 50th Annual IEEE Symposium on Foundations of Computer Science*, pages 527–533. IEEE, 2009.

[CK11] Roger Colbeck and Adrian Kent. Private randomness expansion with untrusted devices. *Journal of Physics A: Mathematical and Theoretical*, 44(9):095305, 2011.

[CM97] Christian Cachin and Ueli Maurer. Unconditional security against memory-bounded adversaries. In *Annual International Cryptology Conference*, pages 292–306. Springer, 1997.

[Cré87] Claude Crépeau. Equivalence between two flavours of oblivious transfers. In *Conference on the Theory and Application of Cryptographic Techniques*, pages 350–354. Springer, 1987.

[Cry] IACR Conference Crypto. https://crypto.iacr.org/2021/.

[CTP+09] TE Chapuran, P Toliver, NA Peters, J Jackel, MS Goodman, RJ Runser, SR McNown, N Dallmann, RJ Hughes, KP McCabe, et al. Optical networking for quantum key distribution and quantum communications. *New Journal of Physics*, 11(10):105001, 2009.

[CW79] J Lawrence Carter and Mark N Wegman. Universal classes of hash functions. *Journal of computer and system sciences*, 18(2):143–154, 1979.

[CZC+21] Yu-Ao Chen, Qiang Zhang, Teng-Yun Chen, Wen-Qi Cai, Sheng-Kai Liao, Jun Zhang, Kai Chen, Juan Yin, Ji-Gang Ren, Zhu Chen, et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*, pages 1–6, 2021.

[DA07] Mehrdad Dianati and Romain Alléaume. Architecture of the secoqc quantum key distribution network. In *2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM'07)*, pages 13–13. IEEE, 2007.

[DAG+11a] Y Dumeige, R Alléaume, P Grangier, F Treussart, and J-F Roch. Controling the single-diamond nitrogen-vacancy color center photoluminescence spectrum with a fabry–perot microcavity. *New Journal of Physics*, 13(2):025015, 2011.

[DAG+11b] Yannick Dumeige, Romain Alléaume, Philippe Grangier, François Treussart, and Jean-François Roch. Coupling of a single nitrogen vacancy colour centre in diamond, to a planar microcavity. In *2011 13th International Conference on Transparent Optical Networks*, pages 1–4, 2011.

[DAGS08] Mehrdad Dianati, Romain Alléaume, Maurice Gagnaire, and Xuemin Shen. Architecture and protocols of the future european quantum key distribution network. *Security and Communication Networks*, 1(1):57–74, 2008.

[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.

[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.

[DH76] Whitfield Diffie and Martin Hellman. New directions in cryptography. *IEEE transactions on Information Theory*, 22(6):644–654, 1976.

[DHP20] Benjamin Dowling, Torben Brandt Hansen, and Kenneth G Paterson. Many a mickle makes a muckle: A framework for provably quantum-secure hybrid key exchange. In *International Conference on Post-Quantum Cryptography*, pages 483–502. Springer, 2020.

[DL15] Eleni Diamanti and Anthony Leverrier. Distributing secret keys with quantum continuous variables: Principle, security and implementations. *Entropy*, 17(9):6072, 2015.

[DLL03] Fu-Guo Deng, Gui Lu Long, and Xiao-Shu Liu. Two-step quantum direct communication protocol using the einstein-podolsky-rosen pair block. *Physical Review A*, 68(4):042317, 2003.

[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.

[DSW+20] Hui Dai, Qi Shen, Chao-Ze Wang, Shuang-Lin Li, Wei-Yue Liu, Wen-Qi Cai, Sheng-Kai Liao, Ji-Gang Ren, Juan Yin, Yu-Ao Chen, et al. Towards satellite-based quantum-secure time transfer. *Nature Physics*, 16(8):848–852, 2020.

[DTA+04] Y Dumeige, F Treussart, R Alléaume, T Gacoin, J-F Roch, and P Grangier. Photo-induced creation of nitrogen-related color centers in diamond nanocrystals under femtosecond illumination. *Journal of luminescence*, 109(2):61–67, 2004.

[EC19] EC. https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network, 2019.

[EHP+19] Tobias A Eriksson, Takuya Hirano, Benjamin J Puttnam, Georg Rademacher, Ruben S Luís, Mikio Fujiwara, Ryo Namiki, Yoshinari Awaji, Masahiro Takeoka, Naoya Wada, et al. Wavelength division multiplexing of continuous variable quantum key distribution and 18.3 tbit/s data channels. *Communications Physics*, 2(1):1–8, 2019.

