Protecting information in a quantum world: from cryptography to error correction

Anthony Leverrier

Université Pierre et Marie Curie

Faculté d'Ingénierie (UFR 919)

Anthony Leverrier

Inria Paris

a présenté publiquement le 27 septembre 2017

ses travaux pour l'obtention de

l'Habilitation à Diriger les Recherches

Protecting information in a quantum world: from cryptography to error correction

Rapporteurs

M. Iordanis Kerenidis,	Directeur de Recherche CNRS
M. Joseph Renes,	Chercheur, ETH Zurich
M. Andreas Winter,	Professeur, Université Autonome de Barcelone

Examinateurs

M. Claude Fabre,	Professeur, Université Pierre et Marie Curie
M. Philippe Grangier,	Directeur de Recherche CNRS
M. Aram Harrow,	Professeur MIT
Mme. Sophie Laplante,	Professeure, Université Paris-Diderot
M. Jean-Pierre Tillich,	Directeur de Recherche, Inria

A Catherine et Matthieu

Contents

Acknowledgements

In the spirit of this document, let me be brief and to the point. Let me first thank Toni Acín, Renato Renner for giving me the opportunity to spend very fruitful years as a postdoc in their respective group, and Anne Canteaut for hosting me and my research at Inria for the last 5 years (and hopefully for many more years to come). Let me obviously warmly thank Iordanis, Joe and Andreas for reviewing the present manuscript, as well as Claude, Philippe, Aram, Sophie and Jean-Pierre to accepting to participate in my habilitation committee.

More than ever, it is clear that research is a collective endeavor and I am grateful to have had many collaborators and co-authors over the years, most notably people in Toni's group at ICFO, Renato's at ETH, and finally here in the Secret project-team at Inria. I'm not going to be exhaustive because I would necessarily forget many people. Let me instead give special thanks to Philippe Grangier and Eleni Diamanti for never-ending discussions on quantum key distribution with continuous variables, to Tobias Fritz and Belén Sainz for an incredible project on contextuality, to André Chailloux and Frédéric Grosshans for many exciting discussions on relativistic cryptography, to Marc Kaplan, María Naya-Plasencia and Gaëtan Leurent for an intriguing project about symmetric cryptography in a quantum world, and to the TOCQ team - Jean-Pierre Tillich, Gilles Zémor, Nicolas Delfosse, Benjamin Audoux, Alain Couvreur - for spending so much time introducing me to the wonderful world of quantum error correction. The latter team was successful in their effort since I'm now convinced that quantum error correction is THE right topic to study.

Let me finally conclude by mentioning my first students, Kaushik, Antoine and Vivien, who never fail to come see me with many questions that I cannot answer! but also with new insights from which I've truly benefited over the past few years. Thanks for teaching me so much! Hopefully I'll be able to return the favor at some point.

List of Publications

Preprints and submitted manuscripts

1. A. Leverrier
"$SU(p, q)$ coherent states and Gaussian de Finetti theorems"
arXiv preprint arXiv:1612.05080.

2. M. Tomamichel, A. Leverrier
"A largely self-contained and complete security proof of quantum key distribution'
arXiv preprint arXiv:1506.08458.

Articles in Peer-Reviewed Scientific Journals

3. A. Leverrier
"Security of continuous-variable quantum key distribution via a Gaussian de Finetti reduction"
Physical Review Letters 118, 200501 (2017)

4. M. Kaplan, G. Leurent, A. Leverrier, M. Naya-Plasencia
"Quantum Differential and Linear Cryptanalysis"
Transactions on Symmetric Cryptology, 1 (2017)

5. K. Chakraborty, A. Chailloux, A. Leverrier
"Robust Relativistic Bit Commitment"
Physical Review A 94, 062314 (2016)

6. K. Chakraborty, A. Chailloux, A. Leverrier
"Arbitrarily long relativistic bit commitment"
Physical Review Letters 115, 250501 (2015)

7. K. Chakraborty, A. Leverrier
"Practical Position-Based Quantum Cryptography"
Physical Review A 92, 052304 (2015)

8. E. Diamanti, A. Leverrier
"Distributing Secret Keys with Quantum Continuous Variables: Principle, Security

and Implementations"
Entropy 17, 6072-6092 (2015)

9. A. Leverrier
"Composable security proof for continuous-variable quantum key distribution with coherent states"
Physical Review Letters, 114, 070501 (2015)

10. A. Leverrier, R. García-Patrón
"Analysis of circuit imperfections in BosonSampling"
Quantum Information & Computation 15, 0489-0512 (2015)

11. A. Acín, T. Fritz, A. Leverrier, A. B. Sainz
"A Combinatorial Approach to Nonlocality and Contextuality"
Communications in Mathematical Physics 334, 533-628 (2015)

12. N. Brunner, M. Kaplan, A. Leverrier, P. Skrzypczyk
"Dimension of physical systems, information processing, and thermodynamics"
New Journal of Physics 16, 123050 (2014)

13. A. B. Sainz, T. Fritz, R. Augusiak, J. B. Brask, R. Chaves, A. Leverrier, A. Acín
"Exploring the local orthogonality principle"
Physical Review A 89, 032117 (2014)

14. S. Pironio, L. Masanes, A. Leverrier, A. Acín
"Security of Device-Independent Quantum Key Distribution in the Bounded-Quantum-Storage Model"
Physical Review X 3, 031007 (2013)

15. T. Fritz, A. B. Sainz, R. Augusiak, J. B. Brask, R. Chaves, A. Leverrier, A. Acín
"Local orthogonality as a multipartite principle for quantum correlations"
Nature Communications 4, 2263 (2013)

16. P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, E. Diamanti
"Experimental demonstration of long-distance continuous-variable quantum key distribution"
Nature Photonics 7, 378-381 (2013)

17. A. Leverrier, R. García-Patrón, R. Renner, N. J. Cerf
"Security of Continuous-Variable Quantum Key Distribution Against General Attacks"
Physical Review Letters, 110, 030502 (2013)

18. P. Jouguet, S. Kunz-Jacques, E. Diamanti, A. Leverrier
"Analysis of imperfections in practical continuous-variable quantum key distribution"
Physical Review A, 86, 032309 (2012)

19. F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, R. F. Werner
"Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks"
Physical Review Letters, 109, 100502 (2012)

20. R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier, R. Tualle-Brouri
"Improving the maximum transmission distance of continuous-variable quantum key distribution using a noiseless amplifier"
Physical Review A, 86, 012327 (2012)

21. P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Alléaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache, P. Painchault
"Field Test of Classical Symmetric Encryption with Continuous Variable Quantum Key Distribution"
Optics Express, volume 20 (13), 14030-1404 (2012)

22. V. Dunjko, E. Kashefi, A. Leverrier
"Blind Quantum Computing with Weak Coherent Pulses"
Physical Review Letters, volume 108, 200502 (2012)

23. J. Bohr Brask, N. Brunner, D. Cavalcanti, A. Leverrier
"Bell tests for continuous-variable systems using hybrid measurements and heralded amplifiers"
Physical Review A, volume 85, 042116 (2012)

24. A. Leverrier
"A symmetrization technique for continuous-variable quantum key distribution"
Physical Review A, volume 85, 022339 (2012)

25. A. Bocquet, R. Alléaume, A. Leverrier
"Optimal eavesdropping on QKD without quantum memory"
Journal of Physics A, volume 45, 025305 (2012)

26. P. Jouguet, S. Kunz-Jacques, A. Leverrier
"Long Distance Continuous-Variable Quantum Key Distribution with a Gaussian Modulation"
Physical Review A, volume 84, 062317 (2011)

27. A. Leverrier, R. García-Patrón
"Percolation of secret correlations in a network"
Physical Review A, volume 84, 032329 (2011)

28. A. Leverrier, P. Grangier
"Continuous-variable quantum-key-distribution protocols with a non-Gaussian modulation"
Physical Review A, volume 83, 042312 (2011)

Papers published or initiated during the PhD

29. A. Leverrier, F. Grosshans, P. Grangier
"Finite-size analysis of continuous-variable quantum key distribution"
Physical Review A, volume 81, 062343 (2010)

30. A. Leverrier, P. Grangier
"Simple proof that Gaussian attacks are optimal among collective attacks against continuous-variable quantum key distribution with a Gaussian modulation"
Physical Review A, volume 81, 062314 (2010)

31. L. Magnin, F. Magniez, A. Leverrier, N. J. Cerf
"Strong no-go theorem for Gaussian quantum bit commitment"
Physical Review A, volume 81, 010302(R) (2010)

32. A. Leverrier, E. Karpov, P. Grangier, N. J. Cerf
"Security of continuous-variable quantum key distribution: towards a de Finetti theorem for rotation symmetry in phase space"
New Journal of Physics, volume 11, 115009 (2009)

33. A. Leverrier, N. J. Cerf
"Quantum de Finetti theorem in phase-space representation"
Physical Review A, volume 80, 0010102(R) (2009)

34. A. Leverrier, P. Grangier
"Unconditional security proof of long-distance continuous-variable quantum key distribution with a discrete modulation"
Physical Review Letters, volume 102, 180504 (2009)

35. A. Leverrier, R. Alléaume, J.J. Boutros, G. Zémor, P. Grangier
"Multidimensional reconciliation for continuous-variable quantum key distribution"
Physical Review A, volume 77, 042325 (2008)

36. A. Zavriyev, A. Leverrier, V. Denchev, A. Trifonov
"Improving the performance of quantum key distribution apparatus"
Journal of Modern Optics, volume 54, Pages 305–313 (2007)

Conference Proceedings

37. A. Chailloux, A. Leverrier
"Relativistic (or 2-prover 1-round) zero-knowledge protocol for NP secure against quantum adversaries"
EUROCRYPT, 2017

38. M. Kaplan, G. Leurent, A. Leverrier, M. Naya-Plasencia
"Breaking Symmetric Cryptosystems using Quantum Period Finding"
CRYPTO 2016

39. A. Leverrier, J.-P. Tillich, G. Zémor
"Quantum Expander Codes"
56th Annual IEEE Symposium on Foundations of Computer Science, FOCS, 2015

40. T. Fritz, A. Leverrier, A. B. Sainz
"Probabilistic models on contextuality scenarios"
Quantum Physics and Logic, QPL, 2013

Papers published or initiated during the PhD

41. A. Leverrier, P. Grangier
"Long distance quantum key distribution with continuous variables"
Sixth Conference on the Theory of Quantum Computation, Communication and Cryptography, 2011

42. D. Elkouss, A. Leverrier, R. Alléaume, J.J. Boutros
"Efficient reconciliation protocol for discrete-variable quantum key distribution",
International Symposium on Information Theory, ISIT, 2009

43. A. Leverrier, R. Alléaume, J.J. Boutros, G. Zémor, P. Grangier
"Multidimensional reconciliation for continuous-variable quantum key distribution",
International Symposium on Information Theory, ISIT, 2008

Patent

- Procédé de distribution quantique de clés à† variables continues
Patent FR2933833 (A1), published on January, 15 2010
Inventors: Anthony Leverrier, Philippe Grangier

Résumé

Ce manuscrit présente mes principaux résultats de recherche obtenus ces 5 dernières années. Ils tournent autour de 3 thèmes principaux :

1. la *distribution quantique de clés à variables continues* était déjà le sujet de ma thèse. Au cours de cette dernière, j'avais proposé de nouvelles solutions pour améliorer les performances de tels protocoles, mais j'avais malheureusement laissé en suspens la question essentielle à mon avis : celle de la sécurité de ces protocoles contre des attaques arbitraires. J'ai finalement récemment résolu cette question en introduisant une nouvelle classe d'états cohérents généralisés et en établissant une version gaussienne du théorème de de Finetti quantique.

2. l'étude des *corrélations quantiques et leur application à la cryptographie*. J'ai commencé à étudier ce qu'on appelle "corrélations quantiques" lors de mon séjour postdoctoral à Barcelone dans le groupe d'Antonio Acín, et j'ai poursuivi cette activité plus récemment en encadrant un étudiant de thèse, Kaushik Chakraborty, qui a travaillé sur certaines applications cryptographiques, notamment la géolocalisation et la mise en gage, en collaboration avec André Chailloux.

3. le *calcul quantique*. Depuis mon arrivée chez Inria, j'ai initié de nouvelles recherches plus éloignées de la cryptographie, qui se tournent davantage vers les codes correcteurs d'erreur nécessaires au calcul quantique. En particulier, j'encadre actuellement deux étudiants en thèse, Antoine Grospellier et Vivien Londe sur ce sujet.

Un point commun de ces thèmes est la volonté de protéger l'information quantique, que ce soit vis-à-vis d'un adversaire dans le contexte cryptographique ou de l'environnement quand on s'intéresse aux mécanismes de correction d'erreur nécessaires à la construction d'un ordinateur quantique universel.

Distribution quantique de clés à variables continues

La distribution quantique de clé (QKD en anglais) vise à distribuer une clé secrète à deux parties distantes qui ont accès à un canal de communication classique authentifié et à un canal quantique sur lequel on ne fait aucune hypothèse. Les protocoles les plus standards sont fondés sur l'échange d'états quantiques encodés sur des photons uniques et nécessitent d'utiliser des détecteurs de photons uniques. Une approche technologique

intéressante consiste plutôt à encoder l'information sur des degrés de liberté continus correspondant aux quadratures du champ électromagnétique quantifié. Dans ce cas, les détecteurs de photons uniques peuvent être remplacés par une détection cohérente, qui peut être mise en oeuvre avec des équipements relativement standard en telecom. La simplicité de cette technologie a toutefois un prix, à savoir une analyse de sécurité nettement plus difficile pour ces protocoles à variables continues. Plus précisément, un protocole de QKD à variables continues est formellement décrit par un canal quantique agissant sur un espace de Fock. Le fait qu'un espace de Fock soit espace de Hilbert de dimension infinie est à l'origine de nombreuses complications mathématiques qui ne peuvent pas être adressées avec les outils développés pour étudier les protocoles en dimension finie.

Dans le premier chapitre de ce manuscrit, je décris un tel protocole de QKD à variables continues, précise les définitions de sécurité pour les protocoles de QKD et présente les principaux outils que j'ai développés pour établir la sécurité de ce protocole particulier. En particulier, j'explique comment exploiter les symétries spécifiques du protocole dans l'espace des phases afin de procéder à la tomographie des états quantiques pertinents en dimension infinie [Lev15]. Puis je démontre une version gaussienne du théorème de de Finetti quantique, qui permet, en le combinant à un test d'énergie initialement introduit dans [LGPRC13], de réduire l'étude de la sécurité du protocole contre des attaques générales à sa sécurité contre une famille restreinte d'attaques appélées "attaques collectives gaussiennes" [Lev17]. De telles attaques peuvent finalement être analysées grâce à la technique d'estimation de matrice de covariance développée dans [Lev15].

La série de papiers [Lev15], [Lev16], [Lev17] permet ainsi d'obtenir la première preuve de sécurité d'un protocole de distribution quantique de clés à variables continues basées sur l'échange d'états cohérents.

Corrélations quantiques et leur application à la cryptographie

Le deuxième chapitre de ce manuscrit porte sur l'étude des corrélations quantique et leur application potentielle à des fins cryptographiques.

Je discute d'abord une approche combinatoire permettant d'appréhender les propriétés de telles corrélations et qui fut introduite dans un travail commun avec Tobias Fritz, Antonio Acín et Ana-Belén Sainz [AFLS15]. Cette approche a été initialement développée afin d'étudier le "principe d'orthogonalité locale", dont l'espoir était qu'il permette de retrouver les corrélations quantiques à partie d'un principe simple de théorie de l'information.

Je considère ensuite la primitive cryptographique de géolocaliation. Alors qu'il est établi que cette primitive ne peut pas être prouvée sûre au sens de la théorie de l'information, les meilleures attaques génériques connues à ce jour nécessitent des ressources en intrication totalement irréalistes. Dans un travail avec Kaushik Chakraborty, nous avons proposé une famille d'attaques efficaces fonctionnant contre une importante classe de protocoles [CL15].

Une observation récente dans le domaine de la cryptographie basée sur des principes physiques est qu'il est possible d'exploiter le fait que l'information ne puisse se propager

plus vite que la vitesse de la lumière pour imposer des contraintes sévères sur les actions qu'une coalition d'agents peuvent effectuer. En particulier, ce principe est suffisant pour obtenir une sécurité au sens de la théorie de l'information pour des primitives qui ne peuvent pas être montrées sûres en exploitant seulement les limitations imposées par la mécanique quantique. Dans deux papiers avec André Chailloux et Kaushik Chakraborty, nous avons étudié plus précisément une forme faible de mise en gage, ou un bit peut être mis en gage pour un temps arbitrairement long [CCL15], [CCL16]. Une aplication de ce travail a été de montrer comment obtenir des preuves à divulgation nulle de connaissance pour NP qui soient sûres contre des attaques quantiques [CL16].

Calcul quantique

Le troisième chapitre s'éloigne de la cryptographie quantique et adresse des questions de plus long terme liées à l'apparition d'ordinateurs quantiques universels. Ce chapitre est divisé en trois parties.

Je considère d'abord le "Boson Sampling", un modèle de calcul quantique non-universel, qui a attiré un intérêt considérable ces dernières années en tant qu'approche possible pour démontrer la supériorité du traitement quantique de l'information par rapport à un traitement purement classique. Mon travail effectué sur ce domaine en collaboration avec Raúl García-Patrón consiste en une analyse de l'effet des imperfections dans des circuits quantiques de Boson Sampling : plus précisément, comprendre comment des erreurs locales dans les portes optiques du circuit affectent le résultat final du calcul. L'analyse est rendue non triviale car elle fait intervenir le permanent (le cousin du déterminant, notoirement plus difficile à manipuler !) d'une grande matrice, et qu'il faut donc étudier comment les petites perturbations liées au bruit local impactent ce permanent [LGP15]. La motivation de ce travail était de comprendre à quel point l'absence de mécanisme de tolérance aux fautes était préjudiciable pour le Boson Sampling.

Ensuite, je discute d'une famille de codes quantiques appelés "codes expanseurs quantiques" que nous avons introduite avec Jean-Pierre Tillich and Gilles Zémor, qui est basée sur leur construction de produit d'hypergraphes [TZ14], et pour laquelle nous avons analysé un algorithme de décodage efficace qui permet de corriger des erreurs adversariales dont le poids est en racine carrée de la longueur du code [LTZ15]. Ces codes sont les meilleurs codes LDPC quantiques connus en termes de distance minimale et notre algorithme est optimale puisqu'il n'y a pas moyen de décoder des erreurs adversariales de poids plus élevé que la distance minimale. De tels codes LDPC avec un algorithme de décodage efficace sont un pré-requis incontournable dans l'optique de construire des ordinateurs quantiques universels de taille importante.

Je temine en mentionnant des travaux récents effectués en collaboration avec Marc Kaplan, Gaëtan Leurent et María Naya-Plasencia sur la cryptanalyse quantique de systèmes de chiffrement symétrique [KLLNP16a], [KLLNP16b]. Le but de ce travail est de comprendre comment la sécurité de la cryptographie symétrique (à clé secrète) serait affectée par l'apparition d'ordinateurs quantiques universel, et de voir si la contre-mesure habituelle consistant à doubler la taille de la clé est suffisante pour parer les attaques

quantiques. Dans notre travail, nous avons recours à principaux algorithmes quantiques et exploitons des variantes de l'algorithme de Grover (marches quantiques) et de l'algorithme de Shor (pour la recherche de période) dans le but de développer de nouvelles attaques qui montrent que l'approche standard consistant à doubler les tailles de clés est sans doute insuffisante et que cette question mérite d'être étudiée plus avant.

Introduction

This manuscript summarizes my research activity of the past 5 years, which revolves around three main themes:

1. quantum key distribution with continuous variables,
2. quantum correlations and their use for cryptography,
3. quantum computation.

Quantum key distribution with continuous variables

Quantum key distribution (QKD) aims at distributing secret keys to two distant parties who have access to an authenticated classical channel, and an untrusted quantum channel. The standard protocols are based on the exchange of single-photon states between the two parties, and require the receiver to use single-photon counters. A technologically appealing alternative is encode the information on the continuous degrees of freedom corresponding to the quadratures of the quantized electromagnetic field. In that case, single-photon detectors can be replaced by coherent detection, relying on standard telecommunication equipment. This technological simplicity comes at a price however, namely that of of more mathematically involved security analysis of the QKD protocol. More precisely, a continuous-variable (CV) QKD protocol corresponds to a quantum channel acting on a Fock space, which is an infinite-dimensional Hilbert space. This infinite dimensionality is at the heart of many technical complications as many of the tools that have been developed to deal with qubit-based protocols break down when the dimension of the quantum systems becomes too large.

In the first chapter of this manuscript, we will describe such a CV QKD protocol, explain the security definitions for QKD protocols and present the main new tools that we have developed in order to address this question. In particular, we will start by explaining how to exploit specific symmetries of the protocol in phase-space in order to perform the tomography of the relevant infinite-dimensional quantum states [Lev15]. Then we will derive a so-called "Gaussian de Finetti" theorem [Lev16], which allows us, when combined with an appropriate energy test initially introduced in [LGPRC13], to reduce the problem of proving that the protocol is secure to establishing its security against a restricted class of attacks, called Gaussian collective attacks [Lev17]. Such

attacks can finally be addressed thanks to the technique for covariance matrix estimation developed in [Lev15].

It should be noted that the series of papers [Lev15], [Lev16], [Lev17] lead to the first full security proof of CV QKD based on the exchange of coherent states.

Quantum correlations and their use for cryptography

The second chapter is concerned with the study of quantum correlations and their potential application for cryptographic purposes.

We first discuss a combinatorial approach to discuss the properties of such correlations that was introduced in a work with Tobias Fritz, Antonio Acín and Ana-Belén Sainz [AFLS15]. This approach was initially developed in order to study the "local orthogonality" principle, which was a candidate to recover quantum correlations from a simple information-based physical principle.

I will then consider the cryptographic task of position verification. While it is known that information-theoretic security cannot be achieved for this task, the current attacks require an exponential amount of resources (entanglement, for quantum protocols) which means that the protocols are hardly broken. In a work with Kaushik Chakraborty, we proposed a family of efficient attacks that apply against a large class of protocols [CL15].

A recent observation in the field of physical-based cryptography is that the fact that information cannot travel faster than the speed of light puts severe constraints on the tasks that a coalition of agents can perform. In particular, this principle is sufficient to obtain information-theoretic security for cryptographic tasks that cannot be achieved with the help of quantum theory alone. In a series of papers with André Chailloux and Kaushik Chakraborty, we studied more particularly a weak form of bit commitment, where a bit can be committed for an arbitrarily long time [CCL15], [CCL16]. As an application, we showed how to obtain zero-knowledge proofs for NP secure against quantum attacks [CL16].

Quantum computation

The third chapter moves away from quantum cryptography and addresses more long term questions related to the appearance of quantum computers. The chapter is divided along three axes.

First, I will consider Boson Sampling, a non-universal model for quantum computing, which has attracted considerable interest in the past few years as a proposal to experimentally demonstrate the superiority of quantum information processing over classical processing. My work together with Raúl García-Patrón in this area consists in an analysis of the effects of imperfections in quantum circuits for Boson Sampling: more precisely, understanding how local errors in the optical gates of the circuit translate into a global error for the overall sampling task. This analysis is made nontrivial because the sampling procedure involves the permanent of a large matrix, and that the error analysis involves the study of how the permanent is modified by the small perturbation corresponding to

the local noise [LGP15]. The motivation behind this work was to understand whether the absence of fault-tolerance mechanisms for Boson Sampling would kill the whole approach, and the answer is apparently not.

In a second part, I will discuss a class of quantum codes named "quantum expander codes" that we introduced with Jean-Pierre Tillich and Gilles Zémor following their hypergraph-product construction [TZ14], and for which we proposed and analyzed an efficient decoding algorithm that can correct adversarial errors with a weight scaling like the square-root of the code length [LTZ15]. These codes are the best known quantum LDPC codes in terms of minimum distance, and our algorithm is optimal since there is no hope of decoding adversarial errors beyond the minimum distance. Such quantum LDPC codes with an efficient decoding algorithm are certainly a prerequisite to building large scale quantum computers.

