Device-independent certification : quantum resources and quantum key distribution

Xavier Valcarce

université
PARIS-SACLAY

Device-independent certification: quantum resources and quantum key distribution

Certification «boîte noire»: ressources quantiques et distribution quantique de clé

Thèse de doctorat de l'université Paris-Saclay

École doctorale n°564 : physique en Île-de-France (PIF)
Spécialité de doctorat: Physique
Graduate School : Physique, Référent : Faculté des sciences d'Orsay

Thèse préparée à l'**Institut de Physique Théorique (Université Paris-Saclay, CNRS, CEA)** sous la direction de **Nicolas Sangouard**, professeur (CEA).

Thèse soutenue à Paris-Saclay, le 17 mai 2023, par

Xavier VALCARCE

Composition du jury

Membres du jury avec voix délibérative

Eleni DIAMANTI Directrice de recherche, Sorbonne Université, Laboratoire d'informatique (LIP6), CNRS.	Présidente
Antonio ACÍN Professeur ICREA, Institut de Ciències Fotòniques (ICFO).	Rapporteur & Examinateur
Nicolas BRUNNER Professeur Ordinaire, Département de Physique Appliquée, Université de Genève.	Rapporteur & Examinateur
Peter BROWN Assistant Professeur, Télécom Paris, Institut Polytechnique de Paris.	Examinateur

THESE DE DOCTORAT
NNT : 2023UPASP049

université PARIS-SACLAY | ÉCOLE DOCTORALE Physique en Île-de-France (PIF)

Title: Device-independent certification: quantum resources and quantum key distribution
Keywords: Quantum Information, Quantum Communication, Quantum Internet, Quantum Cryptography, Device-independent Certification, Device-independent Quantum Key Distribution

Abstract: Quantum information is a new paradigm in which quantum systems are used to carry, transfer and process information. Leveraging fundamental properties of quantum physics, quantum information protocols have been developed to enhance the capabilities of classical protocols for computation and communication tasks. In particular, non-local correlations have been used to reliably certify quantum systems and to provide unprecedented security guarantees on cryptographic protocols. These certifications and security proofs are *device-independent* – they can be formulated solely from the observed statistics of measurement results, without making assumptions on the inner-working of the quantum devices from which these results originate. In this thesis, we study two of these device-independent protocols, from their foundations to their experimental implementations. Firstly, we explore self-testing, the most fundamental device-independent protocol, which suitably certifies the functioning of quantum devices. In our effort, we highlight fundamental limits of self-testing, and widen its range of applicability. Secondly, we investigate device-independent quantum key distribution, a quantum cryptographic protocol that can be used to secure data exchange with provable security guarantees. Beside extensions of existing security proofs, we also propose a way to generate new implementation schemes which could lead to a first photonic realisation of device-independent quantum key distribution. Finally, we wrap up all of these protocols into a global perspective, showing how self-testing and quantum cryptography are complementary elements in the realisation of a quantum internet.

Titre: Certification «boîte noire»: ressources quantiques et distribution quantique de clé
Mots clés: Information Quantique, Communication Quantique, Internet Quantique, Cryptographie Quantique, Certification «boîte noire», Distribution quantique de clé de type «boîte noire»

Résumé: L'information quantique est un nouveau paradigme qui utilise des systèmes quantiques pour le transfert, l'échange et le traitement de l'information. En tirant avantage des propriétés de la physique quantique, les protocoles d'information quantique offrent des améliorations notables sur certains protocoles classiques de calculs et de communication. Grâce aux corrélations non-locales, il est possible de certifier de façon fiable des systèmes quantiques et de construire des protocoles cryptographiques avec des garanties de sécurité inégalée. Certaines de ces certifications et preuves de sécurité adoptent une approche *boîte noire* – elles peuvent être formulées à partir des statistiques de résultats de mesures, sans faire d'hypothèse sur le fonctionnement interne des appareils quantiques à l'origine de ces statistiques. Dans cette thèse, nous étudions deux de ces protocoles boîte noire, de leurs fondements à leurs réalisations expérimentales. Tout d'abord, nous explorons le self-testing, le protocole boîte noire le plus fondamental, qui certifie adéquatement le fonctionnement d'appareils quantiques. Nos recherches ont mis en lumière des limites fondamentales du self-testing et ont permis d'étendre son champ d'application. Dans un second temps, nous analysons la distribution quantique de clé de type boîte noire, un protocole de cryptographie quantique ayant une sécurité démontrable. En plus d'avoir étendu les preuves de sécurité, nous proposons également une méthode produisant des schémas expérimentaux ouvrant la voie à une première expérience photonique de distribution quantique de clés de type boîte noire. Finalement, nous inscrivons ces protocoles dans une perspective plus globale en montrant comment le self-testing et la cryptographie quantique sont des éléments-clés dans le développement d'un internet quantique.