[ELAB09] David Elkouss, Anthony Leverrier, Romain Alléaume, and Joseph J Boutros. Efficient reconciliation protocol for discrete-variable quantum key distribution. In *2009 IEEE International Symposium on Information Theory*, pages 1879–1883. IEEE, 2009.

[ETS21] ETSI QKD-ISG DGS/QKD-016-PP, QKD Common Criteria Protection Profile for QKD., 2021.

[EWL+10] Patrick Eraerds, Nino Walenta, Matthieu Legré, Nicolas Gisin, and Hugo Zbinden. Quantum key distribution and 1 gbps data encryption over a single fibre. *New Journal of Physics*, 12(6):063027, 2010.

[Exc20] Quantum-Secure Hybrid Key Exchange. Many a mickle makes a muckle: A framework for provably quantum-secure hybrid key exchange. In *Post-Quantum Cryptography: 11th International Conference, PQCrypto 2020, Paris, France, April 15–17, 2020, Proceedings*, volume 12100, page 483. Springer Nature, 2020.

[FDD+09] S Fossier, E Diamanti, T Debuisschert, A Villing, R Tualle-Brouri, and P Grangier. Field test of a continuous-variable quantum key distribution prototype. *New J. Phys.*, 11(4):045023, 2009.

[FGG07] A. Ferenczi, P. Grangier, and F. Grosshans. Calibration attack and defense in continuous variable quantum key distribution. In *Lasers and Electro-Optics, 2007 and the International Quantum Electronics Conference. CLEOE-IQEC 2007. European Conference on*, pages 1–1, June 2007.

[Fit17] Joseph F Fitzsimons. Private quantum computation: an introduction to blind quantum computing and related protocols. *npj Quantum Information*, 3(1):1–11, 2017.

[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, 2017.

[GG02] Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Phys. Rev. Lett.*, 88:057902, 2002.

[GGDL19] Shouvik Ghorai, Philippe Grangier, Eleni Diamanti, and Anthony Leverrier. Asymptotic security of continuous-variable quantum key distribution with a discrete modulation. *Physical Review X*, 9(2):021059, 2019.

[GHK+14] 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.

[GLLL+11] Ilja Gerhardt, Qin Liu, Antia Lamas-Linares, Johannes Skaar, Christian Kurtsiefer, and Vadim Makarov. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nature communications*, 2(1):1–6, 2011.

[GMR+13] Marissa Giustina, Alexandra Mech, Sven Ramelow, Bernhard Wittmann, Johannes Kofler, Jörn Beyer, Adriana Lita, Brice Calkins, Thomas Gerrits, Sae Woo Nam, et al. Bell violation using entangled photons without the fair-sampling assumption. *Nature*, 497(7448):227–230, 2013.

[Gol09] Oded Goldreich. *Foundations of cryptography: volume 2, basic applications*. Cambridge university press, 2009.

[GRTZ02a] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of modern physics*, 74(1):145, 2002.

[GRTZ02b] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, Mar 2002.

[GVAW+03] Frederic Grosshans, Gilles Van Assche, Jerome Wenger, Rosa Brouri, Nicolas J. Cerf, and Philippe Grangier. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 421(6920):238–241, January 2003.

[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.

[HCea17] Miguel Herrero-Collantes et al. Quantum random number generators. *Reviews of Modern Physics*, 89(1):015004, 2017.

[HFW+13] D Huang, J Fang, D Wang, P Huang, and G Zeng. A wideband balanced homodyne detector for high speed continuous-variable quantum key distribution systems. In *QCrypt*, 2013.

[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.

[HKJJ+14] Jing-Zheng Huang, Sébastien Kunz-Jacques, Paul Jouguet, Christian Weedbrook, Zhen-Qiang Yin, Shuang Wang, Wei Chen, Guang-Can Guo, and Zheng-Fu Han. Quantum hacking on Quantum Key Distribution using Homodyne Detection. *Phys. Rev. A*, 89:032304, Mar 2014.

[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*, 23:17511–17519, 2015.

[HQI21] Harvard Quantum Initiative HQI. Development of quantum interconnects (quics) for next-generation information technologies. *P R X Quantum*, 2:017002, 2021.

[HWY+13a] Jing-Zheng Huang, Christian Weedbrook, Zhen-Qiang Yin, Shuang Wang, Hong-Wei Li, Wei Chen, Guang-Can Guo, and Zheng-Fu Han. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Phys. Rev. A*, 87:062329, Jun 2013.