Finally, I will mention some recent work on the quantum cryptanalysis of symmetric cryptosystems in collaboration with Marc Kaplan, Gaëtan Leurent and María Naya-Plasencia [KLLNP16a], [KLLNP16b]. The goal of this work is to understand how the security of symmetric cryptography is affected by the advent of quantum computation, and see whether the standard countermeasure consisting in doubling the key size is indeed sufficient. In our work, we make use of the main quantum algorithms and exploit variations of Grover's algorithms (quantum walks) and Shor's algorithm (for period finding) in order to develop attacks against symmetric cryptography, demonstrating that the common wisdom is a bit too simplistic and that further study of the problem is definitely called for.

Chapter 1

Theoretical tools for continuous-variable quantum cryptography

This chapter is devoted to the analysis of quantum key distribution (QKD) with continuous variables. We first introduce the concept of QKD in Section 1.1 and present the "canonical" continuous-variable QKD protocol is Section 1.2. The following three sections are devoted to the main tools we developed to address the security of this protocol: more specifically, Section 1.3 explains how to perform the tomography of the covariance matrix of an arbitrary quantum state, Section 1.4 shows how an energy test allows one to efficiently bound the dimension of the relevant Hilbert space and Section 1.5 introduces the Gaussian de Finetti reduction needed to reduce the full security proof to the analysis of Gaussian collective attacks.

1.1 Quantum key distribution: principle and security

The most advanced application of the field of quantum information is without a doubt quantum cryptography, and more precisely quantum key distribution. The goal of this cryptographic primitive is to allow two distant users who have access to an authenticated classical channel and an untrusted quantum channel to distill a secret key that can be later used to encrypt communication [BB84], [Eke91].

More formally, an Entanglement-Based (EB) QKD protocol $\mathcal{E}$ between Alice and Bob is a Completely-Positive Trace-Preserving (CPTP) map acting on an arbitrary input state ρ_{AB} where $A = A_1 \otimes \cdots \otimes A_n$ (resp. $B = B_1 \otimes \cdots \otimes B_n$) consists of n quantum systems held by Alice (resp. by Bob) and outputs two keys K_A for Alice and K_B for Bob as well as some transcript classical C. The protocol is allowed to abort, in which case the keys have length 0.

Let us immediately note that for many protocols, the quantum systems A_i, B_i are assumed to be finite-dimensional, for instance 2-dimensional for the BB84 protocol. In con-

trast, the protocols we will focus on in this chapter encode their information in the phase-space of bosonic quantum systems, meaning that A_i (or B_i) is an infinite-dimensional quantum system, described by a Fock space with orthonormal basis $\{|k\rangle_{A_i} : k \in \mathbb{N}\}$ where the Fock state $|k\rangle_{A_i}$ corresponds to a state with k photons in the mode A_i.

Two properties are considered when assessing the *security* of a QKD protocol: it should be *correct*, meaning that both keys should be identical, and should output *secret* keys, appearing as uniformly random from the point of view of any adversary, possibly in possession of a quantum system E correlated with ρ_{AB}. In practice, these features cannot be obtained exactly, and one says that the protocol $\mathcal{E}$ is ε-*secure* if it is ε-close to an ideal protocol $\mathcal{F}$ satisfying both properties:

$$\frac{1}{2}\|\mathcal{E} - \mathcal{F}\|_\diamond \leq \varepsilon, \tag{1.1}$$

where the diamond norm (also known as the completely bounded trace norm) quantifies how well one can distinguish the CPTP maps $\mathcal{E}$ and $\mathcal{F}$. It is defined as:

$$\|\Delta\|_\diamond := \sup_{\|\rho\|_1=1} \|\Delta \otimes \mathrm{id}_{\mathcal{E}}(\rho_{ABE})\|_1, \tag{1.2}$$

where the supremum is taken over states ρ on systems A, B and E and $\|\sigma\|_1 := \mathrm{tr}\sqrt{\sigma^\dagger\sigma}$ is the trace norm. Here, the system E is arbitrary but the supremum is always attained for $E \cong AB$. The reader is referred to the monograph [Wat16] for further details on these norms.

Evaluating the diamond distance $\|\mathcal{E} - \mathcal{F}\|_\diamond = \sup_{\rho_{ABE}} \|\mathcal{E}_{AB} \otimes \mathrm{id}_E(\rho)_{ABE} - \mathcal{F}_{AB} \otimes \mathrm{id}_E(\rho)_{ABE}\|_1$ is very challenging in general and one can use a result by Portmann and Renner [PR14] to split this norm into two terms corresponding to correctness and secrecy: a protocol that is $\varepsilon_{\mathrm{corr}}$-correct and $\varepsilon_{\mathrm{secr}}$-secret is ε-secure provided that $\varepsilon_{\mathrm{corr}} + \varepsilon_{\mathrm{secr}} \leq \varepsilon$ where we say that the protocol is $\varepsilon_{\mathrm{corr}}$-correct if for all state ρ_{ABE}

$$\Pr[K_A \neq K_B]_\omega \leq \varepsilon_{\mathrm{corr}}$$

and that the protocol is $\varepsilon_{\mathrm{secr}}$-secret if for all state ρ_{ABE}

$$\Pr[K_A, K_B \neq \varnothing]_\omega \cdot \frac{1}{2}\|\omega_{K_AEC} - \chi_{K_A} \otimes \omega_{EC}\|_1 \leq \varepsilon_{\mathrm{secr}}$$

where $\omega_{K_AK_BEC} := \mathcal{E}_{AB} \otimes \mathrm{id}_E(\rho_{ABE})$ is the output of the protocol and χ_{K_A} is the maximally mixed state over strings x with the same length as K_A. The system E assumed to be in the hands of an eavesdropper can without loss of generality be assumed to purify the state ρ_{AB}. Proving the correctness of a protocol is straightforward: it is sufficient for Alice and Bob to compute a small hash of their keys and compare them publicly to make sure that their keys coincide with high probability. The real challenge lies in establishing the secrecy of the keys. This is achieved thanks to the *leftover hashing lemma* [Ren08], [TSSR11], which holds if K_A is obtained by applying a random universal$_2$ hash function of length ℓ to the raw key X, where ℓ should be slightly smaller than the smooth min-entropy of X conditioned on EC. The smooth min-entropy, $H_{\min}^{\varepsilon}(X|EC)$, introduced in

Ref. [Ren08], characterizes the average probability that Eve guesses X correctly using her optimal strategy with access to the correlations stored in her quantum memory E and the classical transcript C [KRS09], [TCR09]. Applying the privacy amplification procedure to the string X yields a key of size ℓ which is ε_{sec}-secret provided that [TLGR12], [TSSR11], [BFS11]

$$\varepsilon_{\text{sec}} = \min_{\varepsilon'} \frac{1}{2}\sqrt{2^{l-H_{\min}^{\varepsilon'}(X|EC)}} + 2\varepsilon'. \tag{1.3}$$

We refer the reader to [Ren08], [PR14] for a more in-depth discussion of the security of QKD.

One notes that with the formalism described so far, a QKD protocol takes as an input a (large) bipartite quantum state ρ_{AB}, which means that the distribution of the quantum state is not considered to be part of the QKD protocol. The standard picture is that Alice and Bob have access to some untrusted quantum channel $\mathcal{N} : \overline{A} \to B$. Alice therefore starts by preparing some entangled state $\Phi_{A\overline{A}}$ and sends the content of register $\overline{A}$ to Bob through $\mathcal{N}$. One then defines $\rho_{AB} := (\text{id}_A \otimes \mathcal{N}_{\overline{A}\to B})(\Phi_{A\overline{A}})$.

A general QKD protocol will be characterized by the choice of:

- an initial state $\Phi_{A\overline{A}}$ prepared by Alice: for BB84, it is the tensor product of n Bell pairs; for continuous-variable protocols, it is the tensor product of n two-mode squeezed vacuum states $|\lambda\rangle := \sqrt{1-|\lambda|^2}\sum_{k=0}^{\infty}\lambda^k|k,k\rangle$ for some fixed value λ of the squeezing satisfying $|\lambda| < 1$;

- an encoding, or equivalently a measurement map for Alice and Bob: for BB84, both Alice and Bob measure each of their n qubits randomly in the computational or Hadamard basis; for the CV protocol we will investigate, they measure their n modes with heterodyne detection (corresponding to a projection onto coherent states);

- a specific classical postprocessing procedure that helps them turn their measurement results into two secret keys K_A and K_B.

A crucial observation is that provided that Alice's equipment is trusted and well calibrated, the classical-quantum (cq) state that she shares with Bob after she measured register A and before Bob measures B could have been alternatively obtained by preparing an initial cq state and sending the quantum part through the quantum channel. Such a protocol is called Prepare-and-Measure (PM) and typically corresponds to what is done in practical implementations since it is much easier to prepare a cq state than an entangled state. That the security is identical in both versions is well-known and was proven in the case of Gaussian CV protocols in Ref. [GCW+03].

For a protocol to be interesting, security is not enough since a protocol that always aborts is secure according to the definition we gave above. One also wants a protocol that is *robust*, *i.e.*, that produces large keys for *passive adversaries* described by a quantum channel $\mathcal{N}$ modeling the typical behaviour of an optical fiber for instance. One is then interested in the rate $r = \frac{\ell}{n}$ where ℓ is the expected length of K_A, as a function of the

channel parameters such as loss and noise. In the context of finite-size analysis, it is also important to understand how fast r converges to its asymptotic value (limit $n \to \infty$), and in particular what is the minimum block size n that gives a nonzero key length.

Before turning to the protocol itself, let us say a few words about security proofs (more detailed references are [SBPC+09] for general protocols and [DL15] for CV protocols). As already pointed out, establishing the security of a QKD protocol against general attacks in the sense of Eq. 1.1 is nontrivial and a first step is often to prove its security against *collective attacks*: this means proving that the protocol is secure when restricting input states to independent and identically distributed (i.i.d.) states of the form $\rho_{AB} = \sigma^{\otimes n}$ for some state σ on A_1B_1. This is usually a much simpler task. Then, one uses de Finetti-type reductions [Ren07], [CKR09] in order to show that ε-security against collective attacks implies ε'-security against general attacks with $\varepsilon' = \varepsilon \times \text{poly}(n)$. Since ε can be made exponentially small in n by reducing the key size by an arbitrarily small fraction compared to the asymptotic rate, the polynomial overhead is negligible and one obtains a full security proof. For some protocols (such as BB84 and some specific CV protocols), a more direct approach is possible through the use of entropic uncertainty relations [TLGR12], [TL15], [FFB+12].

1.2 A CV QKD protocol with heterodyne detection

QKD protocols with continuous variables were introduced by Ralph [Ral99] but initially tried to copy the ideas from BB84 by using 4 different squeezed states to play the role of the 4 BB84 states. An important breakthrough in the field was the realization that secure protocols could be obtained with a Gaussian modulation of *coherent states* [GG02b], which are both much more practical and exploiting efficiently the phase space by allowing for continuous modulations.

In this document, we will focus on what is arguably the most natural CV protocol, in the sense that it displays the most symmetries making its analysis somewhat more tractable (but not easy!): in its EB version, Alice prepares two-mode squeezed states $|\lambda\rangle$, distribute one half of each state to Bob and both parties measure their systems with heterodyne detection; in its PM version (described in Table 1.1 below), Alice prepares coherent states with a Gaussian modulation. This protocol was first investigated in [WLB+04]. We note that the protocol uses *reverse reconcilation* [GG02a] meaning that Bob's measurement results will be used as the raw key since it is known to increase the robustness of the protocol.

The description of the protocol in Table 1.1 makes some simplifying assumptions. In practice, the measurement results x and y should be discretized but we ignore this in the following. We also assume that the measurement devices of Alice and Bob are trusted and behave according to their theoretical model: in particular, the heterodyne measurement admits the coherent states as POVM elements (recall that the coherent states resolve the identity: $\frac{1}{\pi}\int |\alpha\rangle\langle\alpha| \mathrm{d}\alpha = \mathbb{1}$). In other words, for a single-mode state ρ, the probability density function of measurement outcome is $p(\alpha) = \frac{1}{\pi}\langle\alpha|\rho|\alpha\rangle$ with $|\alpha\rangle := e^{-|\alpha|^2/2}\sum_{i=0}^{\infty}\frac{\alpha^i}{\sqrt{i!}}|i\rangle$. One can also model imperfect preparation and measurement

Input: Alice and Bob have access to a quantum channel $\mathcal{N}_{A\to B} : A \to B$ where $A = A_{[n]}$ and $B_{[n]}$ are comprised of n quantum systems. In practice, the channel will be an optical fiber.

State Preparation: Alice chooses a random string $x = (x_1, \cdots, x_n) \in \mathbb{R}^{2n}$ where $x_k \sim \mathcal{N}(0, \sigma^2)$ and prepares the n-mode quantum state $\rho^x := \bigotimes_{k=1}^{n} |x_{2k} + ix_{2k+1}\rangle$, where $|\alpha\rangle$ is the coherent state centered on $\alpha \in \mathbb{C}$, *i.e.*, $|\alpha\rangle := e^{-|\alpha|^2/2} \sum_{i=0}^{\infty} \frac{\alpha^i}{\sqrt{i!}} |i\rangle$.

State Distribution: Alice sends the n-mode state ρ^x through the quantum channel $\mathcal{N}$ and Bob receives the output state $\rho_B^x = \mathcal{N}(\rho^x)$.

Measurement: Bob measures the n optical modes corresponding to the output state with heterodyne detection and stores his measurement outcomes in a string $y \in \mathbb{R}^{2n}$.

Symmetrization: Alice and Bob pick a random unitary from the Haar measure on $U(n)$ and apply it to their respective vectors x and y, seen as n-dimensional complex vectors, obtaining two new vectors $u, v \in \mathbb{R}^{2n}$.

Error Correction: Bob sends some side-information of size leak_{EC} to Alice who outputs a guess $\hat{v}$ for the string of Bob. Bob computes a hash of v of length $\lceil \log_2(1/\varepsilon_{\text{cor}}) \rceil$ and sends it to Alice who compares it with her own hash. If both hashes differ, the protocol aborts.

Parameter Estimation: Bob sends $n_{\text{PE}} = O(\log(1/\varepsilon_{\text{PE}}))$ bits of information to Alice that allow her to compute $\|x\|^2 = \|u\|^2$, $\|y\|^2 = \|v\|^2$ and $\langle x, y\rangle = \langle u, v\rangle$. Depending on these three values, the protocol either continues or aborts (see Ref. [Lev15] for details).

Privacy Amplification: They compute keys $K_A = H_{\text{pa}}(\hat{v})$ and $K_B = H_{\text{pa}}(v)$ of length ℓ for some hash function H_{pa}.

Table 1.1 – Prepare and Measure version of the CV QKD protocol with Gaussian modulation of coherent states and heterodyne detection

along the lines of [JKJDL12], [LBGP+07], but we will assume here for simplicity that the devices behave perfectly. Another standard assumption in the CV QKD literature is that the eavesdropper cannot tamper with the Local Oscillator used for the measurement. This assumption might appear unjustified at first glance, which prompted some recent research on the development of local generation of the local oscillator at Bob's station [SBC+15], [QLP+15].

Finally, let us note that the protocol above has a *symmetrization* step, which is rather unpractical since it involves drawing a unitary from the Haar measure on $U(n)$. This has complexity $O(n^2)$. We choose to add this extra-step explicitly in order to argue that the protocol is invariant under the action of the unitary group $U(n)$, as we will

see in Section 1.5. For discrete-variable protocols such as BB84, one instead assumes that the protocols are invariant under the action of the symmetric group S_n and one can enforce this symmetry by applying a random permutation. It has been claimed in the literature that this *active symmetrization* is in fact not needed [Ren07] and indeed some security proofs do not require this symmetrization step [TLGR12]. There are therefore reasons to be believe that the symmetrization step is not required either for the CV protocol outlined in Table 1.1. In particular, the crucial part of the postprocessing is the estimation of the correlations $\|x\|^2, \|y\|^2, \langle x, y\rangle$ and these quantities are clearly invariant under the group $U(n)$.

In the EB version of the protocol, Alice would start by preparing n two-mode squeezed vacuum states, measure the $A_{[n]}$ systems with heterodyne detection and store the (properly rescaled) results in the string x. Details can be found for instance in Ref. [Lev15].

We conclude this section by mentioning some difficulties that arise when analyzing CV QKD protocols such as the one above:

- roughly speaking, a QKD protocol is essentially a tomography procedure that aims at deciding whether the state shared by Alice and Bob is sufficiently correlated to allow them to distill a secret key. This is done via the crucial step of *parameter estimation*. For protocols such as BB84, the goal is to estimate the quantum bit error rate, a value between 0 and 1. In CV protocols on the other hand, the right measure of correlations is the covariance matrix of the bipartite state shared by Alice and Bob. Here the complication lies in the fact that this matrix is not *a priori* bounded and providing confidence regions for unbounded random variables turns out to be very challenging. We solve this problem by symmetrizing the protocol under the action of the unitary group [Lev15].

- another challenge results from the infinite dimension of the Fock space Hilbert space, rendering most techniques developed for qubit protocols ineffective. Fortunately, the CV protocols we consider involve states with bounded energy in practice. The goal here consists in designing the right tests of energy that will allow us to truncate the Fock space in order to obtain a finite-dimensional Hilbert space.

- finally, such a truncation still gives a very large local Hilbert space (of order $\log n$) if performed naively. In that case, de Finetti reductions are too weak to guarantee security for practical values of n. We solve this challenge by establishing a new Gaussian version of the de Finetti theorem.

We have been able to address each of these difficulties in a series of papers [LGPRC13], [Lev15], [Lev16], [Lev17] and we will describe the techniques we developed in the next sections.

The general outline of the security proof is as follows. Let us denote by $\mathcal{E}_0$ the protocol of Table 1.1. Let us further design an energy test $\mathcal{T}$ that takes as input a spate in some larger space $A_1 \cdots A_{n+k} B_1 \cdots B_{n+k}$ with $k \ll n$ that either passes and return a state of $A_1 \cdots A_n B_1 \cdots B_n$ or aborts the protocol. In other words, both Alice and Bob start with an $(n+k)$-mode state, measure k of these modes, and are left with an n-mode state. The

overall protocol that we consider is $\mathcal{E} := \mathcal{R} \circ \mathcal{E}_0 \circ \mathcal{T}$, where $\mathcal{R}$ is an additional privacy amplification procedure. The security proof involves several steps:

- showing that $\mathcal{E}_0$ is secure against collective attacks (Section 1.3),
- showing that the test $\mathcal{T}$ allows us to restrict our attention to states in a certain finite-dimensional Hilbert space (Section 1.4),
- showing that the reduction from general to collective attacks is efficient, thanks to a Gaussian de Finetti theorem (Section 1.5).

1.3 Tomography of large continuous-variable systems

In this section, we focus on the problem of bounding the covariance matrix of an unknown quantum state. Recall that for a QKD protocol to be secure, it should output a secret key (possibly of length 0) for *any* possible input state. The parameter estimation step of the protocol is a test where Alice and Bob check whether their measurement outcomes are sufficiently correlated and can be exploited to distill a secret key of length $\ell > 0$. If the test fails, then the protocol aborts. This task is reminiscent of *quantum state tomography*, but differs in two crucial ways: (*i*) in QKD, we are only interested in estimating a specific measure of correlations, not the whole density matrix; (*ii*) in QKD, the procedure should work for arbitrary state, while quantum state tomography is designed to work well on the specific states that are prepared in a given experiment, without any success guarantee for arbitrary states.

For discrete-variable protocols such as BB84, the appropriate measure of correlations is the so-called quantum bit error rate (qber) which takes values between 0 and 1, corresponding to the fraction of bits for which Alice and Bob's results differ. The test then takes the following form: fix some threshold $\delta \in (0, 1)$ and and integers k, m such that $k + m = n$. Alice and Bob publicly reveal a random subset of k of their measurement outputs and check whether the average fraction of errors is below δ. In that case, the test passes and the protocol continues, otherwise it aborts. In order to make a security statement, one then needs to show that the probability that the test passes *and* that the quantum bit error rate on the rest on the measurement results is much larger than δ, is negligible.

For instance, the following theorem was established in [TLGR12].

Theorem 1. *Consider a set of binary random variables $Z = (Z_1, Z_2, \ldots, Z_n)$ with Z_i taking values in $\{0, 1\}$ and $n = m + k$. Let Π be a uniformly distributed random subset of $[n]$ of size k. Then,*

$$\Pr\left[\sum_{i\in\Pi} Z_i \leq k\delta \ \wedge \ \sum_{i\in\bar{\Pi}} Z_i \geq m(\delta+\nu)\right] \leq \exp\left(-2\nu^2 \frac{nk^2}{(m+k)(k+1)}\right). \tag{1.4}$$

Remarkably this bound is valid without any assumption on the distribution of Z.

In the case of CV QKD, the appropriate measure of correlation for a bipartite state ρ_{AB} is its averaged covariance matrix. If the measurement outcomes of Alice and Bob are modeled by 2 random variables $X = (X_1, \ldots, X_n)$ and $Y = (Y_1, \ldots, Y_n)$, we are specifically interested in their variances and covariance, namely $\frac{1}{n}\sum_{i=1}^n |X_i|^2$, $\frac{1}{n}\sum_{i=1}^n |Y_i|^2$ and $\frac{1}{n}\sum_{i=1}^n \langle X_i, Y_i\rangle$.

In other words, we are not concerned anymore with estimating the average of binary variables, but rather that of real variables. The problem we face is the following: given n real-valued random variables $Z = (Z_1, \ldots, Z_n)$, is it possible to devise a statistical test where we are allowed to look at a subset of the variables that will let us bound the average of the remaining variables, similarly as what is done in Theorem 1? To make matters worse, in the context of QKD, the protocol should always work which means that we are not allowed to make any assumption about the distribution of the Z_i.

It is easy to show that the strategy of Theorem 1 will fail, in the sense that the average computed over a subset of the variables will not give us any guarantee about the average over the remaining variables. A simple counter-example is as follows: the variables Z_i are distributed such as one of the n variables takes value A (which is unknown) while the remaining ones take value 0. In that case, sampling a random subset of k coordinates and computing the average will either give 0 or A/k, and in both cases, the result will incorrectly predict the average of the subset that was not observed, which is either A/m or 0. Note that if an upper bound on $|A|$ is available, then one can still make sure that the error equal to $\max(A/k, A/m)$ is small enough by increasing k and m, but without such a bound, it is impossible to know what values of k and m to take to guarantee an arbitrary small error. The problem results from the fact that the variables Z_i are not bounded *a priori*, and this is what makes the security statements for CV QKD more difficult to establish.

It should also be noted that restricting our attention to collective attacks, which means that the Z_i can be assumed to be i.i.d. random variables, does not help. In fact, while the literature on CV QKD often makes the statement that security against collective attacks was proven in [GPC06], [NGA06], it is not the case, precisely for the reason described above that estimating the covariance matrix of the state is a nontrivial task which was not addressed in those papers.

Fortunately, our problem has a solution: replace the random subset of coordinates used in Theorem 1 by a *random subspace*. Equivalently, given a vector $Z = (Z_1, \ldots, Z_n)$, first choose a random R chosen from the Haar measure on the orthogonal group $O(n)$, apply it to Z to get $Z' = RZ$ and measure the first k coordinates of Z'. Then, one can make a prediction about the average value of the remaining coordinates, which will be correct with high probability over the choice of random transformation $R \in O(n)$. In [Lev15], we proved this theorem in the case where Z in a complex vector instead of a real vector, but both cases work similarly.