[HWY+13b] Jing-Zheng Huang, Christian Weedbrook, Zhen-Qiang Yin, Shuang Wang, Hong-Wei Li, Wei Chen, Guang-Can Guo, and Zheng-Fu Han. Quantum hacking of a continuous-variable quantum-key-distribution system using a wavelength attack. *Phys. Rev. A*, 87:062329, Jun 2013.

[IDQ21] IDQ. http://www.idquantique.com, 2021.

[ISO20] ISO/IEC JTC1 SC27 WG3, Security requirements, test and evaluation methods for quantum key distribution., 2020.

[JKJD+12] Paul Jouguet, Sébastien Kunz-Jacques, Thierry Debuisschert, Simon Fossier, Eleni Diamanti, Romain Alléaume, Rosa Tualle-Brouri, Philippe Grangier, Anthony Leverrier, Philippe Pache, et al. Field test of classical symmetric encryption with continuous variables quantum key distribution. *Optics Express*, 20(13):14030–14041, 2012.

[JKJD13] Paul Jouguet, Sébastien Kunz-Jacques, and Eleni Diamanti. Preventing calibration attacks on the local oscillator in continuous-variable quantum key distribution. *Phys. Rev. A*, 87:062313, Jun 2013.

[JKJL+13a] Paul Jouguet, Sebastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, and Eleni Diamanti. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nat Photon*, 7(5):378–381, 2013.

[JKJL+13b] Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, and Eleni Diamanti. Experimental study on the gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. *Nature Photonics*, 7:378,Äì381, 2013.

[Ken12] Adrian Kent. Quantum tasks in minkowski space. *Classical and Quantum Gravity*, 29(22):224013, 2012.

[KJJ15] Sébastien Kunz-Jacques and Paul Jouguet. Robust shot-noise measurement for continuous-variable quantum key distribution. *Physical Review A*, 91(2):022307, 2015.

[KL14] Jonathan Katz and Yehuda Lindell. *Introduction to modern cryptography*. CRC press, 2014.

[KL21] Wen Yu Kon and Charles Ci Wen Lim. Provably secure symmetric private information retrieval with quantum cryptography. *Entropy*, 23(1):54, 2021.

[KMQA21] Rupesh Kumar, Francesco Mazzoncini, Hao Qin, and Romain Alléaume. Experimental vulnerability analysis of qkd based on attack ratings. *Scientific Reports*, 22:9564, 2021.

[KQA15] Rupesh Kumar, Hao Qin, and Romain Alléaume. Coexistence of continuous variable qkd with intense dwdm classical channels. *New Journal of Physics*, 17(4):043027, 2015.

[Kra10] Hugo Krawczyk. Cryptographic extraction and key derivation: The hkdf scheme. In *Annual Cryptology Conference*, pages 631–648. Springer, 2010.

[KRBM07] Robert König, Renato Renner, Andor Bariska, and Ueli Maurer. Small accessible quantum information does not imply security. *Physical Review Letters*, 98(14):140502, 2007.

[KSDS19] Sebastian Kleis, Joachim Steinmayer, Rainer H Derksen, and Christian G Schaeffer. Experimental investigation of heterodyne quantum key distribution in the s-band or l-band embedded in a commercial c-band dwdm system. *Optics express*, 27(12):16540–16549, 2019.

[KTHW13] Jędrzej Kaniewski, Marco Tomamichel, Esther Hänggi, and Stephanie Wehner. Secure bit commitment from relativistic constraints. *IEEE Transactions on Information Theory*, 59(7):4687–4699, 2013.

[KWW12] Robert Konig, Stephanie Wehner, and Jürg Wullschleger. Unconditional security from noisy quantum storage. *IEEE Transactions on Information Theory*, 58(3):1962–1984, 2012.

[LAB+08] Anthony Leverrier, Romain Alléaume, Joseph Boutros, Gilles Zémor, and Philippe Grangier. Multidimensional reconciliation for a continuous-variable quantum key distribution. *Physical Review A*, 77(4):042325, 2008.

[Lan14] Susan Landau. Highlights from making sense of snowden, part ii: What's significant in the nsa revelations. *IEEE Security & Privacy*, 12(1):62–64, 2014.

[LBGP+07] Jérôme Lodewyck, Matthieu Bloch, Raúl García-Patrón, Simon Fossier, Evgueni Karpov, Eleni Diamanti, Thierry Debuisschert, Nicolas J Cerf, Rosa Tualle-Brouri, Steven W McLaughlin, et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Physical Review A*, 76(4):042305, 2007.

[LC97] Hoi-Kwong Lo and Hoi Fung Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78(17):3410, 1997.

[LC98] Hoi-Kwong Lo and Hoi Fung Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D: Nonlinear Phenomena*, 120(1-2):177–187, 1998.

[LCQ12] Hoi-Kwong Lo, Marcos Curty, and Bing Qi. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.*, 108:130503, Mar 2012.

[LCT14] Hoi-Kwong Lo, Marcos Curty, and Kiyoshi Tamaki. Secure quantum key distribution. *Nature Photonics*, 8(8):595–604, 2014.

[LDGP+07] Jérôme Lodewyck, Thierry Debuisschert, Raúl García-Patrón, Rosa Tualle-Brouri, Nicolas J. Cerf, and Philippe Grangier. Experimental implementation of non-gaussian attacks on a continuous-variable quantum-key-distribution system. *Phys. Rev. Lett.*, 98:030503, Jan 2007.

[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.

[LL11] Hoi-Kwan Lau and Hoi-Kwong Lo. Insecurity of position-based quantum-cryptography protocols against entanglement attacks. *Physical review a*, 83(1):012322, 2011.

[LL15] Cosmo Lupo and Seth Lloyd. Quantum data locking for high-rate private communication. *New Journal of Physics*, 17(3):033022, 2015.

[LMC05] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Physical review letters*, 94(23):230504, 2005.

[Lo97] Hoi-Kwong Lo. Insecurity of quantum secure computations. *Physical Review A*, 56(2):1154, 1997.

[LSA+18] Marco Lucamarini, Andrew Shields, 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, and Zhiliang Yuan. Implementation security of quantum cryptography. *ETSI Group Specification Document*, 2018.

[LT19] AM Lewis and M Travagnin. A secure quantum communications infrastructure for europe. *JRC Technical Papers, JRC116937*, 2019.

[LUL19] Jie Lin, Twesh Upadhyaya, and Norbert Lütkenhaus. Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution. *Physical Review X*, 9(4):041064, 2019.

[LWW+10] Lars Lydersen, Carlos Wiechers, Christoffer Wittmann, Dominique Elser, Johannes Skaar, and Vadim Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat Photon*, 4(10):686–689, October 2010.

[LZL+20] Yang Li, Xiaofang Zhang, Yong Li, Bingjie Xu, Li Ma, Jie Yang, and Wei Huang. High-throughput gpu layered decoder of quasi-cyclic multi-edge type low density parity check codes in continuous-variable quantum key distribution systems. *Scientific Reports*, 10(1):1–11, 2020.

[MA17] Adrien Marie and Romain Alléaume. Self-coherent phase reference sharing for continuous-variable quantum key distribution. *Physical Review A*, 95(1):012316, 2017.

[MA20] Francesco Mazzoncini and Romain Alléaume. State of the art analysis in qci security. *QOSAC study report*, 4.1, 2020.

[MACdA06] Rex AC Medeiros, Romain Alléaume, Gérard Cohen, and Francisco M de Assis. Zero-error capacity of quantum channels and noiseless subsystems. In *2006 International Telecommunications Symposium*, pages 900–905. IEEE, 2006.

[Mak09] Vadim Makarov. Controlling passively quenched single photon detectors by bright light. *New J. Phys.*, 11(6):065003–, 2009.

[MAMD02] RA Michniak, R Alleaume, DN McKinsey, and JM Doyle. Alpha and beta particle induced scintillations in liquid and solid neon. *Nuclear Instruments and Methods in Physics Research Section A: Accelerators, Spectrometers, Detectors and Associated Equipment*, 482(1-2):387–394, 2002.

[Mau93] Ueli M Maurer. Secret key agreement by public discussion from common information. *IEEE transactions on information theory*, 39(3):733–742, 1993.

[May97] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical review letters*, 78(17):3414, 1997.

[May01] Dominic Mayers. Unconditional security in quantum cryptography. *Journal of the ACM (JACM)*, 48(3):351–406, 2001.

[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.

[MGA+20] Philipp Muth, Matthias Geihs, Tolga Arul, Johannes Buchmann, and Stefan Katzenbeisser. Elsa: efficient long-term secure storage of large datasets (full version)? *EURASIP Journal on Information Security*, 2020:1–20, 2020.

[MM09] A Theodore Markettos and Simon W Moore. The frequency injection attack on ring-oscillator-based true random number generators. In *International Workshop on Cryptographic Hardware and Embedded Systems*, pages 317–331. Springer, 2009.