Theorem 2. *Given a vector $X \in \mathbb{C}^{2n}$, consider Π the projector on a random subspace*

of dimension n, then for $\varepsilon \geq 2e^{-n/2}$,

$$\Pr\left[\frac{2\|\Pi X\|^2}{\|X\|^2} \geq \left[1+1.5\sqrt{\frac{\ln(2/\varepsilon)}{n}}\right]\right] \leq \varepsilon, \quad \Pr\left[\frac{2\|\Pi X\|^2}{\|X\|^2} \leq \left[1-2.2\sqrt{\frac{\ln(2\varepsilon)}{n}}\right]\right] \leq \varepsilon.$$

While the idea of picking a random unitary or orthogonal transformation is natural to make the parameter estimation possible, it is, however, computationally costly and we would like to avoid it in a real protocol. In the protocol description given in Table 1.1, a symmetrization step is explicitly included but a future goal would be to prove that this is in fact unnecessary. For this reason, it is important to be able to perform the parameter estimation without actively symmetrizing the data. A solution for this is developed in Ref. [Lev15]: the main idea is to perform error correction before parameter estimation, while the opposite order is usually preferred in QKD protocols. This can be done quite efficiently since a rough estimate of the signal-to-noise ratio (SNR) of the data is in general sufficient to choose an appropriate error correcting code and proceed with the reconciliation. The advantage is that once the error correction is finished, Alice knows both her and Bob's measurements results. She can therefore infer the variances and covariances for the whole set of data. She is then able to compute an upper bound on the probability of picking a unitary transformation that would lead to an incorrect prediction in the parameter estimation test.

More specifically, the CV QKD protocol of Table 1.1 admits 3 parameters $\Sigma_a^{\max}, \Sigma_b^{\max}$ and $\Sigma_c^{\min}$ corresponding respectively to the thresholds for the variance of Alice's measurements, the variance of Bob's measurements and a lower bound on the covariance. After the error correction is completed, Alice knows the values of $\|x\|^2, \|y\|^2$ and $\langle x, y\rangle$ and can compute $\gamma_a, \gamma_b, \gamma_c$ defined by

$$\gamma_a := \frac{1}{2n}\left[1+2\sqrt{\frac{\log(36/\varepsilon_{\mathrm{PE}})}{n}}\right]\|X\|^2 - 1, \tag{1.5}$$

$$\gamma_b := \frac{1}{2n}\left[1+2\sqrt{\frac{\log(36/\varepsilon_{\mathrm{PE}})}{n}}\right]\|Y\|^2 - 1 \tag{1.6}$$

$$\gamma_c := \frac{1}{2n}\langle X, Y\rangle - 5\sqrt{\frac{\log(8/\varepsilon_{\mathrm{PE}})}{n^3}}(\|X\|^2 + \|Y\|^2). \tag{1.7}$$

Here, $\varepsilon_{\mathrm{PE}}$ quantifies the probability that the energy test passes while making a wrong prediction about the conditional state of the remaining modes. The parameter estimation test is simply: if $[\gamma_a \leq \Sigma_a^{\max}] \wedge [\gamma_b \leq \Sigma_b^{\max}] \wedge [\gamma_c \geq \Sigma_c^{\min}]$, then ACCEPT, otherwise REJECT. The following theorem proven in [Lev15] gives an upper bound on the probability that the test passes and that the key produced by the protocol with parameters $\Sigma_a^{\max}, \Sigma_b^{\max}, \Sigma_c^{\min}$ is not secret.

Theorem 3. *The probability that the Parameter Estimation Test passes, that is, $[\gamma_a \leq \Sigma_a^{\max}] \wedge [\gamma_b \leq \Sigma_b^{\max}] \wedge [\gamma_c \geq \Sigma_c^{\min}]$ and that the Holevo information $\chi(\hat{v}; E)$ between the raw key and Eve's quantum system computed for the Gaussian state with covariance matrix characterized by $\Sigma_a^{\max}, \Sigma_b^{\max}$ and $\Sigma_c^{\min}$ is underestimated, is upper-bounded by $\varepsilon_{\mathrm{PE}}$.*

Note that for the Holevo information to be well defined, it is crucial that the quantum state has an i.i.d. structure. For this reason, the theorem above and the results of [Lev15] apply in the case of *collective attacks* only, and it will be the goal of the next sections to show that security against collective attacks is sufficient to imply security against general attacks (with a slightly worse security parameter).

For completeness, the Holevo information $\chi(\hat{v};E)$ mentioned in Theorem 3 can be upper bounded by $f(\Sigma_a^{\max},\Sigma_b^{\max},\Sigma_c^{\min}) := g((\nu_1-1)/2)+g((\nu_2-1)/2)-g((\nu_3-1)/2)$ where ν_1 and ν_2 are the symplectic eigenvalues of the covariance matrix $\begin{bmatrix} \Sigma_a^{\max}\mathbb{1}_2 & \Sigma_c^{\min}\sigma_z \\ \Sigma_c^{\min}\sigma_z & \Sigma_b^{\max}\mathbb{1}_2 \end{bmatrix}$, $\nu_3 = \Sigma_a^{\max} - \left(\Sigma_c^{\min}\right)^2/(1+\Sigma_b^{\max})$, $\sigma_z = \mathrm{diag}(1,-1)$ and $g(x) := (x+1)\log_2(x+1) - x\log_2(x)$. This is a standard result in the study of CV QKD protocols established in [GPC06] using the optimality of Gaussian states [WGC06].

The techniques presented in this section allow one to analyze the parameter estimation test of the CV QKD protocol of Table 1.1. This is the crucial step that was missing from Refs. [GPC06], [NGA06] and which gives a composable security proof of the protocol against collective attacks, that is when restricting the input states to states of the form $\sigma_{AB}^{\otimes n}$. Extending such a proof to take care of general attacks requires some de Finetti reduction. Such an approach was first successfully carried out in a work by Renner and Cirac [RC09], but gives bounds that scale poorly with n. In particular, they are too weak to prove that some secure keys can be distilled by exchanging a reasonable number of coherent states, say less than 10^9 or 10^{10}. For this, a better reduction is required and we will describe such a result in Section 1.5.

To conclude this section, let us also note that there exists a different approach to proving the security of a CV QKD protocol (different from that of Table 1.1) which bypasses security proofs against collective attacks altogether. The idea is to appeal to entropic uncertainty relations for smooth-entropies that have been developed both for discrete and continuous variables [TR11], [FFB+12], [FBT+14] (see [CBTW15] for a recent review on the topic). The main advantage of this approach is that it proves that secret keys can be distilled for reasonable block length. Unfortunately, the approach has two important drawbacks: first, the protocols require Alice to prepare and send squeezed states to Bob instead of coherent states, which make these protocols less appealing from a practical point of view; second, the key rate converges to a rate strictly smaller than the one conjectured from the optimality of Gaussian attacks.

1.4 Truncating the Fock space via an energy test

In order to use the Gaussian de Finetti reduction that will be described in Section 1.5, it is necessary to "truncate" the infinite-dimensional Fock space and replace it by a finite-dimensional Hilbert space. The Fock states that form an orthonormal basis of the Fock space are labelled by integers counting the number of photons present in each optical mode. In particular, Fock states with a large number of photons are highly energetic and unlikely to be observed in a CV QKD experiment. The main idea to achieve the truncation is to test a small number of modes and measure their energy. Provided that

the state has been adequately symmetrized (to ensure that the energy is well spread out across the modes), the energy of the measured modes will be a good indicator of the energy of the remaining modes. In particular, if that energy is sufficiently small, it means that the remaining quantum state can be well approximated by a quantum state living in a reasonably small Hilbert space (spanned by the "lowest" Fock states). This is the idea behind our energy test.

It will be useful to introduce a notation for the various Fock spaces that will appear in the following. Let $F_{1,1,n}$ represent the Fock space corresponding to a total of $2n$ modes, n of which being held by Alice, and the remaining modes being held by Bob. Similarly, $F_{1,1,n+k}$ corresponds to a $2(n+k)$-mode Fock space. The meaning of the 1s will become clearer in the next section, but we don't need it here. Finally, we define $F_{1,1,n}^{\leq K}$ to be the finite-dimensional subspace of $F_{1,1,n}$ spanned by Fock states with at most K photons in total. We have:

$$F_{1,1,n} := \mathrm{Span}\Big\{|i_1,\ldots,i_n;j_1,\ldots,j_n\rangle \ : \ i_1,\ldots,i_n,j_1,\ldots,j_n \in \mathbb{N}\Big\}$$

$$F_{1,1,n}^{\leq K} := \mathrm{Span}\Big\{|i_1,\ldots,i_n;j_1,\ldots,j_n\rangle \ : \ i_1,\ldots,i_n,j_1,\ldots,j_n \in \mathbb{N}, \sum_{k=1}^{n} i_k + j_k \leq K\Big\}.$$

Following the results of the previous section, let us suppose that our CV QKD protocol of interest, $\mathcal{E}_0$, is secure against Gaussian collective attacks. Recall that $\mathcal{E}_0$ takes as input states on $F_{1,1,n}$. We will slightly modify the protocol by prepending an initial test $\mathcal{T}$. More precisely, $\mathcal{T}$ is a CP map taking a state in the slightly larger Hilbert space $F_{1,1,n+k}$, applying a randomization of this state (corresponding to processing the modes with a random linear optical network of beamsplitters and phaseshifters), measuring the last k modes and comparing the measurement outcome to a threshold fixed in advance. The test succeeds if the measurement outcome (related to the energy) is small, meaning that the global state is compatible with a state containing only a low number of photons per mode. Such a state is well-described in a low dimensional Hilbert space, as we will discuss below. Depending on the outcome of the test, either the protocol aborts, or one applies the original protocol $\mathcal{E}_0$ on the n remaining modes.

For the test to be practical, it is important that the legitimate parties do not have to physically implement the transformation corresponding to the optical network (which is parameterized by a unitary $u \in U(n+k)$). Rather, they can both measure their $n+k$ modes with heterodyne detection, perform a random rotation of their respective classical vector in $\mathbb{R}^{2(n+k)}$ according to $u \in U(n+k) \cong O(2(n+k)) \cap Sp(2(n+k))$.

Let us denote by $\mathcal{P}(\mathcal{H})$ the set of nonnegative operators on $\mathcal{H}$. We introduce the following maps:

$$\begin{aligned}
&\mathcal{T} : \mathcal{P}(F_{1,1,n+k}) \to \mathcal{P}(F_{1,1,n}) \otimes \{\text{passes/aborts}\},\\
&\mathcal{P} : \mathcal{P}(F_{1,1,n}) \to \mathcal{P}(F_{1,1,n}^{\leq K}),\\
&\mathcal{R} : \{0,1\}^{\ell} \times \{0,1\}^{\ell} \to \{0,1\}^{\ell'} \times \{0,1\}^{\ell'},
\end{aligned}$$

where

- the energy test $\mathcal{T}(k, d_A, d_B)$ takes as input an arbitrary state ρ_{AB} on $F_{1,1,n+k}$, maps it to $W_u \rho_{AB} W_u^\dagger$ where the unitary u is chosen from the Haar measure on $U(n+k)$ and W_u is the corresponding unitary acting on $F_{1,1,n+k}$ (which transforms the $(n+k)$ creation operators of Alice's modes according to the unitary u and the $(n+k)$ creation operators of Bob's modes according to its complex conjugate $\overline{u}$), measures the last k modes for A and B with heterodyne detection and check whether the measurement outputs pass the test, that is whether the k outcomes $\alpha_1, \cdots, \alpha_k$ of Alice and $\beta_1, \cdots, \beta_k$ of Bob satisfy

$$\sum_{i=1}^{k} |\alpha_i|^2 \leq k d_A \quad \text{and} \quad \sum_{i=1}^{k} |\beta_i|^2 \leq k d_B.$$

  If they pass the test, the map returns the state on the first n modes (that were not measured) as well as the flag "passes". Otherwise, it returns the flag "aborts".

- $\mathcal{P}^{\leq K}$ is a map projecting the input state onto the finite-dimensional subspace $F_{1,1,n}^{\leq K}$ (corresponding to states with at most K photons in the $2n$ modes): it maps any density matrix $\rho \in \mathcal{P}(F_{1,1,n})$ to $\Pi^{\leq K} \rho \Pi^{\leq K} \in \mathcal{P}(F_{1,1,n}^{\leq K})$, where $\Pi^{\leq K}$ is the orthogonal projector onto $F_{1,1,n}^{\leq K}$. This trace non-increasing map is introduced as a technical tool for the security analysis but need not be implemented in practice. It simply ensures that the states that are fed to the original QKD protocol $\mathcal{E}_0$ live in a finite-dimensional subspace. In the text, we will alternatively denote this projection by $\mathcal{P}^{\leq K}$ or $\mathcal{P}(n, K)$, depending on which parameters we wish to make explicit.

- $\mathcal{R}$ is a classical map that takes two ℓ-bit strings as input and returns ℓ'-bit strings (for $\ell' < \ell$). It corresponds to an additional privacy amplification procedure, compared to the original protocol $\mathcal{E}_0$, needed to ensure the security of $\mathcal{E}$ against general attacks.

We finally define our CV QKD protocol $\mathcal{E}$ as

$$\mathcal{E} = \mathcal{R} \circ \mathcal{E}_0 \circ \mathcal{T}$$

and the ideal protocol as $\mathcal{F} = \mathcal{S} \circ \mathcal{E}$.

The following result was obtained in [Lev17].

Theorem 4. *Let $\overline{\mathcal{E}}$ be the protocol $\mathcal{R} \circ \mathcal{E}_0 \circ \mathcal{P}$. Then the security of $\overline{\mathcal{E}}$ implies the security of $\mathcal{E}$:*

$$||\mathcal{E} - \mathcal{F}||_\diamond \leq ||\overline{\mathcal{E}} - \overline{\mathcal{F}}||_\diamond + 2||(\mathbb{1} - \mathcal{P}) \circ \mathcal{T}||_\diamond, \tag{1.8}$$

provided that the quantity $||(\mathbb{1} - \mathcal{P}) \circ \mathcal{T}||_\diamond$ can be made arbitrarily small.

The term $||\overline{\mathcal{E}} - \overline{\mathcal{F}}||_\diamond$ will be addressed in Section 1.5, where we will explain how to obtain a tight upper bound by replacing the supremum of Eq. (1.2) by a supremum over a restricted class of Gaussian i.i.d. states. The second term, $||(\mathbb{1} - \mathcal{P}) \circ \mathcal{T}||_\diamond$, corresponds to the failure probability of the energy test and can be bounded using the following theorem that was proven in [Lev17].

Theorem 5. *For integers $n, k \geq 1$, and $d_A, d_B > 0$, define $K = n(d'_A + d'_B)$ for $d'_{A/B} = d_{A/B} g(n, k, \varepsilon/4)$ for the function g defined in Eq. (1.9). Then*

$$\left\| \left(\mathbb{1} - \mathcal{P}(n, K)\right) \circ \mathcal{T}(k, d_A, d_B) \right\|_\diamond \leq \varepsilon.$$

Establishing Theorem 5 requires two main ingredients: the operator inequality of Lemma 6 below and concentration bounds for the χ^2 distribution which yield Lemma 7. For $d > 0$, let us introduce the following operators on an n-mode Fock space:

$$T_n^d := \frac{1}{\pi^n} \int_{\sum_{i=1}^n |\alpha_i|^2 \geq nd} |\alpha_1\rangle\langle\alpha_1| \otimes \ldots \otimes |\alpha_n\rangle\langle\alpha_n| \mathrm{d}\alpha_1 \ldots \alpha_n$$

$$U_n^d := \sum_{m=nd+1}^{\infty} \Pi_m^n,$$

where Π_m^n is the projector onto the finite dimensional Hilbert space spanned by Fock states containing m photons:

$$\Pi_m^n = \sum_{m_1 + \ldots + m_n = m} |m_1, \ldots, m_n\rangle\langle m_1, \ldots, m_n|.$$

In words, T_n^d is the sum of the projectors onto products of coherent states such that the total squared amplitude is greater than nd and U_n^d is the projector onto Fock states containing more that nd photons. Intuitively, both operators should be "close" to each other. This is formalized with the following lemma that was proven in [LGPRC13].

Lemma 6. *For any integer n and any $d \geq 0$, it holds that*

$$U_n^d \leq 2 T_n^d.$$

An n-mode state is called "rotationally invariant" if it is invariant when being processed by any linear optical network consisting of beamsplitters and phase shifters. This is for instance the case of the states that are obtained after the symmetrization procedure that we described in Section 1.2 and we will study these invariant states in more detail in Section 1.5 since they are relevant in the context of de Finetti theorems. For such states, one expects that the energy is spread evenly among the different optical modes. This is formalized in the following lemma that was established in [Lev17].

Lemma 7. *Let ρ be an rotationally invariant state on $\mathcal{H}^{\otimes(n+k)}$. Then, for any $d > 0$,*

$$tr\left[(T_n^{d'} \otimes (\mathbb{1} - T_k^d)) \rho \right] \leq \varepsilon,$$

for $d' = g(n, k, \varepsilon) d$ and

$$g(n, k, \varepsilon) = \frac{1 + 2\sqrt{\frac{\ln(2/\varepsilon)}{2n}} + \frac{\ln(2/\varepsilon)}{n}}{1 - 2\sqrt{\frac{\ln(2/\varepsilon)}{2k}}}. \tag{1.9}$$

The only missing step in the security reduction is therefore a way to obtain an upper bound on $||\overline{\mathcal{E}} - \overline{\mathcal{F}}||_\diamond$. This is the object of the next section.

1.5 $SU(2,2)$ coherent states and Gaussian de Finetti reductions

Despite their wide range of application, there is a regime where "standard" de Finetti theorems fail, namely when the local dimension is not negligible compared to the number n of subsystems [CKMR07]. In particular, these techniques do not apply directly to CV protocols where the local spaces are infinite-dimensional Fock spaces. In this work, we consider a natural symmetry displayed by some important CV QKD protocols, which are invariant under the action of beamsplitters and phase-shifts on their n modes [LKGC09]. For such protocols, one legitimately expects that stronger versions of de Finetti theorems should hold. In particular, a widely held belief that it is enough to consider *Gaussian* i.i.d. input states instead of all i.i.d. states in order to analyze the security of the corresponding protocol.

We prove this statement rigorously here. Our main tool is a family of $SU(2,2)$ generalized coherent states that resolve the identity of the subspace spanned by states invariant under the action of $U(n)$. This implies that for some applications such as QKD, it is sufficient to consider the behaviour of the protocol for these states in order to obtain guarantees that hold for arbitrary input states.

In this section, we discuss our results from Ref. [Lev16] and define $SU(2,2)$ coherent states. Such states allow us to prove a Gaussian de Finetti reduction which in turn provides an upper bound on $||\overline{\mathcal{E}} - \overline{\mathcal{F}}||_\diamond$ that can be computed if the protocol $\mathcal{E}_0$ is secure against Gaussian collective attacks, meaning that the CV QKD protocol $\mathcal{E}_0$ is secure when its input is restricted to Gaussian i.i.d. states (instead of arbitrary states on $F_{1,1,n}$).

1.5.1 The symmetric subspace $F_{2,2,n}^{U(n)}$

Let $H_A \cong H_B \cong H_{A'} \cong H_{B'} \cong \mathbb{C}^n$ and define the Fock space $F_{2,2,n}$ as

$$F_{2,2,n} := \bigoplus_{k=0}^{\infty} \mathrm{Sym}^k(H_A \otimes H_B \otimes H_{A'} \otimes H_{B'}),$$

where $\mathrm{Sym}^k(H)$ is the symmetric part of $H^{\otimes k}$. Hopefully the notation $F_{1,1,n}$ that we introduced in the previous section becomes a little bit clearer here. Indeed, $F_{1,1,n} = \bigoplus_{k=0}^{\infty} \mathrm{Sym}^k(H_A \otimes H_B)$, and any mixed state on $F_{1,1,n}$ admits a purification in $F_{2,2,n}$.

Using the Segal-Bargmann representation, the Hilbert space $F_{2,2,n}$ is realized as a functional space of complex holomorphic functions square-integrable with respect to the Gaussian measure, $F_{2,2,n} \cong L^2_{\mathrm{hol}}(\mathbb{C}^{4n}, \|\cdot\|)$, and a state $\psi \in F_{2,2,n}$ represented by a holomorphic function $\psi(z,z')$ with $z \in \mathbb{C}^{2n}, z' \in \mathbb{C}^{2n}$ satisfying

$$\|\psi\|^2 := \langle \psi, \psi \rangle = \frac{1}{\pi^{4n}} \int \exp(-|z|^2 - |z'|^2) |\psi(z,z')|^2 \mathrm{d}z \mathrm{d}z' < \infty \tag{1.10}$$

where $\mathrm{d}z := \prod_{k=1}^{n} \prod_{i=1}^{2} \mathrm{d}z_{k,i}$ and $\mathrm{d}z' := \prod_{k=1}^{n} \prod_{j=1}^{2} \mathrm{d}z'_{k,j}$ denote the Lebesgue measures on $\mathbb{C}^{2n}$ and $\mathbb{C}^{2n}$, respectively, and $|z|^2 := \sum_{k=1}^{n} \sum_{i=1}^{2} |z_{k,i}|^2, |z'|^2 := \sum_{k=1}^{n} \sum_{j=1}^{2} |z'_{k,j}|^2$.

A state $\psi \in F_{2,2,n}$ therefore corresponds to a holomorphic function of $4n$ complex variables $(z_{1,1}, z_{n,1}; z_{1,2}, \dots, z_{n,2}; z'_{1,1}, \dots, z'_{n,1}; z'_{1,2}, \dots, z'_{n,2})$. For conciseness, we denote by z_i and z'_j the vectors $(z_{1,i}, \dots, z_{n,i})$ and $(z'_{1,j}, \dots, z'_{n,j})$, respectively, for $i, j \in \{1, 2\}$. With these notations, the vector z_1 is associated to the space H_A, the vector z'_1 to H_B, the vector z_2 to H'_B and the vector z'_2 to H'_A.

Formally, one can switch from the Segal-Bargmann representation to the representation in terms of annihihation and creation operators by replacing the variables $z_{k,1}$ by $a_k^\dagger$, $z_{k,2}$ by $b_k'^\dagger$, $z'_{k,1}$ by $b_k^\dagger$ and $z'_{k,2}$ by $a_k'^\dagger$. The function $f(z, z')$ is therefore replaced by an operator $f(a^\dagger, b^\dagger, a'^\dagger, b'^\dagger)$ and the corresponding state in the Fock basis is obtained by applying this operator to the vacuum state.

The *metaplectic* representation of the unitary group $U(n) \subset Sp(2n, \mathbb{R})$ on $F_{2,2,n}$ associates to $u \in U(n)$ the operator W_u performing the change of variables $z \to uz$, $z' \to \overline{u}z'$:

$$U(n) \to \mathrm{End}(F_{2,2,n}) \tag{1.11}$$

$$u \mapsto W_u = \left[\psi(z_1, z_2, z'_1, z'_2) \mapsto \psi(uz_1, uz_2, \overline{u}z'_1, \overline{u}z'_2)\right] \tag{1.12}$$

where $\overline{u}$ denotes the complex conjugate of the unitary matrix u. In other words, the unitary u is applied to the modes of $F_A \otimes F_{B'}$ and its complex conjugate is applied to those of $F_B \otimes F_{A'}$. This representation can be extended to the Fock space $F_{p,q,n}$ for arbitrary integers p and q: in that case the unitary u is applied to the first p sets of n modes, while $\overline{u}$ is applied to the remaining q sets of n modes.

The states that are left invariant under the action of the unitary group $U(n)$ are relevant for instance in the context of CV QKD, and we define the symmetric subspace as the space spanned by such invariant states.

Definition 8 (Symmetric subspace)**.** *For integer $n \geq 1$, the* symmetric subspace $F_{2,2,n}^{U(n)}$ *is the subspace of functions $\psi \in F_{2,2,n}$ such that*

$$W_u \psi = \psi \quad \forall u \in U(n),$$

where W_u is defined in Eq. (1.12).

The name *symmetric subspace* is inspired by the name given to the subspace $\mathrm{Sym}^n(\mathbb{C}^d)$ of $(\mathbb{C}^d)^{\otimes n}$ of states invariant under permutation of the subsystems:

$$\mathrm{Sym}^n(\mathbb{C}^d) := \left\{|\psi\rangle \in (\mathbb{C}^d)^{\otimes n} \ : \ P(\pi)|\psi\rangle = |\psi\rangle, \forall \pi \in S_n\right\} \tag{1.13}$$

where $\pi \mapsto P(\pi)$ is a representation of the permutation group S_n on $(\mathbb{C}^d)^{\otimes n}$ and $P(\pi)$ is the operator that permutes the n factors of the state according to $\pi \in S_n$. See for instance [Har13] for a recent exposition of the symmetric subspace from a quantum information perspective.

In [Lev16], a full characterization of the symmetric subspace $F_{2,2,n}^{U(n)}$ is given. It is helpful to introduce the four operators $Z_{11}, Z_{12}, Z_{21}, Z_{22}$ defined by:

$$Z_{11} = \sum_{i=1}^{n} z_{i,1} z'_{i,1} \quad \leftrightarrow \quad \sum_{i=1}^{n} a_i^\dagger b_i^\dagger, \qquad Z_{12} = \sum_{i=1}^{n} z_{i,1} z'_{i,2} \quad \leftrightarrow \quad \sum_{i=1}^{n} a_i^\dagger a_i'^\dagger,$$
$$Z_{21} = \sum_{i=1}^{n} z_{i,2} z'_{i,1} \quad \leftrightarrow \quad \sum_{i=1}^{n} b_i^\dagger b_i'^\dagger, \qquad Z_{22} = \sum_{i=1}^{n} z_{i,2} z'_{i,2} \quad \leftrightarrow \quad \sum_{i=1}^{n} a_i'^\dagger b_i'^\dagger.$$

For instance, the operator Z_{11} can be thought of as the coherent addition of a photon in one of Alice's n modes and a photon in Bob's corresponding mode.

Definition 9. *For integer $n \geq 1$, let $E_{2,2,n}$ be the space of analytic functions ψ of the 4 variables $Z_{1,1}, \ldots, Z_{2,2}$, satisfying $\|\psi\|_E^2 < \infty$, that is $E_{2,2,n} = L^2_{\mathrm{hol}}(\mathbb{C}^{pq}, \|\cdot\|_E)$, where $\|\cdot\|_E$ is the norm induced by the norm on $F_{2,2,n}$.*

In [Lev16], is was proven that $E_{2,2,n}$ coincides with the symmetric subspace $F_{2,2,n}^{U(n)}$.

Theorem 10. *For $n \geq 2$, the symmetric subspace $F_{2,2,n}^{U(n)}$ is isomorphic to $E_{2,2,n}$.*

In other words, any state in the symmetric subspace can be written as

$$|\psi\rangle = f\Big(\sum_{i=1}^{n} a_i^\dagger b_i^\dagger, \sum_{i=1}^{n} a_i^\dagger a_i'^\dagger, \sum_{i=1}^{n} b_i^\dagger b_i'^\dagger, \sum_{i=1}^{n} a_i'^\dagger b_i'^\dagger\Big)|\text{vacuum}\rangle$$

for some holomorphic function f. Said otherwise, such a state is characterized by only 4 parameters instead of $4n$ for an arbitrary state in $F_{2,2,n}$; or else, the symmetric subspace is isomorphic to a 4-mode Fock space (with "creation" operators corresponding to $Z_{11}, Z_{12}, Z_{21}, Z_{22}$), instead of the ambient $4n$-mode Fock space.

1.5.2 Coherent states for $SU(2,2)/SU(2) \times SU(2) \times U(1)$

In this section, we first review a construction due to Perelomov that associates a family of generalized coherent states to general Lie groups [Per72], [Per86] and then apply it to the pseudo-unitary group $SU(2,2)$. In this language, the standard Glauber coherent states are associated with the Heisenberg-Weyl group, while the atomic spin coherent states are associated with $SU(2)$. A consequence of Theorem 10 is that symmetric subspace $F_{2,2,n}^{U(n)}$ is spanned by $SU(2,2)$ coherent states, where $SU(2,2)$ is the special unitary group of signature $(2,2)$ over $\mathbb{C}$:

$$SU(2,2) := \Big\{ A \in M_4(\mathbb{C}) \ : \ A \mathbb{1}_{2,2} A^\dagger = \mathbb{1}_{2,2} \Big\} \tag{1.14}$$

where $M_4(\mathbb{C})$ is the set of 4×4-complex matrices and $\mathbb{1}_{2,2} = \mathbb{1}_2 \oplus (-\mathbb{1}_2)$.

In Perelomov's construction, a *system of coherent states of type* $(T, |\psi_0\rangle)$ where T is the representation of some group G acting on some Hilbert space $\mathcal{H} \ni |\psi_0\rangle$, is the set

of states $\{|\psi_g\rangle \,:\, |\psi_g\rangle = T_g|\psi_0\rangle\}$ where g runs over all the group G. One defines H, the *stationary subgroup* of $|\psi_0\rangle$ as

$$H := \{g \in G \,:\, T_g|\psi_0\rangle = \alpha|\psi_0\rangle \text{ for } |\alpha| = 1\},$$

that is the group of $h \in G$ such that $|\psi_h\rangle$ and $|\psi_0\rangle$ differ only by a phase factor. When G is a connected noncompact simple Lie group, H is the maximal compact subgroup of G. In particular, for $G = SU(2,2)$, one has $H = SU(2,2) \cap U(4) = SU(2) \times SU(2) \times U(1)$ and the factor space G/H corresponds to a Hermitian symmetric space of classical type (see *e.g.* Chapter X of [Hel79]). The generalized coherent states are parameterized by points in G/H. For $G/H = SU(2,2)/SU(2) \times SU(2) \times U(1)$, the factor space is the set $\mathbb{D}$ of 2×2 matrices Λ such that $\Lambda\Lambda^\dagger < \mathbb{1}_p$, *i.e.*, the singular values of Λ are strictly less than 1.

$$\mathbb{D} = \left\{\Lambda \in M_2(\mathbb{C}) \,:\, \mathbb{1}_2 - \Lambda\Lambda^\dagger > 0\right\},$$

where $A > 0$ for a Hermitian matrix A means that A is positive definite.

We are now ready to define our coherent states for the noncompact Lie group $SU(2,2)$.

Definition 11 ($SU(2,2)$ coherent states)**.** *For $n \geq 1$, the coherent state $\psi_{\Lambda,n}$ associated with $\Lambda \in \mathbb{D}$ is given by*

$$\psi_{\Lambda,n}(Z_{1,1}, \ldots, Z_{2,2}) = \det(1 - \Lambda\Lambda^\dagger)^{n/2} \det \exp\Big(\sum_{i,j=1}^{2} \Lambda_{i,j} Z_{ij}\Big).$$

In the following, we will sometimes abuse notation and write ψ_Λ instead of $\psi_{\Lambda,n}$, when the parameter n is clear from context.

We note that the coherent states have a tensor product form in the sense that

$$\psi_{\Lambda,n} = \psi_{\Lambda,1}^{\otimes n}.$$

We will also write $|\Lambda, n\rangle = |\Lambda, 1\rangle^{\otimes n}$ for $\psi_{\Lambda,n}$. Such a state is called *identically and independently distributed* (i.i.d.) in the quantum information literature. Moreover, the $SU(2,2)$ generalized coherent states are Gaussian states in the sense that their Wigner function is Gaussian. This means that they are entirely characterized by their first two moments, which makes them very appealing for theoretical study [WLB+04].

The main feature of a family of coherent states is that they resolve the identity. This is the case with the $SU(2,2)$ coherent states introduced above: see Ref. [Lev16].

Theorem 12 (Resolution of the identity)**.** *For $n \geq 4$, the $SU(2,2)$ generalized coherent states resolve the identity over the symmetric subspace $F_{2,2,n}^{U(n)}$:*

$$\int_{\mathbb{D}} |\Lambda, n\rangle\langle\Lambda, n| \mathrm{d}\mu_n(\Lambda) = \mathbb{1}_{F_{2,2,n}^{U(n)}}, \tag{1.15}$$

where $\mathrm{d}\mu_n(\Lambda)$ *is the invariant measure on* $\mathbb{D}$ *given by*

$$\mathrm{d}\mu_n(\Lambda) = \frac{(n-1)(n-2)^2(n-3)}{\pi^4 \det(\mathbb{1}_2 - \Lambda\Lambda^\dagger)^4} \prod_{i=1}^{2}\prod_{j=1}^{2} \mathrm{d}\Re(\Lambda_{i,j})\mathrm{d}\Im(\Lambda_{i,j}), \tag{1.16}$$

where $\Re(\Lambda_{i,j})$ *and* $\Im(\Lambda_{i,j})$ *refer respectively to the real and imaginary parts of* $\Lambda_{i,j}$*. This operator equality is to be understood for the weak operator topology.*

The main work of Ref. [Lev17], besides the analysis of the energy test mentioned in the previous section, is to derive a finite-energy version of the resolution of the identity above.

Since the space $F_{2,2,n}^{U(n)}$ is infinite-dimensional, the integral of Eq. (1.15) is not normalizable. In order to obtain an operator with finite norm, we consider the finite-dimensional subspace $F_{2,2,n}^{U(n),\leq K}$ of $F_{2,2,n}^{U(n)}$ spanned by states with less than K "excitations":

$$\mathrm{Span}\left\{ (Z_{11})^i (Z_{12})^j (Z_{21})^k (Z_{22})^\ell |\mathrm{vac}\rangle \ : \ i+j+k+\ell \leq K \right\}.$$

We showed in [Lev17] that an approximate resolution of the identity still holds for this space when restricting the coherent states $|\Lambda, n\rangle$ to $\Lambda \in \mathcal{D}_\eta$ for $\mathcal{D}_\eta = \left\{ \Lambda \in \mathcal{D} \ : \ \eta\mathbb{1}_2 - \Lambda\Lambda^\dagger \succeq 0 \right\}$ for $\eta \in [0,1[$. Let us denote by $\Pi_{\leq K}$ the identity onto the subspace $F_{2,2,n}^{U(n),\leq K}$ (note that this operator differs from $\Pi^{\leq K}$ that was considered in the previous section) and introduce the relative entropy $D(x||y) = x\log\frac{x}{y} + (1-x)\log\frac{1-x}{1-y}$.

Theorem 13. *For* $n \geq 5$ *and* $\eta \in [0,1[$*, if* $K \leq \frac{\eta N}{1-\eta}$ *for* $N = n-5$*, then the operator inequality*

$$\int_{\mathcal{D}_\eta} |\Lambda, n\rangle\langle\Lambda, n| \mathrm{d}\mu_n(\Lambda) \geq (1-\varepsilon)\Pi_{\leq K} \tag{1.17}$$

holds with $\varepsilon = 2N^4(1+K/N)^7 \exp\left(-ND\left(\frac{K}{K+N}\middle\|\eta\right)\right)$.

Combining Theorem 13 together with the approach of Christandl, König and Renner [CKR09], one can finally obtain an upper bound on $||\overline{\mathcal{E}} - \overline{\mathcal{F}}||_\diamond$, provided that we know how $\mathcal{E}_0$ behaves for $SU(2,2)$ generalized coherent state inputs.

1.5.3 Concluding the security proof of the CV QKD protocol $\mathcal{E}$

The second term in the right hand side of Eq. (1.8) is finally taken care of by the following Gaussian de Finetti reduction, which was proven in [Lev17].

Theorem 14. *With the previous notations, if* $\mathcal{E}_0$ *is* ε*-secure against Gaussian collective attacks, then*

$$||\overline{\mathcal{E}} - \overline{\mathcal{F}}||_\diamond \leq 2T(n,\eta)\varepsilon$$

where $T(n,\eta) = (n-1)(n-2)^2(n-3)\frac{\eta^4}{12(1-\eta)^4}$ *and* $\overline{\mathcal{E}} = \mathcal{R}\circ\mathcal{E}_0\circ\mathcal{P}^{\leq K}$.

Putting everything together establishes our security reduction.

Theorem 15. *If the protocol $\mathcal{E}_0$ is ε-secure against Gaussian collective attacks, then the protocol $\mathcal{E} = \mathcal{R} \circ \mathcal{E}_0 \circ \mathcal{P}$ is ε'-secure against general attacks with*

$$\varepsilon' \leq \frac{K^4}{50}\varepsilon$$

for $n \geq 38$ and $K \geq n - 5$.

The security against collective attacks (and therefore also against Gaussian collective attacks) has been worked out in details in [Lev15] and follows essentially from the analysis of the parameter estimation procedure discussed in Section 1.3. In particular, one can choose ε to be exponentially small in n in Theorem 15 at the price of slightly reducing the key rate compared to the asymptotic key rate computed for $\mathcal{E}_0$ against Gaussian attacks. The Gaussian de Finetti reduction of Theorem 15 then implies the security of the protocol $\mathcal{E} = \mathcal{R} \circ \mathcal{E}_0 \circ \mathcal{T}$ against arbitrary attacks.

Chapter 2

Quantum non-locality and applications to cryptography

This chapter is concerned with several topics that revolve around the concept of quantum correlations, which correspond to the conditional probability distributions that can be observed when several agents perform measurements on a multipartite quantum system. In Section 2.1, we present a general framework to describe non-locality (and more generally to contextuality) based on an original idea of Tobias Fritz and extensively developed in [AFLS15] together with Antonio Acín, Tobias Fritz and Ana-Belén Sainz. In Section 2.2, we explain how the strengthening of the non-signaling principle, namely the fact that information cannot travel faster than the speed of light, can be exploited in a cryptographic context: in particular, it allows for informationally-secure bit commitment. These results, which belong to the nascent field of "relativistic cryptography", were obtained in collaboration with André Chailloux and Kaushik Chakraborty. In Section 2.3, we consider quantum protocols for position-verification. While information-theoretic security cannot be achieved for this task, the best known attacks often require an exponential amount of entanglement. In a work with Kaushik Chakraborty, we proposed general classes of attacks that only require polynomial resources. The connection with nonlocality it that cheating strategies can be interpreted as winning strategies for a special kind of nonlocal games where the inputs are allowed to be quantum states.

2.1 A combinatorial approach to contextuality and non-locality

We introduce a framework to describe probabilistic models in Bell experiments, and more generally in *contextuality scenarios*. Such a scenario is described by a hypergraph whose vertices represent elementary events and hyperedges correspond to measurements, and a probabilistic model associates to each event a probability, in such a way that events in a given measurement have a total probability equal to one. We discuss the advantages of this framework, most notably, it unifies the notions of contexuality and non-locality,

and give a short overview of the results presented in Ref. [AFLS15].

The main goal of physics is to understand how Nature works, and usually physicists proceed as follows: first, observe a phenomenon, then propose a model that explains it, and finally, confront the predictions of the model to experimental data. Repeat until the experimental results match the theoretical predictions. In some situations, however, it can be fruitful to limit the model to a minimum. This idea was recently investigated in the paradigm of *device-independence* [BCP+13]. There, an experimenter has access to a physical device with classical commands $x \in \mathcal{X}$ and classical results $a \in \mathcal{A}$ and chooses not to model the inner workings of the device any further. This might seem futile at first sight because how can one hope to say anything meaningful when only observing conditional probabilities of the form $P(a|x)$, corresponding to the probability of obtaining outcome a when applying command (or measurement) x? The key is to consider n physical devices accessed in a space-like separated way by n experimenters. Then, one has access to the conditional probability distribution $P(a_1, \ldots, a_n|x_1, \ldots, x_n)$ where a_i and x_i refer to the outcomes and measurements of the i^{th} party, where the no-signaling principle constrains P non-trivially. Stronger restrictions can be imposed by requiring the devices to be compatible with quantum theory, or even to be classical. In this section, we describe the framework of [AFLS15] allowing to describe such *Bell-type* scenarios in a very general way, and that extends naturally to contextuality scenarios.

2.1.1 Contextuality scenarios

We define a *contextuality scenario* to be a hypergraph $H = (V, E)$ whose vertices $v \in V$ correspond to the events of the scenario, and the (hyper-)edges $e = \{v_1, \cdots, v_k\} \in E$ are subsets of V that should be thought of as the measurements of the scenario. We demand in addition that all the vertices belong to at least one edge, and that no edge is strictly contained in another one. Such scenarios have been studied before in quantum logic where there are known as "test spaces" [Wil09]. A *probabilistic model* on the scenario H is then given by an assignment $p : V \to [0, 1]$ of a probability $p(v)$ to each event $v \in V$ satisfying the normalization condition: $\sum_{v \in e} p(v) = 1$ for each measurement $e \in E$. Let us denote by $\mathcal{G}(H) \subseteq [0, 1]^{|V|}$ the set of probabilistic models for the scenario H. By construction, this set is a polytope, the set of "states on test spaces" in the terminology of test spaces. Let us note that this approach was inspired by the framework developed in [CSW10] (see also [CSW14]), but that a crucial difference between the two works is that we explicitly work with normalized probability distributions, instead of subnormalized ones.

2.1.2 Bell-type scenarios

An important application of this framework concerns Bell-type scenarios where n parties have access to n distinct devices. For simplicity, we restrict ourselves to the scenario $\mathcal{B}_{n,m,k}$ where the n devices all have m different settings and k possible outcomes. In particular, $\mathcal{B}_{2,2,2}$ will correspond to the usual CHSH scenario. We now wish to describe the hypergraph $\mathcal{B}_{n,m,k}$. Its vertices are the $(mk)^n$ events of the form $(a_1, \ldots, a_n|x_1, \ldots, x_n)$.

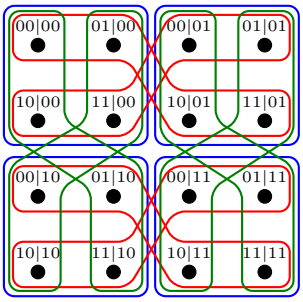

Figure 2.1 – The 16 events and 12 measurements of the CHSH scenario, $\mathcal{B}_{2,2,2}$

The trickier part is to characterize the measurements of the scenario. Usually, one would define a measurement to be the set of events of the form $(\cdot|x_1, \cdots, x_n)$. But our framework includes additional measurements: a measurement in the scenario $\mathcal{B}_{n,m,k}$ corresponds to any strategy applied by the n parties, *possibly coming together*, where each of the parties measures their device. More specifically, a measurement of $\mathcal{B}_{n,m,k}$ is given by a temporal ordering of the parties: $i_1 \leq i_2 \leq \ldots \leq i_n$ where party i_1 first chooses a measurement setting x_{i_1} and obtains an outcome a_{i_1}. Then, party i_2 chooses a setting x_{i_2}, possibly depending on x_{i_1} and a_{i_1}, and obtains an outcome a_{i_2}. This process is repeated until the last party performs their measurement. Note that the strategy can be adaptive, meaning that party i_k can choose their measurement setting to be a function of $a_{i_1}, x_{i_1}, \ldots, a_{i_{k-1}}, x_{i_{k-1}}$. The scenario obtained this way is displayed on Fig. 2.1 in the case of $\mathcal{B}_{2,2,2}$.

The main advantage of defining $\mathcal{B}_{n,m,k}$ as above is that $\mathcal{G}(\mathcal{B}_{n,m,k})$ is exactly the standard no-signaling polytope $\mathcal{NS}(\mathcal{B}_{n,m,k})$, defined as correlations satisfying

$$\sum_{a_{i+1}\ldots a_n} p(a_1, \ldots, a_n|x_1, \ldots, x_n) = p(a_1, \ldots, a_i|x_1, \ldots, x_i)$$

for any splitting of the n parties into two groups. The proof is straightforward (see [AFLS15] for details) and we only give the intuition in the case of $\mathcal{B}_{2,2,2}$ here. We wish to show that the normalization of the edges (*i.e.*, the total probability of the events in a given measurement should be 1) is equivalent to the no-signaling condition. A typical no-signaling condition for CHSH reads: $p(00|00)+p(01|00) = p(00|01)+p(01|01)$ (corresponding to the first row on Fig. 2.1). This can be derived from the normalization of the measurement "00" consisting of events of the form $(\cdot|00)$ and implying that $p(00|00) + p(01|00) = 1 - p(10|00) - p(11|00)$ and of the event $\{(10|00), (11|00), (00|01), (01|01)\}$ implying that $p(00|01)+p(01|01)$ is also equal to $1-p(10|00)-p(11|00)$. Hence, normalization implies no-signaling and the converse property can also be checked in the same fashion.

2.1.3 Classical and quantum models

There are two natural restrictions that one might want to impose on the devices: either a classical, or a quantum nature, leading respectively to the notions of *classical* and *quantum* probabilistic models. First, a *deterministic* model on H is a probabilistic model (hence satisfying normalization) such that $p(v) \in \{0, 1\}$ for any event $v \in V$. Then, classical models are given by convex combinations of deterministic models: $p(v) = \sum_\lambda q_\lambda p_\lambda(v)$, where q_λ is a probability distribution, and p_λ correspond to deterministic models on H. The set of classical models on H is denoted $\mathcal{C}(H)$. If H is a Bell-type scenario, then $\mathcal{C}(H)$ is the standard Bell polytope. If H is a general contextuality scenario, classical models are those that can be explained by noncontextual hidden variables [Fin82].

A quantum model p on H is a probabilistic model such that there exist a Hilbert space $\mathcal{H}$, a normalized density matrix $\rho \in \mathcal{P}(\mathcal{H})$, and for each vertex $v \in V$, a projector P_v such that $\sum_{v \in e} P_v = \mathbb{1}_\mathcal{H}$ for each measurement $e \in E$ that give rise to p via the Born rule: $p(v) = \mathrm{tr}\,(\rho P_v)$, for each event v. The set of quantum models on H is denoted $\mathcal{Q}(H)$. Contrary to $\mathcal{C}(H)$ and $\mathcal{G}(H)$, the quantum set is usually not a polytope, and a recurring question in the literature is to find some "natural principle" that would limit correlations observable in Nature to be in the quantum set. Since $\mathcal{Q}(\mathcal{B}_{2,2,2}) \subsetneq \mathcal{NS}(\mathcal{B}_{2,2,2})$, it is clear that the no-signaling principle alone is not sufficient to restrict the correlations to be quantum.

2.1.4 The quantum set from a natural principle

Several candidate principles for recovering the set of quantum correlations have been suggested and investigated in the literature: Information Causality [PPK+09], Macroscopic Locality [NW10], the nontriviality of communication complexity [vD05], and more recently, Local Orthogonality [FSA+13], [SFA+14]. The latter is particularly interesting in the sense that it is a genuinely multipartite principle, a necessary condition in order to recover the quantum set [GWAN11]. The framework introduced above turns out to be remarkably well-suited for the study of Local Orthogonality (LO). This principle defines a notion of orthogonality between events of a scenario: two events u and v are orthogonal is they belong to a common measurement, *i.e.*, there exists a measurement $e \in E$ such that $\{u, v\} \subseteq e$. Then, a set $C = \{v_1, \cdots, v_l\} \subseteq V$ of events is said to be *orthogonal* if its elements are pairwise orthogonal. The principle finally says that the sum of the individual probabilities of a set of orthogonal events is less than one, namely, $\sum_{v \in C} p(v) \leq 1$. The set obtained this way is a polytope denoted by $\mathcal{LO}^1(H)$. A natural strengthening of the principle assumes that if a given probabilistic model is "physical", then so should be an arbitrary number k of copies of this model. Then, Local Orthogonality should also be satisfied by the model corresponding to these k copies. Copies of a scenario can be defined via the k-fold *Foulis-Randall* product of the scenario H with itself, $H^{\otimes k}$. The Foulis-Randall product [FR81] is especially relevant in the context of Bell scenarios since scenarios with many parties can be obtained by taking the product of several single-party scenarios. In particular, $\mathcal{B}_{n,m,k} = \mathcal{B}_{1,m,k}^{\otimes n}$. Now, the strengthening of LO says that the

product distribution $p^{\otimes k} \in \mathcal{G}(H^{\otimes k})$ should also satisfy LO. We denote by $\mathcal{LO}^k(H)$ the set of probabilistic models on H such that $p^{\otimes k} \in \mathcal{LO}^1(H^{\otimes k})$. In the limit of an arbitrary number of copies, this gives rise to the set $\mathcal{LO}^\infty(H)$, which would ideally match the set $\mathcal{Q}(H)$, were the LO principle sufficient to recover quantum correlations. We note that another way to naturally strengthen LO would be to allow for wirings of boxes. However, it was proved in [FSA+13] that these leave the set $\mathcal{LO}^\infty(H)$ invariant. It turns out that characterizing the set $\mathcal{LO}^\infty(H)$ of correlations satisfying the LO principle is quite challenging. While it is reasonably easy to verify that $\mathcal{Q}(H) \subseteq \mathcal{LO}^\infty(H) \subseteq G(H)$, being more precise is difficult.