[MMLO+15] Mohammad Mirhosseini, Omar S Magaña-Loaiza, Malcolm N O?Sullivan, Brandon Rodenburg, Mehul Malik, Martin PJ 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, 2015.

[MMMP99] Vicente Martin, Jesus Martinez-Mateo, and Momtchil Peev. Introduction to quantum key distribution. *Wiley Encyclopedia of Electrical and Electronics Engineering*, pages 1–17, 1999.

[MNR+20] Miralem Mehic, Marcin Niemiec, Stefan Rass, Jiajun Ma, Momtchil Peev, Alejandro Aguado, Vicente Martin, Stefan Schauer, Andreas Poppe, Christoph Pacher, et al. Quantum key distribution: a networking perspective. *ACM Computing Surveys (CSUR)*, 53(5):1–41, 2020.

[Moc07] Carlos Mochon. Quantum weak coin flipping with arbitrarily small bias. *arXiv preprint arXiv:0711.4114*, 2007.

[MPZ20] Ueli Maurer, Christopher Portmann, and Jiamin Zhu. Unifying generic group models. *Cryptology ePrint Archive*, 2020.

[MSJ+14] Xiang-Chun Ma, Shi-Hai Sun, Mu-Sheng Jiang, Ming Gui, Yan-Li Zhou, and Lin-Mei Liang. Enhancement of the security of a practical continuous-variable quantum-key-distribution system by manipulating the intensity of the local oscillator. *Phys. Rev. A*, 89:032310, Mar 2014.

[MSJL13] Xiang-Chun Ma, Shi-Hai Sun, Mu-Sheng Jiang, and Lin-Mei Liang. Wavelength attack on practical continuous-variable quantum-key-distribution system with a heterodyne protocol. *Phys. Rev. A*, 87:052309, May 2013.

[MWZ+18] Yingqiu Mao, Bi-Xiao Wang, Chunxu Zhao, Guangquan Wang, Ruichun Wang, Honghai Wang, Fei Zhou, Jimin Nie, Qing Chen, Yong Zhao, et al. Integrating quantum key distribution with classical communications in backbone fiber network. *Optics express*, 26(5):6010–6020, 2018.

[NCS20] NCSC. Quantum security technologies, 2020.

[NSA20] NSA. Quantum key distribution (qkd) and quantum cryptography (qc), 2020.

[NWS+13] J Nunn, LJ Wright, C Söller, L Zhang, IA Walmsley, and BJ Smith. Large-alphabet time-frequency entangled quantum key distribution by means of time-to-frequency conversion. *Optics express*, 21(13):15959–15973, 2013.

[PAB+20] Stefano Pirandola, Ulrik L Andersen, Leonardo Banchi, Mario Berta, Darius Bunandar, Roger Colbeck, Dirk Englund, Tobias Gehring, Cosmo Lupo, Carlo Ottaviani, et al. Advances in quantum cryptography. *Advances in Optics and Photonics*, 12(4):1012–1236, 2020.

[PAL+07] M Peev, Romain Alléaume, T Langer, Lutkenhaus N, Maurhart O., and Salvail L. The secoqc quantum key distribution network prototype: Principles, design and implementation. In *Globecom*. IEEE, 2007.

[PAM+10] Stefano Pironio, Antonio Acín, Serge Massar, A Boyer de La Giroday, Dzmitry N Matsukevich, Peter Maunz, Steven Olmschenk, David Hayes, Le Luo, T Andrew Manning, et al. Random numbers certified by bell's theorem. *Nature*, 464(7291):1021–1024, 2010.

[PDC+12] KA Patel, JF Dynes, I Choi, AW Sharpe, AR Dixon, ZL Yuan, RV Penty, and AJ Shields. Coexistence of high-bit-rate quantum key distribution and data on optical fiber. *Physical Review X*, 2(4):041010, 2012.

[PDL+14] KA Patel, JF Dynes, M Lucamarini, I Choi, AW Sharpe, ZL Yuan, RV Penty, and AJ Shields. Quantum key distribution for 10 gb/s dense wavelength division multiplexing networks. *Applied Physics Letters*, 104(5):051123, 2014.

[Per95] Michael Perelman. Retrospectives: Schumpeter, david wells, and creative destruction. *Journal of Economic Perspectives*, 9(3):189–197, 1995.

[Pet13] Carlo Petrini. *Slow food nation: Why our food should be good, clean, and fair*. Rizzoli Publications, 2013.

[PGea18] Damián Pitalúa-García et al. Practical and unconditionally secure spacetime-constrained oblivious transfer. *Physical Review A*, 98(3):032327, 2018.