Our framework, however, allows for a reformulation of $\mathcal{LO}^\infty(H)$ in terms of graph invariants. Introduce the *orthogonality graph* $G = \mathrm{Ort}(H)$ of the contextuality scenario H to be the graph with vertex set $V(H)$, and such that $\{u, v\}$ is an edge if u and v do not belong to a common measurement $e \in E(H)$. Then, one can show (see [AFLS15] for details) that a probabilistic model p belongs to $\mathcal{LO}^\infty(H)$ if and only if $\Theta(\mathrm{Ort}(H), p) = 1$ where $\Theta(G, p)$ refers to the Shannon capacity of the graph G weighted by the distribution p. This characterization can then be used to prove that $\mathcal{LO}^\infty(H)$ is in generally strictly larger than $\mathcal{Q}(H)$[1], and that there even exist contextuality scenarios for which $\mathcal{LO}^\infty(H)$ is not convex [SFA+13].

2.1.5 Hierarchies

Another feature of our framework is that the various sets of correlations we mentioned can be approximated through some hierarchies of relaxations. Such hierarchies have been intensely studied in convex optimization (see Ref. [Lau09] for a recent review) and been adapted to the context of quantum correlations [NPA07]. In particular, the hierarchies we will consider may be seen as a special case of the general hierarchy for noncommutative polynomial optimization [DLTW08], [PNA10]. Let us first introduce the notion of moment matrix associated with a contextuality scenario $H = (V, E)$. A moment matrix of order k associated with H is a symmetric matrix M_k whose rows and columns are indexed by *words* of size at most k written in the alphabet formed by V. More explicitly, if $V = \{v_1, \ldots, v_n\}$, the rows of the moment matrix will be indexed by: $\varnothing, v_1, \ldots, v_n, v_1v_1, v_1v_2, \ldots, v_1v_n, \ldots, v_n^2, \ldots, v_1^3, \ldots, v_n^k$, where v_i^k is the word obtained by concatenating k times the letter v. Here, $\varnothing$ refers to the empty string, and we choose the normalization $M_k(\varnothing, \varnothing) = 1$. We denote by V^* the set of strings of arbitrary size on V. A matrix M_k will be a *certificate of order* k for the probabilistic model p on H if it is positive semidefinite, $M_k \succeq 0$, and if $M_k(v, \varnothing) = p(v)$ for every $v \in V$.

The matrices M_k can display additional "natural" properties that we define now: Normalization, Orthogonality and Commutativity. A moment matrix is *normalized* with respect to the contextuality scenario $H = (V, E)$ if for every two strings $\vec{v}, \vec{w} \in V^*$, and

[1] In fact, a proof that the sets $\mathcal{LO}^\infty(H)$ and $\mathcal{Q}(H)$ are not equal was found by Miguel Navascués before this formalism had been set up.

every edge $e \in E$, the following condition holds:

$$\sum_{u \in e} M(\vec{v}u, \vec{w}) = M(\vec{v}, \vec{w}). \qquad \text{(Normalization)}$$

A matrix is *orthogonal* with respect to H if for every $e \in E$, and $\vec{v}, \vec{w} \in V^*$, the fact that $v, w \in e$ implies that

$$M(\vec{v}v, \vec{w}w) = 0 \quad \forall \vec{v}, \vec{w} \in V^*. \qquad \text{(Orthogonality)}$$

Finally, a matrix is *commutative* if for any two strings $\vec{v}, \vec{w} \in V^*$, and every permutation π of size $|\vec{v}|$,

$$M(\pi(\vec{v}), \vec{w}) = M(\vec{v}, \vec{w}), \qquad \text{(Commutativity)}$$

where $\pi(\vec{v})$ is the string obtained by permuting the letters of $\vec{v}$ with the permutation π.

We are now in position to define sets of models for which there exist certificates satisfying some of these properties. These sets actually form hierarchies of sets $(\mathcal{S}_k)_{k\geq 1}$, such that $\mathcal{S}_k \subseteq \mathcal{S}_{k-1}$ corresponds to the probabilistic models with a certificate of order k. The hierarchies we will introduce admit limits that we denote by $\mathcal{S}_\infty := \bigcap_{k\leq 0} \mathcal{S}_k$. Let us define three hierarchies of sets $\mathcal{G}_k, \mathcal{Q}_k$ and $\mathcal{C}_k$ as follows. A probabilistic model p on H belongs to $\mathcal{G}_k(H)$ is there exists a certificate of order k for p satisfying Normalization; it belongs to $\mathcal{Q}_k(H)$, if there exists a certificate of order k satisfying Normalization and Orthogonality; and it belongs to $\mathcal{C}_k(H)$ if there exists a certificate of order k satisfying Normalization, Orthogonality and Commutativity. Our results show that these hierarchies converge to the expected sets [FLS13].

Theorem 16 (Convergence of the hierarchies)**.** *For every contextuality scenario $H = (V, E)$,*

$$\begin{aligned}
\mathcal{G}_\infty(H) &= \mathcal{G}_1(H) = \mathcal{G}(H), \\
\mathcal{Q}_\infty(H) &= \mathcal{Q}(H), \\
\mathcal{C}_\infty(H) &= \mathcal{C}_{|V|}(H) = \mathcal{C}(H).
\end{aligned}$$

The hierarchies $(\mathcal{G}_k)_{k\geq 1}$ and $(\mathcal{C}_k)_{k\geq 1}$ both converge after a finite number of steps, and it is natural to ask whether the same holds for $(\mathcal{Q}_k)_{k\geq 1}$. While a finite number of steps is indeed sufficient if there exists a *finite-dimensional* quantum model, it is an open question related to difficult problems in the theory of C^*-algebras whether there exist contextuality scenarios H for which the hierarchy needs infinitely many steps to converge (see Section 8.3 of [AFLS15] for details).

2.1.6 Link between $\mathcal{LO}^\infty(H)$ and the quantum set

In the same way as $\mathcal{LO}^\infty(H)$ can be characterized via the Shannon capacity of the orthogonality graph $\mathrm{Ort}(H)$, weighted by the distribution p, the first level of the quantum hierarchy, $\mathcal{Q}_1(H)$ can be characterized by the Lovasz function of $\mathrm{Ort}(H)$, weighted by

p. More precisely, a probabilistic model p on the contextuality scenario H, belongs to $\mathcal{Q}_1(H)$ if and only if $\vartheta(\mathrm{Ort}(H), p) = 1$.

For every graph G, and any choice of weight p for the vertices of G, it is known that $\Theta(G, p) \leq \vartheta(G, p)$, which immediately implies that for every contextuality scenario, $\mathcal{Q}_1(H) \subseteq \mathcal{LO}^\infty(H)$. This proves that the Local Orthogonality principle is not sufficient to recover the set of quantum correlations for arbitrary contextuality scenarios since $\mathcal{Q}_1(H) \neq \mathcal{Q}(H)$ in general.

2.2 Bit commitment from no superluminal signaling

We now move on to possible cryptographic applications of the study of quantum correlations and nonlocality. This section discusses how security guarantees can be obtained from the no superluminal signaling (NSS) principle which states that no information carrier can travel faster than the speed of light. The whole field of quantum cryptography is based on the idea that quantum theory puts severe constraints on what an adversary can do, in particular, that there often exists a fundamental trade-off between the amount of information they can acquire and the disturbance on the physical systems this information is encoded on. This is what we saw in the previous chapter devoted to quantum key distribution. The reason we trust quantum cryptography is that we trust the quantum theory it relies on. Another pillar of modern physics is the law that no information can travel faster than the speed of light. It is sensible to ask whether this law allows one to perform cryptographic tasks with proven security. This is the theme we explore in this section. Since the NSS principle is related to special relativity, this field is referred to as "relativistic cryptography", even though no relativistic effects are exploited for this type of cryptography.

2.2.1 Context and history of the field

Let us first note that the NSS principe is closely related to the *non-signaling principle* that says that a local action performed in a laboratory cannot have an *immediate* influence outside of the lab. NSS is more precise since it gives an upper bound on the speed at which such an influence can propagate. The current goal of relativistic cryptography is to understand what cryptographic tasks can be achieved with *information-theoretic* security meaning that the schemes proposed cannot be attacked by any classical (or quantum) computers, even with infinite computing power. This is in contrast with currently deployed schemes, which most often rely on computational assumptions such as the hardness of factoring [RSA78]. In the future, it will perhaps make sense to consider hybrid scenarios involving both a relativistic and a more conventional (based on such hardness assumptions) components, but as we will see, it is premature to consider such scenarios today, since we are far from completely understanding what can be achieved from the NSS principle alone.

The idea of exploiting the NSS principle for cryptographic protocols originated in a pioneering work by Kent in 1999 [Ken99] as a way to physically enforce a non communic-

ation constraint between the different agents of one party (the idea of splitting up a party into several agents dates back to [BOGKW88], but without an explicit implementation proposal). The main idea is to ask questions to several agents in a synchronized fashion, to make sure that their respective answer cannot depend on the questions asked to the other agents. This is in this sense that the NSS principle puts nontrivial constraints on what a *coalition* of agents can achieve. The original goal of Kent was to bypass the well-known no-go theorems for quantum bit-commitment [May97], [LC97]. Bit commitment is a natural two-party cryptographic primitive where one player, Alice, commits to a bit and unveils its value after some sustain time. A bit commitment protocol is deemed to be secure if it satisfies two properties: (*i*) it should be *hiding*, which means that the second player, Bob, should not be able to learn the value of the bit before Alice reveals it; and (*ii*) it should be *binding*, meaning that Alice should not be able to change her mind during the sustain time and reveal a value different from the one she committed to. It is well-known that informationally-secure bit commitment cannot be obtained in the standard (classical) model and the early success of quantum key distribution raised the hope that quantum theory could once more provide security for a protocol involving the exchange of quantum states. Some quantum bit commitments were studied in the 90s but attacks were always found, until the works of Mayers, and Lo and Chau put an end to this line of work: no quantum bit commitment protocol can be both hiding and binding [May97], [LC97].

With his work, Kent managed to circumvent these no-go theorems by changing the rules of the game and imposing timing constraints on the exchanges performed by the various participants [Ken99]. The main novelty of this work was to split Alice and Bob into coalitions of agents who would exchange messages in a synchronized fashion. An important concept in the context of cryptography is that the NSS puts limits on the information available to the agents, but only during a very limited time, corresponding to the time that light needs to reach the agents in question. For bit commitment, it means that if Alice's agents (as well as Bob's agents) are separated by some distance d, then they all have access to full information after a time at most d/c, where c is the speed of light. This time is therefore an upper bound on the sustain time of the protocol. In order to allow for longer sustain times, multi-round protocols are required. For instance, an N-round protocol will allow for a sustain time of order Nd/c.

Interestingly, the original protocol of Kent was classical in the sense that all the communication only involved classical messages and allowed for several rounds which increased the lifespan of the protocol. However, the protocol required to exchange messages whose length scaled exponentially in the number of rounds (*i.e.*, the commitment time) and a feasible implementation was not possible for a large number of rounds. A subsequent work [Ken05] improved this scaling, but to our knowledge, no precise time/security tradeoff is available for this protocol. More recently, quantum relativistic bit commitment protocols were developed where the parties exchange quantum systems, with the hope that combining the no superluminal signaling principle with quantum theory will lead to more secure (but less practical) protocols [Ken11], [Ken12b], [KTHW13]. In particular, the protocol [Ken12b] was implemented in Ref. [LKB+13].

The original idea of [BOGKW88] was recently revisited by Crépeau *et al.* [CSST11] (see also [Sim07]). Based on this work, Lunghi *et al.* devised a multi-round bit commitment protocol involving only four agents, two for Alice and two for Bob [LKB+15]. They managed to prove that this protocol, which we call the "$\mathbb{F}_Q$ protocol" from now on, remains secure for several rounds, against classical attacks. Unfortunately, this proof was rather inefficient since the complexity of the protocol (the size of the messages the agents need to exchange at each round) scaled exponentially with the number of rounds. Recently, together with Kaushik Chakraborty and André Chailloux, we improved the security proof and showed that the complexity of the protocol in fact only scales logarithmically with the number of rounds citeCCL15 (see also the independent work of Fehr and Fillinger [FF15]), implying that the commitment time is essentially unlimited:

Theorem 17 ([CCL15], [FF15])**.** *The $\mathbb{F}_Q$ relativistic r-round bit commitment protocol is ε-secure with $\varepsilon = O\left(\frac{N}{Q^{1/2}}\right)$ against classical adversaries. The number of bits exchanged at each round is $\log_2(Q)$, which can be taken equal to $2(\log(1/\varepsilon) + \log(N))$ in order to perform the protocol over r rounds with security parameter ϵ.*

This security proof is based on an analysis of CHSH_Q, a non-signaling game that generalizes the well-known CHSH game to the case where inputs and outputs are not restricted to being bits, but rather belong to $\mathbb{F}_Q$ the Galois Field of order Q. We discuss it in the next subsection.

2.2.2 Relativistic bit commitment protocols

We will first describe the single-round protocol (with commitment time bounded by $\tau = d/c$ where d is the distance between the distant locations and c is the speed of light), before focussing on the $\mathbb{F}_Q$ multi-round protocol.

To simplify the analysis, we consider here that all computations are performed instantaneously and that information travels at the speed of light. One could relax these assumptions by replacing τ by a smaller constant, but this would not change the various scalings of parameters and we therefore ignore this issue here.

The protocols we consider are all perfectly hiding in the sense that Bob has no information about the committed values before the reveal step. An important consequence is that the spatial configuration of the agents needs only to be checked by Bob: in particular, it is sufficient for Bob to make sure that his agents are at a distance at least d from each other. If this is the case, and if Alice's agents answer their challenges in time, then Bob can deduce that her agents are also separated by a distance d.

The single-round protocol. The single-round version of the protocol was introduced by Crépeau *et al.* [CSST11] (see also [Sim07]). Both players, Alice and Bob, have agents $\mathcal{A}_1, \mathcal{A}_2$ and $\mathcal{B}_1, \mathcal{B}_2$ present at two spatial locations, L_1 and L_2, separated by a distance d. We consider the case where Alice makes the commitment. The protocol (followed by honest players) consists of four phases: preparation, commit, sustain and reveal. The sustain phase in the single-round protocol is trivial and simply consists in waiting for a time less than τ, which is the time needed for light to travel between the two locations.

Overall the bit commitment protocol goes as follows.

1. *Preparation phase*: $\mathcal{A}_1, \mathcal{A}_2$ (resp. $\mathcal{B}_1, \mathcal{B}_2$) share a random number $a \in \mathbb{F}_Q$ (resp. $b \in \mathbb{F}_Q$).

2. *Commit phase*: $\mathcal{B}_1$ sends b to $\mathcal{A}_1$, who returns $y = a + c * b$ where $c \in \mathbb{F}_2$ is the committed bit. Here and everywhere in this paper, all operations like $+$ and $*$ are understood as addition and multiplications in $\mathbb{F}_Q$.

3. *Sustain phase*: $\mathcal{A}_1$ and $\mathcal{A}_2$ wait for some time less than τ.

4. *Reveal phase*: $\mathcal{A}_2$ reveals the values of c and a to $\mathcal{B}_2$ who checks that $y = a + c * b$.

The $\mathbb{F}_Q$-protocol (multi-round). The single-round protocol above was recently extended to a multi-round commitment scheme [LKB+15]. The main idea to increase the commitment time is to delay the reveal phase and have $\mathcal{A}_2$ commit to the *string* a instead of revealing it. In fact, the new sustain phase will now consist of many rounds where the active agents (*i.e.*, the agent of Alice who commits in that given round and the corresponding agent for Bob) alternate between locations L_1 and L_2. Overall, the required number of rounds scales linearly with the commitment time one wishes to achieve. The k-round bit commitment protocol goes as follows (for k even):

1. *Preparation phase*: $\mathcal{A}_1, \mathcal{A}_2$ (resp. $\mathcal{B}_1, \mathcal{B}_2$) share k random numbers $a_1, \ldots, a_k$ (resp. $b_1, \ldots, b_k$) $\in \mathbb{F}_Q$.

2. *Commit phase* (round 1): $\mathcal{B}_1$ sends b_1 to $\mathcal{A}_1$, who returns $y_1 = a_1 + c * b_1$ where $c \in \mathbb{F}_2$ is the committed bit.

3. *Sustain phase*: at round $j \leq k$, active Bob sends $b_j \in \mathbb{F}_Q$ to active Alice, who returns $y_j = a_j + b_j * a_{j-1}$.

4. *Reveal phase*: $\mathcal{A}_1$ reveals d and a_k to $\mathcal{B}_1$. $\mathcal{B}_1$ computes recursively $\alpha_0 = c$ and $\alpha_{i+1} = y_{i+1} - b_{i+1} * \alpha_i$ and checks that $\alpha_k = a_k$. If this is the case, Alice has successfully revealed the bit c.

We require that round j finishes before any information about b_{j-1} reaches the other Alice: this is where we exploit the NSS principle (see Figure 2.2). For any j, this implies that Alice's active agent has no information about b_{j-1}. In particular, this means that y_j is independent of b_{j-1}.

Security of the $\mathbb{F}_Q$-protocol. In order to prove that the protocols above are secure, it is sufficient to prove that they are binding. This is a consequence of the fact that the CHSH_Q nonlocal game cannot be won perfectly. In this game introduced by Buhrman and Massar [BM05], two non-communicating parties, Adeline and Bastian, each receive an input string x and y from $\mathbb{F}_Q$ chosen uniformly at random. They respectively output strings a and b in $\mathbb{F}_Q$ and win the game if their outputs satisfy $a + b = x * y$, where $+$

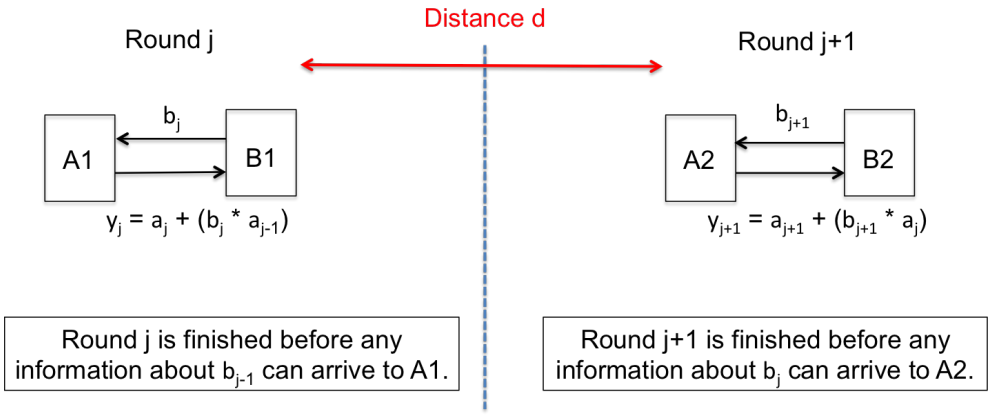

Figure 2.2 – Description of the $\mathbb{F}_Q$ protocol.

and $*$ denote the addition and multiplication in $\mathbb{F}_Q$. Unlike to the usual CHSH game, corresponding to the case $Q = 2$, the CHSH_Q game has hardly been studied in the literature (see, however [BS15], [How15], [RAM16]). In particular, Bavarian and Shor [BS15] proved an upper bound on the quantum value ω^* of the game, that is the maximum winning probability if both players (which correspond to Alice's agents in a cheating strategy) share an entangled state:

$$\omega^*(\mathsf{CHSH}_Q) \leq \frac{1}{Q} + \frac{Q-1}{Q}\frac{1}{\sqrt{Q}}.$$

This essentially implies the security of the single-round protocol against classical or quantum adversaries.

Proving that the multi-round protocol remains binding is more involved as the two cheaters are now asked to win a multi-round game, which might be a much easier task. If one restricts the adversaries to be classical (*i.e.*, not sharing an entangled state), it is possible to reduce the security of the protocol to the analysis of a variant of the CHSH_Q game where the inputs are not uniform anymore. In [CCL15], we showed that the classical value ω of CHSH_Q games where one of the inputs is biased with maximum probability p is

$$\omega(\mathsf{CHSH}_Q(p)) \leq p + \sqrt{\frac{2}{Q}}.$$

This result allowed us to establish Theorem 17 which proves the security of the $\mathbb{F}_Q$ protocol against classical adversaries. The remarkable feature of this result is that the protocol turns out to be very practical, contrary to previous intuition based on the works of Kent. In particular, a convincing experiment recently demonstrated the possibility of sustaining a commitment for 24 hours [VMH+16], consisting of 5×10^9 rounds.

Robust version of the $\mathbb{F}_Q$ protocol. In a subsequent work [CCL16], we introduced a new relativistic bit commitment protocol that addresses one of the main weaknesses of

the $\mathbb{F}_Q$ protocol, namely its fragility against network failures. Indeed, the $\mathbb{F}_Q$ protocol aborts as soon as one agent fails to respond to a single challenge in time. We fixed this issue by modifying the $\mathbb{F}_Q$ protocol so that each party is now represented by 3 agents in 3 distinct locations. The communication cost of this variant is relatively modest, but the gain in terms of tolerance to loss is very good: one obtains a quadratic gain for the expected number of rounds that the protocol can sustain, making it very promising for implementations in real telecom networks (instead of dedicated networks), which is crucial for a possible future deployment of this technology.

2.2.3 Application to zero-knowledge proofs for NP

An example of application of bit commitment is in the context of zero-knowledge proofs. The goal here is for a prover to convince a verifier that a statement is true, without conveying any information other than the fact that the statement is indeed true. A particularly relevant class of problems is the class NP of decision problems for which instances with a yes answer admit a proof that is efficiently verifiable. Zero-knowledge proofs are interactive protocols that usually involve a bit commitment scheme. It is therefore natural to investigate whether the relativistic (single-round) bit commitment considered above is useful in this context.

In Ref. [CL16], we showed that the zero-knowledge construction for Hamiltonian Cycle remains secure against quantum adversaries in the relativistic setting. Since Hamiltonian Cycle is an NP-complete problem, our result provides zero-knowledge proofs secure against quantum adversaries for the whole class NP.

It was not *a priori* clear that the relativistic bit commitment would allow for such zero-knowledge proofs. Indeed, the security definition of the bit commitment protocol is rather weak and does not "compose" well in the sense that it does not imply that the security of a larger protocol using the bit commitment scheme as an elementary brick will automatically inherit the security of that scheme. In order to prove our result, we developed a new tool for studying the action of consecutive measurements on a quantum state, which in turn yields upper bound on the entangled value of some nonlocal games. In particular, we obtained the following generalization of the *gentle measurement* lemma [Win99] (albeit with a worse constant).

Theorem 18 ([CL16])**.** *Let $P_1, \dots, P_n$ be n projectors which can be written as $P_k = \sum_{s=1}^{S} P_k^s$ with $P_k^s P_k^{s'} = \delta_{s,s'} P_k^s$, for all k, s, s'. Let σ be an arbitrary density matrix and define $V := \frac{1}{n}\sum_{k=1}^{n} \mathrm{tr}(\sigma P_k)$ and $E := \frac{1}{n(n-1)} \sum_{k,\ell \neq k} \sum_{s,s'} \mathrm{tr}(P_\ell^{s'} P_k^s \sigma P_k^s P_\ell^{s'})$. Then it holds that*

$$E \geq \frac{1}{64S}\left(V - \frac{1}{n}\right)^3.$$

The quantities V and E quantify the disturbance cause by one, or 2 consecutive measurements, respectively: they are close to 1 if the state is almost not disturbed and much smaller otherwise. The case of $n = 2$ can be seen as a worst-case consecutive measurement theorem: how much can the first measurement disturb the measured state

before the second measurement? However, for larger values of n, this shows that when we pick 2 measurements out of n, the disturbance is much smaller, as shown by the dependence of the lower bound in n. Our theorem also improves on known results since it deals with larger values of S. Interestingly, this kind of statement has already appeared previously in a paper by Unruh [Unr12], who studied quantum sigma protocols and in particular quantum proofs of knowledge.

The goal of this work was to demonstrate that it is possible to plug in the $\mathbb{F}_Q$ relativistic bit commitment protocol into the well-known zero-knowledge protocol for Hamiltonian Cycle due to Blum [Blu86]. This widens the possible applications for relativistic cryptography and raises the question of what other cryptographic tasks can benefit from the NSS principle.

2.2.4 Future work on relativistic cryptography

The security proof for the multi-round bit commitment protocol only holds against classical adversaries. Although the protocol is itself classical, it is quite possible that a cheating strategy becomes available if the agents of a cheating party share entanglement instead of classical randomness. And indeed, for the single-round protocol, allowing for entanglement slightly helps the cheating party since the entangled value of the CHSH_Q game is a bit larger than its classical value. The main difficulty to extend the analysis to the quantum case is that the composition of the rounds is more complicated to handle because the history is not described by classical random variables anymore, but rather by quantum states. Technically, one has to analyze nonlocal games where the players are allowed to initially share an entangled state that can (weakly) depend on their input states. This is a rather uncommon scenario in the field of quantum cryptography and the tools needed to deal with it have not been developed yet.

Another important open question is to better understand what cryptographic primitives can be achieved via the NSS principle. In [CL16], we have shown that zero-knowledge proofs could take advantage of the NSS principle. An obvious candidate is Oblivious Transfer, which cannot be informationally-secure using quantum theory alone [May97], [LC97]. Unfortunately, although this has not been formally proven so far, it seems unlikely that secure OT can be obtained in a relativistic setting. Other natural candidates which have not been studied so far are multipartite computation, electronic voting or password-based authentication schemes for instance.

2.3 Position-based quantum cryptography

In this third section, we turn our attention to another quantum cryptographic task: position verification. The goal of position-based cryptography is for an honest party to use her spatio-temporal position as her only credentials in a cryptographic protocol. In particular, Position Verification aims at verifying that a certain party, called the prover, holds a given position in space-time. Such a protocol typically goes as follows: a set of verifiers will coordinate and send some challenge to the prover, and it is expected that

only someone sitting in the correct position can successfully pass the challenge.

Position verification protocols have been studied in the classical setting where the challenges are described by classical information, and it was shown in [CGMO09] that information-theoretic security could never be obtained in the standard model. More precisely, it is always possible for a *coalition* of adversaries to convince the verifiers, even if none of the adversaries sits in the spatio-temporal region where the prover is supposed to be. A possible way-out of this no-go theorem would be to consider a quantum setting.

Position-based cryptography in the quantum setting was first investigated under the name of *quantum tagging* by Kent around 2002, but only appeared in the literature much later in [KMS11] where attacks against possible quantum constructions are described. Malaney independently introduced a quantum position verification scheme in [Mal10]. An example of a quantum protocol for position verification involves two verifiers V_0 and V_1: V_0 sending a qubit $|\phi\rangle = U|x\rangle$ with $x \in \{0, 1\}$ and U some unitary, and V_1 sending a classical description of the unitary U. The task for the prover is then to measure the qubit in the basis $\{U|0\rangle, U|1\rangle\}$ and to return the classical value of x to both provers. There are many variations around this protocol, and the intuition for the possible security of such protocols is that only someone receiving both U and $|\phi\rangle$ can perform the required measurement, and return the correct value x on time. In [LL11], Lau and Lo extended the attack from [KMS11] to show that the above intuition is incorrect if the unitary U is a *Clifford* gate. In that case, a couple of cheaters, Alice lying between V_0 and the prover P, and Bob lying between V_1 and P, can always fool the verifiers provided that they share a small number of EPR pairs. This result was later generalized by Buhrman *et al.* [BCF+11] who showed that such an attack always exists provided that the coalition of cheaters share sufficiently many EPR pairs: no position-based quantum cryptographic protocol can display information-theoretic security.

Two general families of attacks against such position-verification protocols have been considered in the literature so far, both based on quantum teleportation. The first one is inspired by Vaidman's protocol for non-local computation [Vai03] and consists in the cheaters teleporting some quantum state back and forth, with the number of exchanges depending on the success probability of the attack. If the position-based protocol involves n qubits, the resource (number of EPR pairs) required for this type of attacks to succeed typically scales double-exponentially with n [BCF+11]. Another class of attacks uses *port-based* teleportation [IH08] and requires only exponential entanglement to succeed [BK11]. If one could prove that such an attack was indeed optimal, one would obtain a secure position-based protocol for all practical purposes.

Establishing lower bounds for the amount of entanglement shared by the coalition in order to successfully attack the protocol is a non trivial task. Current lower bounds are linear in the security parameter of the protocol [BK11], [TFKW13], [RG15]. It was also shown by Unruh that security of some position-verification protocols could be established in the quantum random oracle model, that is if one has access to one-way functions [Unr14].

Let us comment on some assumptions that we make in this work. Our main goal is to present some natural position verification protocols and to study general classes

of attacks that can be carried out by coalitions of cheaters. While we try to be as general as possible, we think it is sensible to make some specific choices in order to simplify the analysis. For instance, we restrict our protocols to using qubit states, and more importantly, we consider one-dimensional protocols with only 2 verifiers. Most of our analysis would carry through to arbitrary qudit protocols involving many verifiers. We also decided to leave aside all the problems related to timing in order to focus on the genuinely quantum part of the procedure. This means that we consider that all communication (classical or quantum) is performed at the speed of light, and that all computation is instantaneous. These are obviously unrealistic assumptions, but dealing with more realistic ones can be done independently of the analysis we provide here (see for instance the work of Kent [Ken12a]). The main source of imperfection in a position verification protocol is the quantum channel between the verifiers and the prover, which can never be assumed to be perfect. In general, the channel is both lossy and noisy, which is why even an ideal prover cannot possibly pass the test perfectly. On the other hand, it makes sense to assume that the classical channels are essentially perfect (lossless and noiseless).

In this section, we investigate a family of protocols where the verifiers send respectively an n-qubit state $|\phi\rangle$ and unitary U is chosen from a family of n-qubit gates. The prover is asked to apply the unitary U, measure the resulting state $U|\phi\rangle$ in the computational basis and to send the measurement results to both verifiers. We present some new attacks against such protocols that might become particularly efficient when the position-verification protocol is practical for the honest prover, meaning that the family $\mathcal{U}$ is efficiently implementable.

2.3.1 A general family of position-verification protocols

Following the literature, we find it useful to describe the protocol in terms of distributed collaborative games, where two players, named Alice and Bob, independently receive some query from some referee, are allowed a single round of (bipartite) communication and need to output some answer. In the honest prover case, Alice and Bob hold the same spatial position and the prover has access to both their inputs. In the cheating coalition case, Alice and Bob only have access to their own input and their share of the entangled state and are only allowed one simultaneous round of communication. The main result of [BCF+11] is that if Alice and Bob can win the game with arbitrarily many rounds of communication, then they can also win it with a single simultaneous round, provided that they are sufficiently entangled.

The main family of protocols we will consider corresponding to games denoted by $G(n,\mathcal{U})$ where n refers to the number of qubits involved in the protocol and $\mathcal{U}$ is a set of n-qubit unitaries. The protocol $G(n,\mathcal{U})$ consists of the following phases:

1. Preparation Phase:

   (a) The verifier V_0 chooses an n-qubit unitary operator $U \in_R \mathcal{U}$ and an n-bit string $x = (x_1, \ldots, x_n) \in_R \{0,1\}^n$. V_0 prepares $|\psi\rangle = U|x\rangle$, where $|x\rangle = \bigotimes_{i=1}^n |x_i\rangle$ is a computational basis state.

(b) V_0 sends x and U to V_1 through some secure authenticated classical channel.

2. Execution Phase:

   (a) V_0 sends the n qubit quantum state $|\psi\rangle$ to prover P at time 0. V_1 sends the unitary U to P at time $\tau = 0$.

   (b) The prover P receives both $|\psi\rangle$ and U at time $\tau = 1$.

   (c) After receiving $|\psi\rangle$ and U, the honest prover P computes $U^\dagger|\psi\rangle$ and measures it in computational basis, obtaining some outcome string y. P then sends back y to both V_0 and V_1.

3. Verification Phase:

   (a) The prover P wins the game if V_0 and V_1 receive the same string y at time $\tau = 2$, and if the Hamming distance between x and y is less than ηn: $d_H(x, y) \leq \eta n$.

In the literature, this family is often considered in the single qubit case, for instance with $\mathcal{U} = \{\mathrm{id}, H\}$ where H is the Hadamard gate [CGMO09], [BCF+11], [RG15]. Then it makes sense to repeat the protocol n times in order to build some statistics. Here, we are interested in the most general scenario and consider n-qubit gates. For such protocols, we show that there exists a trade-off between the complexity of the protocol for the honest prover and the resources needed to break the protocol for a coalition of cheaters.

2.3.2 Attacks strategies against position verification protocols

The attack strategies we consider have the following structure:

1. Alice and Bob initially share a (possibly entangled) initial bipartite state ρ_{AB} of dimension to be specified later. Typically, ρ_{AB} consists of many EPR pairs.

2. Alice intercepts the communication from V_0, namely a quantum register ρ_C (where C stands for challenge), as well as some classical information.

3. Bob intercepts the classical communication from V_1.

4. Depending on the classical information they received, Alice and Bob perform respectively a quantum measurement on their respective registers, AC and B.

5. They forward all the classical information as well as the outcomes of the measurement to their partner.

6. Finally, upon receiving this information, they prepare and send their response to the verifiers.

The main question of interest is to decide how the dimension of ρ_{AB}, and more particularly the entanglement of this state, scales with the parameters of the position verification protocol. This scenario allows us to see the cheating procedure as a distributed task, or game, where Alice and Bob are asked questions (possibly consisting of a quantum state), are allowed a single round of communication and are required to output some specific answer. They win the game if they fool the verifiers.

We will give explicit attacks that may be efficient in the following practically relevant cases: (1) if $\mathcal{U} \subseteq C_k(n)$, that is if the unitaries all belong to some low level k of the Clifford hierarchy, (2) if the unitaries in $\mathcal{U}$ can all be implemented with a quantum circuit with a fixed layout.

We note that these two cases correspond to protocols that appear to be practical for a honest prover. Indeed, gates in a low level of the Clifford Hierarchy are much easier to implement fault tolerantly than arbitrary gates. Moreover, if the quantum states are photonic states, and the honest prover uses integrated photonics to implement the unitaries in $\mathcal{U}$, a fairly reasonable choice in practice, then it makes sense to fix some layout, that is an optical circuit consisting of single or 2-qubit gates for instance, and to obtain the family $\mathcal{U}$ by changing the value of the single and 2-qubit gates.

2.3.3 Attacks based on the Clifford hierarchy

The *Clifford Hierarchy* introduced in [GC99] is an infinite hierarchy of sets $C_1(n) \subset C_2(n) \subset \cdots \subset C_k(n) \cdots$ of n-qubit unitaries where $C_1(n) = \mathcal{P}_n$ corresponds to the Pauli group (on n qubits), and the higher levels are defined recursively by:

$$U \in C_{k+1}(n) \text{ if and only if } U\sigma U^\dagger \in C_k(n) \text{ for all } \sigma \in C_1(n).$$

When n is clear from context, we simply write C_k instead of $C_k(n)$ for the k^{th} level of the Clifford hierarchy for n-qubit gates. It should be noted that the first two levels of the hierarchy are groups, namely the Pauli and the Clifford groups, whereas none of the higher levels are groups.

The gates from C_1 and C_2 can be "easily" implemented fault-tolerantly [Got97a]. However, it is well known that they do not form a universal set for quantum computation. One therefore requires at least one gate from C_3 to obtain a universal set of gates. Not surprisingly, gates from C_3 or higher levels are usually much harder to implement fault-tolerantly.

Let us first define the *Clifford complexity* of a family $\mathcal{U}$ of unitaries.

Definition 19. *Let $\mathcal{U}$ be a set of n-qubit unitaries. We define the* Clifford complexity *of the set $\mathcal{U}$, denoted by* $\mathrm{CC}[\mathcal{U}]$*, to be the minimum number of EPR pairs that Alice and Bob must share to perfectly win the game $G(n,\mathcal{U})$.*

We obtain the following upper bound for the Clifford complexity of the k^{th} level of the Clifford hierarchy, $C_k(n)$ [CL15].

Theorem 20.

$$\mathrm{CC}[C_1(n)] = 0, \quad \mathrm{CC}[C_1(n)] \leq n, \quad \mathrm{CC}[C_k(n)] \leq 4n\, 4^{n(k-2)} \quad \textit{for } k \geq 2. \tag{2.1}$$

2.3.4 Protocols with fixed layout circuit unitaries

The attack mentioned above is general and works for any n-qubit gate in some given level of the Clifford hierarchy. In the context of position verification protocols, however, the interesting set of gates $\mathcal{U}$ from which the unitary to be implemented is chosen, is often more restricted. Indeed, for the protocol to be practical, a honest prover should be able to implement the unitaries reasonably efficiently. For this reason, it is interesting to consider unitaries described by quantum circuits.

In a practical scenario, where the quantum states given to Alice are photonic qubits, it makes sense to consider photonic implementations for the quantum circuit, and therefore to consider unitaries with a fixed layout for the quantum circuit, and adjustable single and two-qubit gates. This is typically the case for experimental implementations based on integrated photonics [OFV09].

For this reason, we define $\mathcal{U}_{\mathcal{L}}$ to be the set of unitaries described by a fixed layout $\mathcal{L}$, and a specific unitary $U \in \mathcal{U}$ is then described by giving the value of each single or two-qubit gate in the layout. For a quantum circuit based on linear optics, the layout $\mathcal{L}$ corresponds to the position of the phase-shifters and beamsplitters, and the unitary is given by the specific values of the phase-shifts and transmission of the beamsplitters.

We obtain the following upper bound for the Clifford complexity of any layout, as a function of its depth and size [CL15].

Theorem 21. *Let $\mathcal{L}$ be the layout of an n-qubit quantum circuit of depth d where each layer consists of gates in C_{k_i}. Then*

$$\mathrm{CC}[\mathcal{U}_{\mathcal{L}}] \leq 4^{n\sum_{i=1}^{d}(k_i-2)} \times (4n)^d. \tag{2.2}$$

In conclusion, we have established a connection between several well-studied quantum information processing tasks and position-based quantum cryptography. It was previously known that there exists some efficient attack when the verifiers choose the challenge unitary from Clifford group. In [CL15], we showed that this remains true if the unitaries are chosen from a set that is easily implementable, a natural requirement for the protocol to be practical for a honest prover.

Chapter 3

Towards quantum fault-tolerance

In this chapter, we move away from cryptography and focus on quantum information processing tasks. We illustrate this broad theme through three topics: (*i*) a study of the effect of experimental imperfections on Boson Sampling, a non-universal model of quantum computing that has attracted a lot of attention in the community recently; (*ii*) a proposal for a family of quantum LDPC codes with an efficient decoding algorithm; and (*iii*) new quantum algorithms for the cryptanalysis of symmetric cryptosystems.

3.1 Error analysis for Boson Sampling

While quantum computers are widely believed to provide speed-ups over classical computers in theory, it remains an outstanding experimental challenge to provide hard evidence for such a speed-up. The BosonSampling problem, recently introduced by Aaronson and Arkhipov [AA13], makes a step in that direction: while being provably intractable on a classical computer (in its exact version) unless the Polynomial Hierarchy collapses to the third level, it can be efficiently solved with current linear optics technology (see Refs [BFRK+13], [TDH+13], [SMH+13], [COR+13] for recent experimental demonstrations).

Boson Sampling is a simple generalization of the two-photon Hong-Ou-Mandel effect, well-known in quantum optics [HOM87], to larger optical interferometers. Indeed, to an arbitrary unitary matrix $U \in \mathcal{U}(m)$, one can associate an interferometer consisting of beamsplitters and phase-shifters acting on m optical modes, which maps the annihilation operators $\vec{a}^{\text{in}} = (a_1^{\text{out}}, \ldots, a_m^{\text{out}})$ of the inputs modes to those, $\vec{a}^{\text{out}} = (a_1^{\text{out}}, \ldots, a_m^{\text{out}})$, of the output modes via the relation $\vec{a}^{\text{out}} = U\vec{a}^{\text{in}}$. Given such an interferometer corresponding to the unitary U, the Boson Sampling experiment consists in inputing the state $|1, 1, \ldots, 1, 0, 0, \ldots, 0\rangle$ containing a single photon in the first n modes, and the vacuum in the remaining $m - n$ modes, and observing the photon number statistics in the output modes. Scheel [Sch04] showed that the probability of observing a sequence $\vec{s} = (s_1, \ldots, s_m)$ where s_k photons are detected in the k^{th} output mode (and $\sum s_k = n$

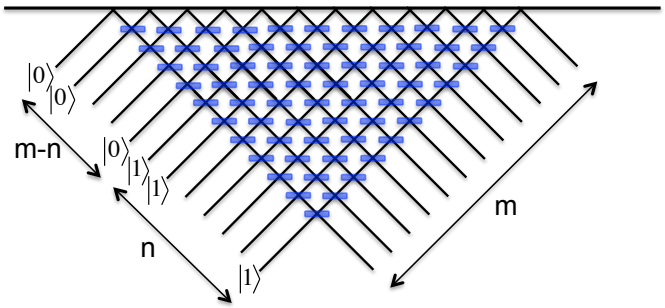

Figure 3.1 – Implementation of the Boson Sampling experiment, following the scheme of Ref. [RZBB94], with input modes on the left and output modes on the right. In general, one would need both phase-shifters and beamsplitters. Here, for simplicity, we consider beamsplitters with complex entries. In other words, phase-shifters are absorbed in the beamsplitters.

by conservation of the photon number) is given by

$$P_U(\vec{s}) = \frac{|\mathrm{Per}(U_{\vec{s}})|^2}{s_1! \cdots s_m!}, \tag{3.1}$$

where Per is the permanent and $U_{\vec{s}}$ is the $n \times n$ matrix obtained from U by discarding all but the n first columns of U^{BS} and then, for all $k \in \{1, \ldots, m\}$, taking s_k copies of the k^{th} row of U. With these notations, we can define the BosonSampling problem:

BosonSampling(m, n)

Input: a unitary matrix U, drawn from the Haar measure on $\mathcal{U}(m)$,

Output: a sample $\vec{s}$ drawn from the distribution P_U.

As we mentioned, it is straightforward to solve this problem (approximately) with linear optics: the idea is that the unitary U can be decomposed in the product of a polynomial number of 2×2 unitaries corresponding to beamsplitters [RZBB94]. Then one simply needs to process the state $|1\rangle^{\otimes n}|0\rangle^{\otimes(m-n)}$ through the corresponding optical network and count the number of photons in each output mode (see Fig.3.1).

The catch here is that due to unavoidable experimental imperfections, one cannot hope to solve the problem exactly, but only approximately. Classical hardness of the approximate version of the problem is still believed to hold but depends on two mathematical conjectures saying that the permanent of random Gaussian matrices is not too concentrated around its expected value, and that approximating the permanent of a random Gaussian matrix is a ♯P-complete problem (see Ref. [AA13] for details). If both conjectures hold, in order to provide evidence for quantum superiority, one still needs to perform an experiment solving the approximate version of the BosonSampling problem. This means that the various sources of errors in the experiment should not alter the output distribution too much compared to p_U. Various sources of imperfection can be

considered: (*i*) single photons not perfectly indistinguishable; (*ii*) losses; (*iii*) imperfect detection efficiency; (*iv*) beamsplitters and phase shifters not implementing exactly the desired transformation. Note that the effect of losses, imperfect detection and imperfect sources sending vacuum with a nonzero probability can be treated similarly (provided that these imperfections are invariant under a permutation of the modes). According to Refs [RR12], [Roh12], the lossy variant of BosonSampling remains a hard problem classically, provided the losses are not too large: one can then use postselection to recover the original problem, and this postselection can be implemented efficiency is the number of single photons is on the order of 20 to 30.

In a work with Raúl Garciá-Patrón [LGP15], we focus on the impact of an imperfect calibration of the optical elements, leading to implementing an interferometer slightly different from the desired one. We therefore assume that the rest of the implementation is ideal: perfect photon sources, no losses, perfect detection. The question we ask is how accurate should the implementation of U be in order for the sampled distribution to be reasonably close to the ideal one? If this requirement cannot be met, then one will have to make the scheme fault-tolerant in order to solve the approximate version of BosonSampling, thereby losing one of the most appealing features of the scheme, namely the simplicity of its experimental implementation.

Our main result is that in order for the implementation to provide a reasonably good output distribution, the average fidelity of the elementary gates should scale at least like $1-O(1/n^2)$. This result indicates that the faulty implementation might not be the main experimental concern for implementations where $n \approx 30$, which should be sufficient to establish quantum superiority.

Model of noise and results

Using the algorithm of Ref.[RZBB94], the unitary can be written $U = U_1 \cdots U_N$ where $N = m(m-1)/2$ is the number of beamsplitters on Fig. 3.1. We consider a model of noise where each beamsplitter U_k is replaced by a beamsplitter $\Phi(U_k)$ acting on the same two modes, where $\Phi : \mathcal{U}(2) \to \mathcal{U}(2)$ is a random map acting identically and independently on each beamsplitter. The map Φ we use is such that $\Phi(U_k)\Phi(U_k^\dagger) = \exp(i\varepsilon h_k)$, where $\varepsilon \geq 0$ controls the noise intensity, and h_k is a 2×2 random Hermitian matrix drawn from the Gaussian Unitary Ensemble, *i.e.*, $h_k = \begin{pmatrix} \alpha_k & \gamma_k \\ \gamma_k^* & \beta_k \end{pmatrix}$ with $\alpha_k, \beta_k \sim \mathcal{N}(0,1)_{\mathbb{R}}$ and $\gamma_k \sim \mathcal{N}(0,1/2)_{\mathbb{C}}$. With this convention, the average fidelity of a beamsplitter is $1-\varepsilon^2$. Denoting by $\Phi(U) := \Phi(U_1) \cdots \Phi(U_N)$ the unitary that is implemented in the lab, our goal is to study the trace distance between the ideal distribution and the real one, that is

$$\mathbb{E}_U \mathbb{E}_\Phi \| P_U - P_{\Phi(U)} \|_1,$$

where we take the expectation over the Haar measure for U and over the noise Φ. Unfortunately, this quantity is really difficult to handle because it is the sum of an exponential number of exponentially small terms. Our solution around this problem consists in studying the implementation of the unitary U followed by that of $U^\dagger$ (see Fig. 3.2): for a perfect implementation ($\varepsilon = 0$), this optical network implements the identity map, and

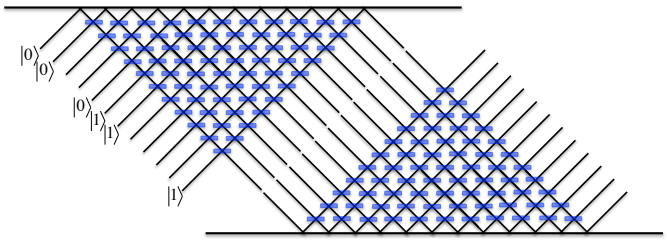

Figure 3.2 – Implementation of the unitary U followed by the unitary $U^\dagger$. A perfect implementation should leave the input state unchanged.

one should obtain the output distribution $(1,\dots,1,0,\dots,0)$ with probability 1. When the noise increases ($\varepsilon > 0$), other output distributions appear with nonzero probability. Denoting by $\tilde{p}_1$ the probability of the output sequence $\vec{s}_1 = (1,\dots,1,0,\dots,0)$ for the distribution $P_{\Phi(U^\dagger)\Phi(U)}$, we obtain

$$\mathbb{E}_U \mathbb{E}_\Phi \|P_{U^\dagger U} - P_{\Phi(U^\dagger)\Phi(U)}\|_1 = \mathbb{E}_U \mathbb{E}_\Phi 2(1-\tilde{p}_1) = 2\left(1 - \mathbb{E}_U \mathbb{E}_\Phi |\mathrm{Per}([\Phi(U)\cdot\Phi(U^\dagger)]_{n\times n})|^2\right),$$

where $[A]_{n\times n}$ is the $n \times n$ upper left minor of A.