[PLOB17] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. Fundamental limits of repeaterless quantum communications. *Nature communications*, 8(1):1–15, 2017.

[PMLA13] Stefano Pironio, Ll Masanes, Anthony Leverrier, and Antonio Acín. Security of device-independent quantum key distribution in the bounded-quantum-storage model. *Physical Review X*, 3(3):031007, 2013.

[PPA+09] Momtchil Peev, Christoph Pacher, Romain Alléaume, Claudio Barreiro, Jan Bouda, W Boxleitner, Thierry Debuisschert, Eleni Diamanti, M Dianati, JF Dynes, et al. The secoqc quantum key distribution network in vienna. *New Journal of Physics*, 11(7):075001, 2009.

[PPS07] Kenneth G Paterson, Fred Piper, and Rüdiger Schack. Quantum cryptography: a practical information security perspective. *Nato Security Through Science Series D-Information and Communication Security*, 11:175, 2007.

[PTC+09] NA Peters, P Toliver, TE Chapuran, RJ Runser, SR McNown, CG Peterson, D Rosenberg, N Dallmann, RJ Hughes, KP McCabe, et al. Dense wavelength multiplexing of 1550 nm qkd with strong classical channels in reconfigurable networking environments. *New Journal of physics*, 11(4):045012, 2009.

[QC421] QC40. https://qiskit.org/events/physics-of-computation/, 2021.

[QFLM07] Bing Qi, Chi-Hang Fred Fung, Hoi-Kwong Lo, and Xiongfeng Ma. Time-shift attack in practical quantum cryptosystems. *Quantum Info. Comput.*, 7(1):73–82, 2007.

[QHQL07] Bing Qi, Lei-Lei Huang, Li Qian, and Hoi-Kwong Lo. Experimental study on the gaussian-modulated coherent-state quantum key distribution over standard telecommunication fibers. *Phys. Rev. A*, 76:052323, Nov 2007.

[Qi16] Bing Qi. Simultaneous classical communication and quantum key distribution using continuous variables. *Physical Review A*, 94(4):042340, 2016.

[QKA13a] Hao Qin, Rupesh Kumar, and Romain Alléaume. Saturation attack on continuous-variable quantum key distribution system. In *Emerging Technologies in Security and Defence; and Quantum Security II; and Unmanned Sensor Systems X*, volume 8899, page 88990N. International Society for Optics and Photonics, 2013.

[QKA13b] Hao Qin, Rupesh Kumar, and Romain Alléaume. Saturation Attack On Continuous-Variable Quantum Key Distribution System. In *Proc. SPIE 8899, Emerging Technologies in Security and Defence; and Quantum Security II; and Unmanned Sensor Systems X, 88990N*, volume 8899, pages 88990N–88990N–7, 2013.

[QKA16] Hao Qin, Rupesh Kumar, and Romain Alléaume. Quantum hacking: Saturation attack on practical continuous-variable quantum key distribution. *Physical Review A*, 94(1):012325, 2016.

[QKMA18] Hao Qin, Rupesh Kumar, Vadim Makarov, and Romain Alléaume. Homodyne-detector-blinding attack in continuous-variable quantum key distribution. *Physical Review A*, 98(1):012312, 2018.

[QL18] Bing Qi and Charles Ci Wen Lim. Noise analysis of simultaneous quantum key distribution and classical communication scheme using a true local oscillator. *Physical Review Applied*, 9(5):054008, 2018.

[QLP+15] Bing Qi, Pavel Lougovski, Raphael Pooser, Warren Grice, and Miljko Bobrek. Generating the local oscillator locally in continuous-variable quantum key distribution based on coherent detection. *Phys. Rev. X*, 5:041009, Oct 2015.

[QRa] QRange. Qt flagship project 2018-2022.

[Rab05] Michael O Rabin. How to exchange secrets with oblivious transfer. *IACR Cryptol. ePrint Arch.*, 2005(187), 2005.

[Ren05] R Renner. Security of quantum key distribution (phd thesis). *arXiv preprint quant-ph/0512258*, 2005.

[Ren08] Renato Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6(01):1–127, 2008.

[RK05] Renato Renner and Robert König. Universally composable privacy amplification against quantum adversaries. In *Theory of Cryptography Conference*, pages 407–425. Springer, 2005.

[RR20] Joseph M Renes and Renato Renner. Are quantum cryptographic security claims vacuous? *arXiv preprint arXiv:2010.11961*, 2020.