Our main result is:

Theorem 22. *In the relevant regime where the number of modes m scales quadratically with n,*

$$\mathbb{E}_U \mathbb{E}_\Phi \|P_{U^\dagger U} - P_{\Phi(U^\dagger)\Phi(U)}\|_1 = \Omega(n^2\varepsilon^2). \tag{3.2}$$

Moreover, we conjecture that the bound is tight in the regime where $n^2\varepsilon^2 \ll 1$. The proof of the theorem follows this strategy:

- the matrix $\Phi(U)\cdot\Phi(U^\dagger)$ can be written as $\exp(i\varepsilon H_N)$ where H_N is the N^{th} element of a random walk on Hermitian matrices,
- using the Baker-Campbell-Haussdorff formula, one can write

$$H_N = \sum_{k=1}^{N} \Phi(U_n^\dagger)\cdots\Phi(U_k^\dagger) h_k \Phi(U_k)\cdots\Phi(U_N),$$

- the permanent of the $n \times n$ upper left minor of $e^{i\varepsilon H_N}$ can be linked to $\mathbb{E}_x\|(\mathbb{1}_m - \Pi_n)H_N\Pi_n x\|^2$, where $x = (e^{i\theta_1},\dots,e^{i\theta_m})$ is a random vector with θ_k chosen uniformly from $[0, 2\pi]$, and Π_n is the projector of the subspace spanned by the first n vectors of the canonical basis of $\mathbb{C}^m$,
- the quantity $\mathbb{E}_x\mathbb{E}_U\mathbb{E}_\Phi\|(\mathbb{1}_m - \Pi_n)H_N\Pi_n x\|^2$ can be analyzed using two matrix concentration bounds due to Tropp [Tro12]: the randomness linked to the noise Φ is dealt with a Gaussian matrix series while the randomness of the BosonSampling unitary is dealt with a matrix Chernoff bound.

One surprising aspect of our result is that the dependence of the noise on the parameters is not too bad: naively, one could have expected the error $\|P_{U^\dagger U} - P_{\Phi(U^\dagger)\Phi(U)}\|_1$ to scale with nm, which is basically the number of relevant gates in an implementation (note indeed that all the gates which only act on vacuum in Fig. 3.1 do not affect the results). While we only have proven a lower bound on the error, we believe our analysis to be tight in the regime where $n^2\varepsilon^2 \ll 1$. For reasonable values of n and m, for instance $n \sim 30$ and $m \sim 1000$, one expects the impact of imperfect calibration of the beamsplitters and phase-shifters to remain negligible (*i.e.*, on the order of a few percents) if the fidelity of each elementary gate is typically on the order of 0.999. While certainly challenging, we do not expect such numbers to be a real problem in any forthcoming Boson Sampling experiment.

3.2 Quantum Expander Codes

We now move to the question of quantum error correcting codes, which definitely needs to be addressed if we ever want to build a large scale universal quantum computer.

In collaboration with Jean-Pierre Tillich and Gilles Zémor, we obtained in [LTZ15] an efficient decoding algorithm for constant rate quantum hypergraph product LDPC codes which *provably* corrects adversarial errors of weight proportional to the code minimum distance, or equivalently to the square-root of the blocklength. The algorithm runs in time linear in the number of qubits, which makes its performance the strongest to date for linear-time decoding of quantum codes. The algorithm relies on expanding properties, not of the quantum code's factor graph directly, but of the factor graph of the original classical code it is constructed from.

3.2.1 Quantum LDPC and CSS codes

A quantum CSS code is a particular instance of a quantum stabilizer code, and can be defined by two classical binary linear codes $\mathcal{C}_X$ and $\mathcal{C}_Z$ in the ambient space $\mathbb{F}_2^n$, with the property that $\mathcal{C}_X^\perp \subset \mathcal{C}_Z$ and $\mathcal{C}_Z^\perp \subset \mathcal{C}_X$. In other words, the classical codes $\mathcal{C}_X$ and $\mathcal{C}_Z$ come together with respective parity-check matrices H_X and H_Z such that the linear space $R_X = \mathcal{C}_X^\perp$ generated by the rows of H_X is orthogonal to the row space $R_Z = \mathcal{C}_Z^\perp$ of H_Z, where orthogonality is with respect to the standard inner product. An *error pattern* is defined as a couple (e_X, e_Z), where e_X and e_Z are both binary vectors. The decoder is given the pair of *syndromes* $\sigma_X = H_X e_X^T$ and $\sigma_Z = H_Z e_Z^T$ and decoding succeeds if it outputs, not necessarily the initial error pattern (e_X, e_Z), but a couple of the form $(e_X + f_X, e_Z + f_Z)$ where $f_X \in R_Z$ and $f_Z \in R_X$. See [Got97b] for the equivalence with the stabilizer formalism and a detailed introduction to quantum coding.

If efficient quantum computing is to be achieved, it will come with a strong error-correcting component, that will involve very fast decoders, probably in not much more than linear time in the blocklength n. The likeliest candidates for this task are quantum LDPC codes: in the CSS case, an LDPC code is simply a code whose above parity-check matrices H_X and H_Z have row and column weights bounded from above by a

constant. Among recent developments, the recent paper [Got14] has shown how fault tolerant quantum computation with constant multiple overhead can be obtained, and quantum LDPC codes are an essential component of the scheme, making them possibly even more appealing.

It is natural to hope that the success of classical LDPC codes, both in terms of performance and of decoding efficiency, can eventually be matched in the quantum setting. This agenda involves two major difficulties, however. The first one is that coming up with intrinsically good constructions of quantum LDPC codes is in itself a challenge. In particular the random constructions that can be so effective in the classical case do not work at all in the quantum case. Indeed if one chooses randomly a sparse parity-check matrix H_X, then, precisely since this gives a good classical code, there are no low-weight codewords in the dual of the row-space of H_X and therefore an appropriate matrix H_Z does not exist. Presently, the known constructions of families of quantum LDPC codes that come with constant rates and minimum distances that grow with the qubit length can be reduced to essentially three constructions. The first consists of quantum codes based on tilings of two-dimensional hyperbolic manifolds (surfaces) that generalise Kitaev's toric code and originate in [FML02]. The minimum distance of these codes grows as $\log n$, where n is the qubit length. A recent generalisation of this approach to 4-dimensional hyperbolic geometry [GL14] yields minimum distances that behave as n^{ε} with $\varepsilon \in [0.2, 0.3]$ [Mur16]. Finally, the construction [TZ14] yields codes of constant rate with minimum distances that grow as $n^{1/2}$. These codes are perhaps the closest to classical LDPC codes in spirit, since they are constructed by taking a properly defined product of a classical LDPC code with itself. We note that all known constructions of quantum codes, even if they are allowed to have vanishing rate, fail to significantly break the $n^{1/2}$ barrier for the minimum distance and it is an intriguing open question as to whether there exist asymptotically good quantum LDPC codes (*i.e.*, with constant rate and minimum distance linear in n). We also make the side remark that Gottesman [Got14] requires, for the purpose of fault-tolerant quantum computation, constant rate LDPC codes with good minimum distance properties that should behave well under some sort of adversarial error setting.

The second difficulty in attempting to match the achievements of classical LDPC coding, is to devise efficient decoding algorithms. The vast majority of decoding algorithms developed for classical LDPC codes rely on iterative techniques whose ultimate goal is to take decisions on individual bits. A straightforward transposition to the quantum setting of this strategy would consist in trying to recover the bits of e_X and e_Z by decoding the LDPC codes $\mathcal{C}_X$ and $\mathcal{C}_Z$. The problem with this approach is that the classical LDPC codes $\mathcal{C}_X$ and $\mathcal{C}_Z$ are somewhat non-standard in that they have by construction bounded minimum distance. Indeed, $\mathcal{C}_X$ has minimum distance at most equal to the smallest row weight of H_Z since $\mathcal{C}_Z^{\perp} \subset \mathcal{C}_X$ and by definition $\mathcal{C}_Z^{\perp}$ is generated by the rows of H_Z. Such a decoder for $\mathcal{C}_X$ is doomed to fail because it is fooled by any error that spans only half the weight of a row of H_Z [PC08]. In other words, such decoding algorithms can not have vanishing error probability.

The way to overcome this problem is really to look for the most likely error modulo

the stabilizer group. However this also implies that bit-oriented decoding strategies are mostly pointless, there is here no "correct value" for a single bit of e_X or e_Z which can always be just as well 0 or 1. Decoding quantum LDPC codes requires therefore additional elements to the classical toolkit.

Decoding quantum LDPC codes seems to be easier in one case, namely for the surface codes mentioned above. This is due to the fact that the underlying classical codes $\mathcal{C}_X$ and $\mathcal{C}_Z$ are cycle codes of graphs: full decoding, which is NP-hard in general for linear codes, can be achieved for cycle codes of graphs in polynomial time (with the help of Edmonds' weighted matching algorithm [Edm65]), and this strategy (which does not really qualify as a local technique) yields a decoding scheme for the quantum code that achieves vanishing error-probability for random errors. Unfortunately, this technique does not extend to other classes of LDPC codes, and in an adversarial setting is limited to correcting at most $\log n$ errors, since the minimum distance of surface codes of constant rate can never surpass a logarithm of the qubit length [Del13].

An alternative decoding algorithm was recently proposed [Has14] for the 4-dimensional hyperbolic codes of Guth and Lubotzky that is devised to work in a probabilistic setting and for which its adversarial performance is unclear. The third class of constant rate quantum codes with growing minimum distance, namely the codes [TZ14], had no known decoding algorithm to go with it and our goal in [LTZ15] was to tackle this very problem.

3.2.2 Results and implications

We devised a decoding algorithm for the product codes [TZ14] that runs in linear time and decodes an arbitrary pattern of errors of any weight up to a constant fraction of the minimum distance, *i.e.*, $cn^{1/2}$ for some constant $c > 0$. Our decoding algorithm is inspired by that of Sipser and Spielman [SS96] which applies to classical LDPC codes whose Tanner graph is an expander graph. The quantum codes under consideration here are products (in a well-defined sense) of a classical LDPC code $\mathcal{C}$ with itself, and we take the original code $\mathcal{C}$ to be an expander code. The resulting Tanner graphs of the two classical codes $\mathcal{C}_X$ and $\mathcal{C}_Z$ that make up the quantum code are not strictly speaking expander graphs, but they retain enough expanding structure from the original code for a decoding algorithm to work. Arguably, this is the first time that an import from classical LDPC coding theory succeeds in decoding a quantum LDPC code from a non-constant number of errors in an adversarial setting. There are some twists to the original Sipser-Spielman decoding scheme however, since it guesses values of individual bits and we have pointed out that this strategy cannot carry through to the quantum setting. The solution is to work with *generators* rather than qubits: the generators are the row vectors of H_X and H_Z. At each iteration, the decoding algorithm looks for a pattern of qubits inside the support of a single generator that will decrease the syndrome weight.

Our results also have some significance in the area of local testability. Locally Testable Codes (LTC) play a fundamental role in complexity theory: they have the property that code membership can be verified by querying only a few bits of a word [Gol10]. More precisely, the number of constraints not satisfied by a word should be proportional to the distance of the word from the code. Given their importance, it is natural to ask whether a

quantum version of LTC exists, and to investigate their consequences for the burgeoning field of quantum Hamiltonian complexity, which studies quantum satisfaction problems [GHLS14].

Quantum LTC were recently defined in [AE13b], and these hypothetical objects are mainly characterized by their *soundness* (or *robustness*) $R(d)$, *i.e.*, the probability that an error at distance d from the code violates a randomly chosen constraint. Ideally we would like to have this probability greater than some constant $\varepsilon > 0$ for d linear in the length n of the code. Note that a recent preprint of Hastings [Has16] exhibits codes which are almost local and have soundness inverse logarithmic in n. While we do not exhibit such quantum LTC here, we construct codes which are robust for errors at distance to the code of order $\sqrt{n}$, meaning that they violate a number of constraints which is linear in the distance. Reaching beyond the regime of moderate weight errors appears to be much harder since it is well-known that the random expander codes at the heart of our construction are not locally testable [BSHR05]. Interestingly, for our construction, better expansion translates into greater robustness. This should be seen in contrast to results in Ref. [AE13a], [AE13b], where good expansion (admittedly not of the same graph) appears to hurt the local testability of the quantum codes. We also remark that in the very recent result of [EH15], quantum codes are constructed by applying [TZ14] to classical LTC, which leads to an alternative form of robustness where errors with small syndrome weight correspond to highly entangled states.

3.2.3 Open questions

We have exhibited a linear-time decoding algorithm that corrects up to $\Omega(n^{1/2})$ *adversarial* quantum errors over n qubits. While this is the largest such asymptotic quantity to date, one would hope to break this barrier and eventually achieve correction of $\Omega(n)$ errors. If one were to do this with quantum LDPC codes, this would imply obtaining the elusive proof of existence of low-density codes with a minimum distance scaling linearly in the number of qubits.

Kovalev and Pryadko have shown [KP13] that the codes of [TZ14] have the potential to correct number of *random* depolarizing errors that scales linearly in n, with a vanishing probability of decoding error. This is without decoding complexity limitations however, and a natural question is whether the ideas of the present paper can extend to decoding $\Omega(n)$ random errors in linear or quasi-linear time.

3.3 Quantum cryptanalysis of symmetric cryptosystems

In this last section, I move away from questions related to dealing with errors in quantum information processing to ask about possible applications of quantum computers. One of the best-known such applications is Shor's factoring algorithm [Sho94] which would break most of the cryptography currently deployed. Very broadly, there are two main approaches to encrypt information transiting on the internet: *public key cryptography* which is based on the hardness of certain mathematical problems such as factoring (in

the case of RSA) or discrete-logarithm, both broken using Shor's algorithm if a universal quantum computer is available, and *symmetric cryptography* where the users exploit a short secret key to encrypt long messages. Intuitively, symmetric cryptography protocols are much less structured than RSA, and the best attack is believed to be a brute-force search of the secret key, which might be say 256-bit long. For this reason, quantum computers are expected to have limited impact on symmetric cryptography: the common wisdom is that the only possible speedup comes from Grover's search algorithm [Gro96], which provides a quadratic advantage compared to classical attacks [Ber10]. In particular, doubling the key length should be sufficient to restore the appropriate level of security. This picture turns out however, to be a little bit too simplistic, as we illustrated in two recent papers written in collaboration with Marc Kaplan, Gaëtan Leurent and María Naya-Plasencia [KLLNP16a], [KLLNP16b].

Our most striking result is that Simon's algorithm [Sim97], which is the main subroutine of Shor's algorithm, can lead to devastating attacks against many widely used modes of operation for authentication and authenticated encryption [KLLNP16a]. Simon's algorithm provides an exponential speedup for an apparently rather contrived problem involving finding the period of a boolean function. What is remarkable is that instances of this very problem occur in the context of symmetric cryptography with block ciphers, which correspond to permutations of $\{0,1\}^n$ parameterized by a secret key k. If the block cipher is assumed to be secure, it means that the only possible attack to recover the key is a brute-force search over the key space. The size of the key is typically equal to the block length, for instance 256 bits. A mode of operation is an algorithm describing how such a block cipher can be used repeatedly to securely transform a message larger than the block size. It turns out that in many cases, depending how successive blocks are processed, a periodic boolean function can appear in the description of the mode of operation. Moreover, knowing the period of the function is sufficient to compromise the security of the whole scheme. Classically, this is not a problem since one requires $\Omega(2^{n/2})$ queries to the block cipher of length n (seen as a black box) in order to recover the period. If one has a quantum access to the oracle, however, Simon's algorithm kicks in and allows the malicious party to recover the period with $O(n)$ queries, which shows that the overall security of the scheme is quite compromised.

This "fully quantum" model of attacks where an adversary can perform quantum queries to the encryption device has been studied in the literature under the names of *superposition attacks* [DFNS13], *quantum chosen message attacks* [BZ13b] or *quantum security* [Zha12]. Of course, this model is not at all realistic, and even if quantum computers were available today, our result would not imply that all these modes of operations are broken. The model is very strong since it says that if one queries the algorithm with a superposition of quantum inputs, then the output is the superposition of the outputs. More precisely, if the oracle returns $\mathcal{O}_k(x)$ for the input x, where k is the secret key, then the quantum oracle is assumed to prepare the state $\frac{1}{2^{n/2}}\sum_x |x\rangle|\mathcal{O}_k(x)\rangle$ when queried with the uniform superposition $\frac{1}{2^{n/2}}\sum_x |x\rangle|0\rangle$. It is rather unclear how to query a physical device in such a quantum manner, and quite hard to imagine that there exists a way to prevent decoherence to ensure that this superposition is indeed

prepared. This is certainly true but there are at least two reasons for caring about such a model. First, in the future, assuming that quantum computers exist (which is a prerequisite for this study in the first place), it will make sense to design encryption schemes that can deal with quantum messages. In that case, our results show that the schemes currently deployed are vulnerable against quantum attacks relying on Simon's algorithm. The second reason why this model makes sense is that coming up with natural models of attacks that would be intermediate between the "all-classical" model and the "fully-quantum" model is nontrivial. How should one describe the behaviour of an encryption circuit when it is probed quantumly? It seems that requiring that full decoherence takes place immediately leads to a very weak model. Allowing the superposition to be preserved throughout is certainly unrealistic, but leads to a very *clean* model and security in this model certainly implies security in all other possible attack models one might want to consider. Let us finally point out that certain constructions of message authenticated codes are known to remain secure in that model [BZ13a].

Our second result deals with "quantizing" well-known cryptanalysis techniques that have been developed against block ciphers [KLLNP16b]. These are clever techniques that sometimes allow to recover the key without exploring the whole key space. One such example is differential cryptanalysis [BS90]. These techniques are very useful for the design of new cryptosystems. Indeed, many block ciphers consist of applying many "rounds" of a simple transformation. The security of the cipher usually increases with the number of rounds, but of course, so is its complexity. For this reason, it is crucial to be able to choose the appropriate compromise between security and complexity. This is where cryptanalysis techniques come into play: they allow one to test the security of toy cryptosystems with a small number of rounds, and choose the number of rounds of the final design appropriately. In our project, we considered two models of quantum attacks: one similar to the fully-quantum model described above where one can query the oracle in superposition, and a second one where all queries are classical but the adversary has access to a quantum computer to process this classical data. Our techniques rely on the framework of quantum walks and we often obtain a quadratic speed-up compared to classical attacks, but not always. In fact, the situation is rather nuanced and the speed-up we obtain depend on the specific variants of the attacks that are considered. In particular, picking the best classical attack and applying a quadratic speed-up is not the right way to analyse the security of block ciphers in a world where quantum computers exist.

The conclusion of this work is that the claim that the only impact of quantum computing to the cryptanalysis of symmetric cryptography is restricted to the use of Grover's algorithm is not justified. For instance, in some models, it is possible to obtain an exponential speed-up over the best classical attacks, which is much more problematic than the quadratic speed-up promised by Grover. A difficulty here in contrast to the case of public key cryptography is that the security model matters a lot: how should one model that an adversary has access to a universal quantum computer? The fully quantum model is certainly very strong, but presents the advantage of encompassing all reasonable attack models. The question is then to develop cryptosystems that remain secure in that model.

Some already exist for some specific functionalities and it seems worthwhile investigating this problem further.

Conclusion

We end by mentioning some open problems that seem worth studying in the coming years:

- **on continuous-variable quantum cryptography:** our recent results on Gaussian de Finetti theorem unveiled a duality between the groups $U(n)$ and $SU(p,q)$ acting on the $n(p+q)$-mode Hilbert space $F_{p,q,n}$. While we exclusively focused on the symmetric subspace $F_{p,q,n}^{U(n)}$ because of its natural application to cryptography, it is tempting to investigate this duality further. In particular, the Schur-Weyl duality between $U(d)$ and the symmetric group S_n acting on $(\mathbb{C}^d)^{\otimes n}$ is a powerful tool in the context of quantum information, with more applications that the symmetric subspace. For this reason, it would be interesting to better understand the duality between $U(n)$ and $SU(p,q)$ beyond the study of $F_{p,q,n}^{U(n)}$.

- **on relativistic cryptography:** a natural follow-up of our work on bit commitment is to consider quantum cheating strategies. While we can prove the security of this protocol against quantum adversaries in the single-round case, which leads for instance to zero-knowledge proofs for NP, our proof techniques currently don't extend to several rounds. For this reason, we only obtain arbitrarily long commitment times when restricting adversaries to performing classical strategies, and it is a major open question to understand what is the power of entangled strategies in this context.

- **on quantum error correcting codes:** a natural follow-up question on our work on quantum expander codes is to investigate the behaviour of our efficient decoding algorithm against random errors. In particular, is there a finite value $p_0 > 0$ such that the decoder corrects all errors with high probability for the depolarizing channel of parameter $p \leq p_0$? If true, this would have important applications in the theory of quantum fault-tolerance computation as such codes would reduce the overhead imposed by a fault-tolerant construction. A second question of great interest is to better understand whether good quantum LDPC codes exist, *i.e.* codes with constant rate and linear minimum distance. Right now, the best minimum distance for quantum LDPC codes scales like $n^{1/2}\log^{1/4} n$ [FML02] while some codes are conjectured to achieve a minimum distance of $n^{1-\varepsilon}$ for any $\varepsilon > 0$ [Has16].

Bibliography

[AA13] Scott Aaronson and Alex Arkhipov. The computational complexity of linear optics. *Theory of Computing*, 9(4):143–252, 2013.

[AE13a] Dorit Aharonov and Lior Eldar. Commuting local Hamiltonians on expanders, locally testable quantum codes, and the qPCP conjecture. *arXiv preprint arXiv:1301.3407*, 2013.

[AE13b] Dorit Aharonov and Lior Eldar. Quantum locally testable codes. *arXiv preprint arXiv:1310.5664*, 2013.

[AFLS15] A Acín, T Fritz, A Leverrier, and AB Sainz. A combinatorial approach to nonlocality and contextuality. *Communications in Mathematical Physics*, 334(2):533–628, 2015.

[BB84] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, volume 175, 1984.

[BCF+11] Harry Buhrman, Nishanth Chandran, Serge Fehr, Ran Gelles, Vipul Goyal, Rafail Ostrovsky, and Christian Schaffner. Position-based quantum cryptography: Impossibility and constructions. In *Advances in Cryptology–CRYPTO 2011*, pages 429–446. Springer, 2011.

[BCP+13] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani, and Stephanie Wehner. Bell nonlocality. *arXiv preprint arXiv:1303.2849*, 2013.

[Ber10] Daniel J. Bernstein. Grover vs. McEliece. In Nicolas Sendrier, editor, *Post-Quantum Cryptography, Third International Workshop, PQCrypto 2010, Darmstadt, Germany, May 25-28, 2010. Proceedings*, volume 6061 of *Lecture Notes in Computer Science*, pages 73–80. Springer, 2010.

[BFRK+13] Matthew A Broome, Alessandro Fedrizzi, Saleh Rahimi-Keshari, Justin Dove, Scott Aaronson, Timothy C Ralph, and Andrew G White. Photonic boson sampling in a tunable circuit. *Science*, 339(6121):794–798, 2013.

[BFS11] Mario Berta, Fabian Furrer, and Volkher B Scholz. The smooth entropy formalism on von neumann algebras. *arXiv preprint arXiv:1107.5460*, 2011.

[BK11] Salman Beigi and Robert König. Simplified instantaneous non-local quantum computation with applications to position-based cryptography. *New Journal of Physics*, 13(9):093036, 2011.

[Blu86] Manuel Blum. How to prove a theorem so no one else can claim it. In *Proceedings of the International Congress of Mathematicians*, volume 1, page 2. Citeseer, 1986.

[BM05] H. Buhrman and S. Massar. Causality and tsirelson's bounds. *Phys. Rev. A*, 72:052103, Nov 2005.

[BOGKW88] Michael Ben-Or, Shafi Goldwasser, Joe Kilian, and Avi Wigderson. Multi-prover interactive proofs: How to remove intractability assumptions. In *Proceedings of the twentieth annual ACM symposium on Theory of computing*, pages 113–131. ACM, 1988.

[BS90] Eli Biham and Adi Shamir. Differential cryptanalysis of des-like cryptosystems. In Alfred Menezes and Scott A. Vanstone, editors, *Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings*, volume 537 of *Lecture Notes in Computer Science*, pages 2–21. Springer, 1990.

[BS15] Mohammad Bavarian and Peter W. Shor. Information causality, szemerédi-trotter and algebraic variants of chsh. In *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science*, ITCS '15, pages 123–132, New York, NY, USA, 2015. ACM.

[BSHR05] Eli Ben-Sasson, Prahladh Harsha, and Sofya Raskhodnikova. Some 3CNF properties are hard to test. *SIAM Journal on Computing*, 35(1):1–21, 2005.

[BZ13a] Dan Boneh and Mark Zhandry. Quantum-secure message authentication codes. In *Advances in Cryptology - EUROCRYPT 2013, 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings*, pages 592–608, 2013.

[BZ13b] Dan Boneh and Mark Zhandry. Secure signatures and chosen ciphertext security in a quantum computing world. In *Advances in Cryptology - CRYPTO 2013 - 33rd Annual Cryptology Conference, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part II*, pages 361–379, 2013.

[CBTW15] Patrick J Coles, Mario Berta, Marco Tomamichel, and Stephanie Wehner. Entropic uncertainty relations and their applications. *arXiv preprint arXiv:1511.04857*, 2015.

[CCL15] Kaushik Chakraborty, André Chailloux, and Anthony Leverrier. Arbitrarily long relativistic bit commitment. *Physical Review Letters*, 115(25):250501, 2015.

[CCL16] Kaushik Chakraborty, André Chailloux, and Anthony Leverrier. Robust relativistic bit commitment. *Physical Review A*, 94(6):062314, 2016.

[CGMO09] Nishanth Chandran, Vipul Goyal, Ryan Moriarty, and Rafail Ostrovsky. Position based cryptography. In *Advances in Cryptology-CRYPTO 2009*, pages 391–407. Springer, 2009.

[CKMR07] M. Christandl, R. König, G. Mitchison, and R. Renner. One-and-a-half quantum de finetti theorems. *Communications in mathematical physics*, 273(2):473–498, 2007.

[CKR09] Matthias Christandl, Robert König, and Renato Renner. Postselection Technique for Quantum Channels with Applications to Quantum Cryptography. *Phys. Rev. Lett.*, 102(2):020504, 2009.

[CL15] Kaushik Chakraborty and Anthony Leverrier. Practical position-based quantum cryptography. *Physical Review A*, 92(5):052304, 2015.

[CL16] André Chailloux and Anthony Leverrier. Relativistic (or 2-prover 1-round) zero-knowledge protocol for NP secure against quantum adversaries. *arXiv preprint arXiv:1612.07627*, 2016.

[COR+13] Andrea Crespi, Roberto Osellame, Roberta Ramponi, Daniel J Brod, Ernesto F Galvao, Nicolò Spagnolo, Chiara Vitelli, Enrico Maiorino, Paolo Mataloni, and Fabio Sciarrino. Experimental boson sampling in arbitrary integrated photonic circuits. *Nature Photonics*, 7:545, 2013.

[CSST11] Claude Crépeau, Louis Salvail, Jean-Raymond Simard, and Alain Tapp. Two provers in isolation. In *Advances in Cryptology–ASIACRYPT 2011*, pages 407–430. Springer, 2011.

[CSW10] Adán Cabello, Simone Severini, and Andreas Winter. (non-) contextuality of physical theories as an axiom. *arXiv preprint arXiv:1010.2163*, 2010.

[CSW14] Adán Cabello, Simone Severini, and Andreas Winter. Graph-theoretic approach to quantum correlations. *Physical Review Letters*, 112(4):040401, 2014.

[Del13] Nicolas Delfosse. Tradeoffs for reliable quantum information storage in surface codes and color codes. In *Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on*, pages 917–921. IEEE, 2013.

[DFNS13] Ivan Damgård, Jakob Funder, Jesper Buus Nielsen, and Louis Salvail. Superposition attacks on cryptographic protocols. In *Information Theoretic Security - 7th International Conference, ICITS 2013, Singapore, November 28-30, 2013, Proceedings*, pages 142–161, 2013.

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

[DLTW08] Andrew C. Doherty, Yeong-Cherng Liang, Ben Toner, and Stephanie Wehner. The quantum moment problem and bounds on entangled multi-prover games. In *Computational Complexity, 2008. CCC'08. 23rd Annual IEEE Conference on*, pages 199–210. IEEE, 2008.

[Edm65] Jack Edmonds. Paths, trees, and flowers. *Canadian Journal of mathematics*, 17(3):449–467, 1965.

[EH15] Lior Eldar and Aram W Harrow. Local hamiltonians whose ground states are hard to approximate. *arXiv preprint arXiv:1510.02082*, 2015.

[Eke91] A.K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67(6):661–663, 1991.

[FBT+14] Fabian Furrer, Mario Berta, Marco Tomamichel, Volkher B Scholz, and Matthias Christandl. Position-momentum uncertainty relations in the presence of quantum memory. *Journal of Mathematical Physics*, 55(12):122205, 2014.

[FF15] Serge Fehr and Max Fillinger. On the composition of two-prover commitments, and applications to multi-round relativistic commitments. *arXiv preprint arXiv:1507.00240v1*, 2015.

[FFB+12] Fabian Furrer, Torsten Franz, Mario Berta, Anthony Leverrier, Volkher B Scholz, Marco Tomamichel, and Reinhard F Werner. Continuous variable quantum key distribution: Finite-key analysis of composable security against coherent attacks. *Phys. Rev. Lett.*, 109(10):100502, 2012.

[Fin82] Arthur Fine. Hidden variables, joint probability, and the bell inequalities. *Phys. Rev. Lett.*, 48(5):291–295, 1982.

[FLS13] Tobias Fritz, Anthony Leverrier, and Ana Belén Sainz. Probabilistic models on contextuality scenarios. In *Proceedings of the 10th International Workshop on Quantum Physics and Logic*, 2013.

[FML02] Michael H Freedman, David A Meyer, and Feng Luo. Z2-systolic freedom and quantum codes. *Mathematics of quantum computation, Chapman & Hall/CRC*, pages 287–320, 2002.

[FR81] David James Foulis and Charles Hamilton Randall. Empirical logic and tensor products. *Interpretations and foundations of quantum theory*, pages 9–20, 1981.

[FSA+13] Tobias Fritz, Ana Belén Sainz, Remigiusz Augusiak, Jonatan Bohr Brask, Rafael Chaves, Anthony Leverrier, and A Acín. Local orthogonality: a multipartite principle for correlations. *Nature Communications*, 4(2263), 2013.

[GC99] Daniel Gottesman and Isaac L Chuang. Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations. *Nature*, 402(6760):390–393, 1999.

[GCW+03] F. Grosshans, N.J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. *QIC*, 3(Sp. Iss. SI):535–552, 2003.

[GG02a] F. Grosshans and P. Grangier. Reverse reconciliation protocols for quantum cryptography with continuous variables. *Arxiv preprint quant-ph/0204127*, 2002.

[GG02b] Frédéric Grosshans and Philippe Grangier. Continuous Variable Quantum Cryptography Using Coherent States. *Phys. Rev. Lett.*, 88(5):057902, 2002.

[GHLS14] Sevag Gharibian, Yichen Huang, Zeph Landau, and Seung Woo Shin. Quantum Hamiltonian complexity. *arXiv preprint arXiv:1401.3916*, 2014.

[GL14] Larry Guth and Alexander Lubotzky. Quantum error correcting codes and 4-dimensional arithmetic hyperbolic manifolds. *Journal of Mathematical Physics*, 55(8):082202, 2014.

[Gol10] Oded Goldreich. Short locally testable codes and proofs: A survey in two parts. In *Property testing*, pages 65–104. Springer, 2010.

[Got97a] Daniel Gottesman. Stabilizer codes and quantum error correction. *PhD Thesis, California Institute of Technology, arXiv:quant-ph/9705052*, 1997.

[Got97b] Daniel Gottesman. *Stabilizer codes and quantum error correction.* PhD thesis, California Institute of Technology, Pasadena, CA, 1997.

[Got14] Daniel Gottesman. Fault-tolerant quantum computation with constant overhead. *Quantum Information & Computation*, 14(15-16):1338–1372, 2014.

[GPC06] Raúl García-Patrón and Nicolas J. Cerf. Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution. *Phys. Rev. Lett.*, 97:190503, Nov 2006.

[Gro96] Lov K Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pages 212–219. ACM, 1996.

[GWAN11] Rodrigo Gallego, Lars Erik Würflinger, Antonio Acín, and Miguel Navascués. Quantum correlations require multipartite information principles. *Phys. Rev. Lett.*, 107(21):210403, 2011.

[Har13] Aram W Harrow. The church of the symmetric subspace. *arXiv preprint arXiv:1308.6595*, 2013.

[Has14] Matthew B Hastings. Decoding in hyperbolic spaces: quantum LDPC codes with linear rate and efficient error correction. *Quantum Information & Computation*, 14(13-14):1187–1202, 2014.

[Has16] MB Hastings. Quantum codes from high-dimensional manifolds. *arXiv preprint arXiv:1608.05089*, 2016.

[Hel79] Sigurdur Helgason. *Differential geometry, Lie groups, and symmetric spaces*, volume 80. Academic press, 1979.

[HOM87] CK Hong, ZY Ou, and Leonard Mandel. Measurement of subpicosecond time intervals between two photons by interference. *Physical Review Letters*, 59(18):2044–2046, 1987.

[How15] Mark Howard. Maximum nonlocality and minimum uncertainty using magic states. *Physical Review A*, 91(4):042103, 2015.

[IH08] Satoshi Ishizaka and Tohya Hiroshima. Asymptotic teleportation scheme as a universal programmable quantum processor. *Physical review letters*, 101(24):240501, 2008.

[JKJDL12] Paul Jouguet, Sébastien Kunz-Jacques, Eleni Diamanti, and Anthony Leverrier. Analysis of imperfections in practical continuous-variable quantum key distribution. *Phys. Rev. A*, 86(3):032309, 2012.

[Ken99] Adrian Kent. Unconditionally secure bit commitment. *Phys. Rev. Lett.*, 83:1447–1450, Aug 1999.

[Ken05] Adrian Kent. Secure classical bit commitment using fixed capacity communication channels. *Journal of Cryptology*, 18(4):313–335, 2005.

[Ken11] Adrian Kent. Unconditionally secure bit commitment with flying qudits. *New Journal of Physics*, 13(11):113015, 2011.

[Ken12a] Adrian Kent. Quantum tasks in minkowski space. *Classical and Quantum Gravity*, 29(22):224013, 2012.

[Ken12b] Adrian Kent. Unconditionally secure bit commitment by transmitting measurement outcomes. *Phys. Rev. Lett.*, 109:130501, Sep 2012.

[KLLNP16a] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. In *Annual Cryptology Conference*, pages 207–237. Springer, 2016.

[KLLNP16b] Marc Kaplan, Gaëtan Leurent, Anthony Leverrier, and María Naya-Plasencia. Quantum differential and linear cryptanalysis. *IACR Transactions on Symmetric Cryptology*, 2016(1):71–94, 2016.

[KMS11] Adrian Kent, William J Munro, and Timothy P Spiller. Quantum tagging: Authenticating location via quantum information and relativistic signaling constraints. *Physical Review A*, 84(1):012326, 2011.

[KP13] Alexey A Kovalev and Leonid P Pryadko. Fault tolerance of quantum low-density parity check codes with sublinear distance scaling. *Physical Review A*, 87(2):020304, 2013.

[KRS09] R König, Renato Renner, and Christian Schaffner. The operational meaning of min-and max-entropy. *Information Theory, IEEE Transactions on*, 55(9):4337–4347, 2009.

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

[Lau09] Monique Laurent. Sums of squares, moment matrices and optimization over polynomials. In *Emerging applications of algebraic geometry*, pages 157–270. Springer, 2009.

[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, and Philippe Grangier. Quantum key distribution over 25 km with an all-fiber continuous-variable system. *Phys. Rev. A*, 76(4), 2007.

[LC97] Hoi-Kwong Lo and H. F. Chau. Is quantum bit commitment really possible? *Phys. Rev. Lett.*, 78(17):3410–3413, Apr 1997.

[Lev15] Anthony Leverrier. Composable security proof for continuous-variable quantum key distribution with coherent states. *Phys. Rev. Lett.*, 114:070501, Feb 2015.

[Lev16] Anthony Leverrier. $su(p, q)$ coherent states and gaussian de finetti theorems. *arXiv preprint arXiv:1612.05080*, 2016.

[Lev17] Anthony Leverrier. Security of continuous-variable quantum key distribution via a gaussian de finetti reduction. *Phys. Rev. Lett.*, 118:200501, May 2017.

[LGP15] Anthony Leverrier and Raúl García-Patrón. Analysis of circuit imperfections in bosonsampling. *Quantum Information & Computation*, 15(5-6):0489–0512, 2015.

[LGPRC13] Anthony Leverrier, Raúl García-Patrón, Renato Renner, and Nicolas J. Cerf. Security of continuous-variable quantum key distribution against general attacks. *Phys. Rev. Lett.*, 110:030502, Jan 2013.

[LKB+13] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden. Experimental bit commitment based on quantum communication and special relativity. *Phys. Rev. Lett.*, 111:180504, Nov 2013.

[LKB+15] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, S. Wehner, and H. Zbinden. Practical relativistic bit commitment. *Phys. Rev. Lett.*, 115:030502, Jul 2015.

[LKGC09] A. Leverrier, E. Karpov, P. Grangier, and N.J. Cerf. Security of continuous-variable quantum key distribution: towards a de Finetti theorem for rotation symmetry in phase space. *New J. Phys.*, 11(11):115009, 2009.

[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.

[LTZ15] Anthony Leverrier, Jean-Pierre Tillich, and Gilles Zémor. Quantum expander codes. In *Foundations of Computer Science (FOCS), 2015 IEEE 56th Annual Symposium on*, pages 810–824. IEEE, 2015.

[Mal10] Robert A Malaney. Quantum location verification in noisy channels. *arXiv preprint arXiv:1004.4689*, 2010.

[May97] Dominic Mayers. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.*, 78(17):3414–3417, Apr 1997.

[Mur16] Plinio GP Murillo. Systole of congruence coverings of arithmetic hyperbolic manifolds. *arXiv preprint arXiv:1610.03870*, 2016.

[NGA06] Miguel Navascués, Frédéric Grosshans, and Antonio Acín. Optimality of Gaussian Attacks in Continuous-Variable Quantum Cryptography. *Phys. Rev. Lett.*, 97(19):190502, 2006.

[NPA07] Miguel Navascués, Stefano Pironio, and Antonio Acín. Bounding the set of quantum correlations. *Phys. Rev. Lett.*, 98(1):010401, 2007.

[NW10] Miguel Navascués and Harald Wunderlich. A glance beyond the quantum model. *Proceedings of the Royal Society A*, 466(2115):881–890, 2010.

[OFV09] Jeremy L O'Brien, Akira Furusawa, and Jelena Vučković. Photonic quantum technologies. *Nature Photonics*, 3(12):687–695, 2009.

[PC08] David Poulin and Yeojin Chung. On the iterative decoding of sparse quantum codes. *Quantum Information and Computation*, 8:987, 2008.

[Per72] AM Perelomov. Coherent states for arbitrary Lie group. *Communications in Mathematical Physics*, 26(3):222–236, 1972.

[Per86] Askold Perelomov. *Generalized coherent states and their applications*. Springer, 1986.

[PNA10] Stefano Pironio, Miguel Navascués, and Antonio Acin. Convergent relaxations of polynomial optimization problems with noncommuting variables. *SIAM Journal on Optimization*, 20(5):2157–2180, 2010.

[PPK+09] Marcin Pawlowski, Tomasz Paterek, Dagomir Kaszlikowski, Valerio Scarani, Andreas Winter, and Marek Zukowski. Information causality as a physical principle. *Nature*, 461:1101–1104, 2009.

[PR14] Christopher Portmann and Renato Renner. Cryptographic security of quantum key distribution. *arXiv preprint arXiv:1409.3525*, 2014.

[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. *Physical Review X*, 5(4):041009, 2015.

[Ral99] T. C. Ralph. Continuous variable quantum cryptography. *Phys. Rev. A*, 61(1):010303(R), 1999.

[RAM16] Ravishankar Ramanathan, Remigiusz Augusiak, and Gláucia Murta. Generalized xor games with d outcomes and the task of nonlocal computation. *Physical Review A*, 93(2):022333, 2016.

[RC09] R. Renner and J. I. Cirac. de Finetti Representation Theorem for Infinite-Dimensional Quantum Systems and Applications to Quantum Cryptography. *Phys. Rev. Lett.*, 102(11):110504, 2009.

[Ren07] R. Renner. Symmetry of large physical systems implies independence of subsystems. *Nat. Phys.*, 3(9):645–649, 2007.

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

[RG15] Jérémy Ribeiro and Frédéric Grosshans. A tight lower bound for the bb84-states quantum-position-verification protocol. *arXiv preprint arXiv:1504.07171*, 2015.

[Roh12] Peter P Rohde. Optical quantum computing with photons of arbitrarily low fidelity and purity. *Physical Review A*, 86(5):052321, 2012.

[RR12] Peter P Rohde and Timothy C Ralph. Error tolerance of the boson-sampling model for linear optics quantum computing. *Physical Review A*, 85(2):022332, 2012.

[RSA78] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Commun. ACM*, 21(2):120–126, February 1978.

[RZBB94] Michael Reck, Anton Zeilinger, Herbert J Bernstein, and Philip Bertani. Experimental realization of any discrete unitary operator. *Physical Review Letters*, 73(1):58, 1994.

[SBC+15] Daniel BS Soh, Constantin Brif, Patrick J Coles, Norbert Lütkenhaus, Ryan M Camacho, Junji Urayama, and Mohan Sarovar. Self-referenced continuous-variable quantum key distribution protocol. *Physical Review X*, 5(4):041010, 2015.

[SBPC+09] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81(3):1301, 2009.

[Sch04] Stefan Scheel. Permanents in linear optical networks. *arXiv preprint quant-ph/0406127*, 2004.

[SFA+13] A. B. Sainz, T. Fritz, R. Augusiak, J. Bohr Brask, R. Chaves, A. Leverrier, and A. Acín. Exploring the local orthogonality principle. *arXiv preprint arXiv:1311.6699*, 2013.

[SFA+14] Ana Belén Sainz, Tobias Fritz, Remigiusz Augusiak, J Bohr Brask, Rafael Chaves, Anthony Leverrier, and Antonio Acín. Exploring the local orthogonality principle. *Physical Review A*, 89(3):032117, 2014.

[Sho94] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. In *IEEE Symposium on Foundations of Computer Science*, pages 124–134, 1994.

[Sim97] Daniel R Simon. On the power of quantum computation. *SIAM journal on computing*, 26(5):1474–1483, 1997.

[Sim07] Jean-Raymond Simard. Classical and quantum strategies for bit commitment schemes in the two-prover model. Master's thesis, McGill University, 2007.

[SMH+13] Justin B Spring, Benjamin J Metcalf, Peter C Humphreys, W Steven Kolthammer, Xian-Min Jin, Marco Barbieri, Animesh Datta, Nicholas Thomas-Peter, Nathan K Langford, Dmytro Kundys, et al. Boson sampling on a photonic chip. *Science*, 339(6121):798–801, 2013.

[SS96] Michael Sipser and Daniel A Spielman. Expander Codes. *IEEE Transactions on Information Theory*, 42(6):1710–1722, 1996.

[TCR09] Marco Tomamichel, Roger Colbeck, and Renato Renner. A fully quantum asymptotic equipartition property. *Information Theory, IEEE Transactions on*, 55(12):5840–5847, 2009.

[TDH+13] Max Tillmann, Borivoje Dakić, René Heilmann, Stefan Nolte, Alexander Szameit, and Philip Walther. Experimental boson sampling. *Nature Photonics*, 7:540, 2013.

[TFKW13] Marco Tomamichel, Serge Fehr, Jedrzej Kaniewski, and Stephanie Wehner. One-sided device-independent qkd and position-based cryptography from monogamy games. In *Advances in Cryptology–EUROCRYPT 2013*, pages 609–625. Springer, 2013.

[TL15] Marco Tomamichel and Anthony Leverrier. A rigorous and complete proof of finite key security of quantum key distribution. *arXiv preprint arXiv:1506.08458*, 2015.

[TLGR12] Marco Tomamichel, Charles Ci Wen Lim, Nicolas Gisin, and Renato Renner. Tight finite-key analysis for quantum cryptography. *Nat. Comm.*, 3:634, 2012.

[TR11] Marco Tomamichel and Renato Renner. Uncertainty relation for smooth entropies. *Physical review letters*, 106(11):110506, 2011.

[Tro12] Joel A Tropp. User-friendly tail bounds for sums of random matrices. *Foundations of Computational Mathematics*, 12(4):389–434, 2012.

[TSSR11] M. Tomamichel, C. Schaffner, A. Smith, and R. Renner. Leftover hashing against quantum side information. *Information Theory, IEEE Transactions on*, 57(8):5524–5535, Aug 2011.

[TZ14] Jean-Pierre Tillich and Gilles Zémor. Quantum LDPC codes with positive rate and minimum distance proportional to the square root of the blocklength. *IEEE Transactions on Information Theory*, 60(2):1193–1202, 2014.

[Unr12] Dominique Unruh. Quantum proofs of knowledge. In *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, pages 135–152, 2012.

[Unr14] Dominique Unruh. Quantum position verification in the random oracle model. In *Advances in Cryptology–CRYPTO 2014*, pages 1–18. Springer Berlin Heidelberg, 2014.

[Vai03] Lev Vaidman. Instantaneous measurement of nonlocal variables. *Phys. Rev. Lett.*, 90:010402, Jan 2003.

[vD05] Wim van Dam. Implausible consequences of superstrong nonlocality. *arXiv preprint quant-ph/0501159*, 2005.

[VMH+16] Ephanielle Verbanis, Anthony Martin, Raphaël Houlmann, Gianluca Boso, Félix Bussières, and Hugo Zbinden. 24-hour relativistic bit commitment. *Physical Review Letters*, 117(14):140506, 2016.

[Wat16] John Watrous. *Theory of quantum information.* 2016.

[WGC06] Michael M. Wolf, Geza Giedke, and J. Ignacio Cirac. Extremality of Gaussian Quantum States. *Phys. Rev. Lett.*, 96(8):080502, 2006.

[Wil09] Alexander Wilce. Test spaces. *Handbook of quantum logic and quantum structures: quantum logic*, page 443, 2009.

[Win99] Andreas Winter. Coding theorem and strong converse for quantum channels. *IEEE Transactions on Information Theory*, 45(7):2481–2485, 1999.

[WLB+04] Christian Weedbrook, Andrew M. Lance, Warwick P. Bowen, Thomas Symul, Timothy C. Ralph, and Ping Koy Lam. Quantum cryptography without switching. *Phys. Rev. Lett.*, 93(17):170504, Oct 2004.

[Zha12] Mark Zhandry. How to construct quantum random functions. In *53rd Annual IEEE Symposium on Foundations of Computer Science, FOCS 2012, New Brunswick, NJ, USA, October 20-23, 2012*, pages 679–687, 2012.