[RRL+21] Ravi Raghunathan, Guillaume Ricard, Baptiste Lefaucher, Antoine Henry, Filippo Miatto, Isabelle Zaquine, and Romain Alléaume. Parallelizable synthesis of arbitrary single-qubit gates with linear optics and time-frequency encoding. *In Preparation*, 2021.

[RRM+18] Ravi Raghunathan, G Ricard, Filippo Miatto, Isabelle Zaquine, and Romain Alléaume. Single qubit arbitrary unitary synthesis using photonic spectral encoding. In *Quantum Technology International Conference (QTech 2018)*, 2018.

[RWC] RWC. https://rwc.iacr.org/.

[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.

[SAL22] Shihan Sajeed, Romain Alléaume, and Hoi-Kwong Lo. A direct look at quantum secure communication. *In Preparation*, 2022.

[Sas18] Masahide Sasaki. Quantum key distribution and its applications. *IEEE Security & Privacy*, 16(5):42–48, 2018.

[SBC+15] Daniel B. S. Soh, Constantin Brif, Patrick J. Coles, Norbert Lütkenhaus, Ryan M. Camacho, Junji Urayama, and Mohan Sarovar. Self-referenced continuous-variable quantum key distribution protocol. *Phys. Rev. X*, 5:041010, Oct 2015.

[SBF+17] Alicia Sit, Frédéric Bouchard, Robert Fickler, Jérémie Gagnon-Bischoff, Hugo Larocque, Khabat Heshami, Dominique Elser, Christian Peuntinger, Kevin Günthner, Bettina Heim, et al. High-dimensional intracity quantum cryptography with structured photons. *Optica*, 4(9):1006–1010, 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. *Reviews of modern physics*, 81(3):1301, 2009.

[SBV+20] Pavel Sekatski, J-D Bancal, Xavier Valcarce, EY-Z Tan, Renato Renner, and Nicolas Sangouard. Device-independent quantum key distribution from generalized chsh inequalities. *arXiv preprint arXiv:2009.01784*, 2020.

[SC14] Valerio Scarani and Kurtsiefer Christian. The black paper of quantum cryptography: real implementation. *Theoretical Computer Science*, 560:27–32, 2014.

[SCB+15] Shihan Sajeed, Poompong Chaiwongkhot, Jean-Philippe Bourgoin, Thomas Jennewein, Norbert Lütkenhaus, and Vadim Makarov. Security loophole in free-space quantum key distribution due to spatial-mode detector-efficiency mismatch. *Phys. Rev. A*, 91:062301, Jun 2015.

[Sch10] Christian Schaffner. Simple protocols for oblivious transfer and secure identification in the noisy-quantum-storage model. *Physical Review A*, 82(3):032308, 2010.

[Sch18] Bruce Schneier. Cryptography after the aliens land. *IEEE Security & Privacy*, 16(5):86–88, 2018.

[Seq] SequreNet. Spin-off from telecom paris, 2008-2017.

[SFI+11] Masahide Sasaki, Mikio Fujiwara, H Ishizuka, W Klaus, K Wakui, M Takeoka, S Miki, T Yamashita, Z Wang, A Tanaka, et al. Field test of quantum key distribution in the tokyo qkd network. *Optics express*, 19(11):10387–10409, 2011.

[SGG+11] Jean-Loup Smirr, Sylvain Guilbaud, Joe Ghalbouni, Robert Frey, Eleni Diamanti, Romain Alléaume, and Isabelle Zaquine. Simple performance evaluation of pulsed spontaneous parametric down-conversion sources for quantum communications. *Optics express*, 19(2):616–627, 2011.

[Sho94] Peter W Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science*, pages 124–134. Ieee, 1994.

[Sho97] Victor Shoup. Lower bounds for discrete logarithms and related problems. In *International Conference on the Theory and Applications of Cryptographic Techniques*, pages 256–266. Springer, 1997.

[slo] Slow food movement.

[SML09] Douglas Stebila, Michele Mosca, and Norbert Lütkenhaus. The case for quantum key distribution. In *International Conference on Quantum Comunication and Quantum Networking*, pages 283–296. Springer, 2009.

[SP00] Peter W Shor and John Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Physical review letters*, 85(2):441, 2000.

[SPD+10] Louis Salvail, Momtchil Peev, Eleni Diamanti, Romain Alléaume, Norbert Lütkenhaus, and Thomas Länger. Security of trusted repeater quantum key distribution networks. *Journal of Computer Security*, 18(1):61–87, 2010.

[Sti94] Douglas R. Stinson. Universal hashing and authentication codes. *Designs, Codes and Cryptography*, 4(3):369–380, 1994.

[TACR04] Francois Treussart, Romain Alléaume, Jean-Michel Courty, and Jean-Francois Roch. Emission properties of a single photon source. *Physica Scripta*, 2004(T112):95, 2004.

[TALF+02] François Treussart, Romain Alléaume, Véronique Le Floch, LT Xiao, J-M Courty, and J-F Roch. Direct measurement of the photon statistics of a triggered single photon source. *Physical review letters*, 89(9):093601, 2002.

[TALF+03] F Treussart, R Alléaume, V Le Floc?h, LT Xiao, J-F Roch, and J-M Courty. Photon statistics of a single photon source. In *Organic Nanophotonics*, pages 413–422. Springer, 2003.

[TALFR02] François Treussart, Romain Alléaume, Véronique Le Floc'h, and Jean-François Roch. Single photon emission from a single molecule. *Comptes Rendus Physique*, 3(4):501–508, 2002.

[Tow97] Paul D Townsend. Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using wavelength-division multiplexing. *Electronics Letters*, 33(3):188–190, 1997.

[TZS+04] Alexei Trifonov, Anton Zavriyev, Darius Subacius, Romain Alléaume, and Jean-François Roch. Practical quantum cryptography. In *Quantum Information and Computation II*, volume 5436, pages 1–11. International Society for Optics and Photonics, 2004.

[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.

[Unr15] Dominique Unruh. Revocable quantum timed-release encryption. *Journal of the ACM (JACM)*, 62(6):1–76, 2015.

[VA20] Nilesh Vyas and Romain Alléaume. Everlasting secure key agreement with performance beyond qkd in a quantum computational hybrid security model. *arXiv preprint arXiv:2004.10173*, 2020.

[WEH18] Stephanie Wehner, David Elkouss, and Ronald Hanson. Quantum internet: A vision for the road ahead. *Science*, 362(6412), 2018.

[Wie83] Stephen Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983.

[WLW+11] C Wiechers, L Lydersen, C Wittmann, D Elser, J Skaar, Ch Marquardt, V Makarov, and G Leuchs. After-gate attack on a quantum cryptosystem. *New J. Phys*, 13(1):013043–, 2011.

[WPGP+12] Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J Cerf, Timothy C Ralph, Jeffrey H Shapiro, and Seth Lloyd. Gaussian quantum information. *Reviews of Modern Physics*, 84(2):621, 2012.

[WST08] Stephanie Wehner, Christian Schaffner, and Barbara M Terhal. Cryptography from noisy storage. *Physical Review Letters*, 100(22):220502, 2008.

[Wyn75] Aaron D Wyner. The wire-tap channel. *Bell system technical journal*, 54(8):1355–1387, 1975.

[XAX+03] Lian-Tuan Xiao, Romain Alléaume, Quyen Dinh Xuan, Francois Treussart, Bernard A Journet, and Jean-françois Roch. Measurement of photon distribution in attenuated diode laser pulses. In *Physics and Simulation of Optoelectronic Devices XI*, volume 4986, pages 463–468. International Society for Optics and Photonics, 2003.

[XAX+06] Quyên Dinh Xuân, R Alléaume, Liantuan Xiao, F Treussart, B Journet, and J-F Roch. Intensity noise measurement of strongly attenuated laser diode pulses in the time domain. *The European Physical Journal Applied Physics*, 35(2):117–121, 2006.

[XMZ+20] Feihu Xu, Xiongfeng Ma, Qiang Zhang, Hoi-Kwong Lo, and Jian-Wei Pan. Secure quantum key distribution with realistic devices. *Reviews of Modern Physics*, 92(2):025002, 2020.

[YLL+20] Juan Yin, Yu-Huai Li, Sheng-Kai Liao, Meng Yang, Yuan Cao, Liang Zhang, Ji-Gang Ren, Wen-Qi Cai, Wei-Yue Liu, Shuang-Lin Li, et al. Entanglement-based secure quantum cryptography over 1,120 kilometres. *Nature*, 582(7813):501–505, 2020.

[ZCP+20] Yichen Zhang, Ziyang Chen, Stefano Pirandola, Xiangyu Wang, Chao Zhou, Binjie Chu, Yijia Zhao, Bingjie Xu, Song Yu, and Hong Guo. Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. *Phys. Rev. Lett.*, 125:010502, Jun 2020.

[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.

[Zha19] Mark Zhandry. Quantum lightning never strikes the same state twice. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 408–438. Springer, 2019.