Acknowledgements

First and foremost, I would like to express my deepest gratitude to my supervisor, Nicolas Sangouard, who, four years ago, gave me the opportunity to join his group first in Basel, then in Paris. Nicolas has always been extremely supportive and available, and his many precious advices, both scientific and personal, helped me grow a lot. I especially appreciate the efforts Nicolas has put in creating a pleasant group environment. It has been an immense joy to share all of these moments, from la Roche de Solutré to Fontainebleau. I could not have hoped for a better supervisor, Nicolas, merci du fond du coeur.

I owe big gratitude to Jean-Daniel Bancal, the friendliest co-worker who turned into an amazing co-supervisor. I am particularly thankful to Jean-Daniel for our scientific discussions and for his incredible pedagogy. Jean-Daniel has taught me a lot, his feedback on this thesis has been invaluable, and he makes a fantastic vin de noix.

I am grateful to Eleni Diamanti, Nicolas Brunner, Toni Acín and Peter Brown for accepting to be part of my jury. I am deeply indebted, in particular, to Nicolas and Toni who have introduced me to the field of quantum information back in my master and who have agreed to review this manuscript.

During my PhD I met many wonderful people. In Basel, I had fantastic colleagues in our Quantum Goptnics group: Alexey, Azadeh, Davide, Melvyn and Sebastian, thank you for being amazing colleagues. I am particularly grateful to Enky Oudot and Pavel Sekatski, who helped me a lot in Basel, both scientifically and personally. You guys also taught me how to open a beer with two standing desks. In Paris, I have been surrounded by incredible people at the Institut de Physique Théorique. Elie, Juli and Victor many thanks for being amazing office mates, Skype mates, and colleagues. Juli, our friendship has been a true fortune, from Basel to Paris, in the ups and downs. I would gladly exchange more debugging time against your culinary delicacies. Bastien, Corentin and Pierre, it has been a too short but lovely time, I wish you all a great PhD. I also want to thank the people who, all in their unique ways, made these last years memorable : Dario, Ernest, Felix, Flavio, Grégoire, Jed, Joe and Gaby, Marc-Oliver and Peter.

Supports from outside the field has been incredibly precious, and a paragraph would never be sufficient to express my gratitude. I received so much love from my friends of the CFFH and RadioMambo, thank you a thousand. Coline, Eliso, Jéri, Legzouz and his chat, Matt, Maxence and Will, time with you has been always priceless and revitalizing. A particular thanks goes to Dodo that not only has been a true friend but has also produced a beautiful artwork for this thesis. Max and Livia, danke viel viel mol. Diego, my crimpy lobster, I cherish our friendship so much, you have been an essential support through these years. To my bouldering friends from Elys and elsewhere, thank you for all the fun and the beta. Shanta, Sofie, Sobi and all my Kleibasel peeps, I owe you.

À ma famille, pépère, maman et papa, un énorme merci pour votre soutien, votre générosité et votre amour inconditionnel, je vous dois tant. Maxime et Chloé, merci mille fois pour tous ces moments à Paris, votre accueil, et votre confortable canapé-lit.

Märta, nothing that I could ever write will be grateful enough. Your love, support and understanding has been boundless, even when I didn't wake up to make your coffee. I am looking forward to go on the next adventure with you.

Contents

Acronyms

CHSH	Clauser-Horne-Shimony-Holt.
CPTP	completely-positive trace-preserving.
DIQKD	device-independent quantum key distribution.
EPR	Einstein, Podolsky and Rosen.
LO	local operations.
LOCC	local operations and classical communication.
LOSR	local operations and share randomness.
NPNR	non photon-number resolving.
POVM	positive operator-valued measurement.
PPO	proximal-policy optimization.
QKD	quantum key distribution.
RL	reinforcement learning.

Thesis overview

0.1 . Motivations and background

Physics went through a drastic paradigm change at the beginning of the 20th century. The perspective of a continuous world, provided both by the differential equations of Newtonian mechanics and by the Maxwell-Boltzmann equations, clashed with the discrete world depicted by the quantization of energy postulated by Max Planck. Moreover, our intuitive comprehension of physical objects, locally and deterministically characterized in space and time, was blown away by the fundamentally probabilistic nature of quantum theory. This led to numerous philosophical debates on the interpretation of the quantum world, with some of them still thriving nowadays. Additionally, new models widening the understanding of our surrounding were constructed from quantum physics. From quantum chemistry to the Standard model, all of these models met unprecedented success in predicting natural phenomena. Furthermore, these models enabled a myriad of new technological applications. The laser, transistors or MRIs are some famous examples of such applications. Together, these models and technologies constitute what is today known as the *first quantum revolution*.

The 1980s marked a shift in focus from understanding quantum objects to engineering and controlling them. This change was driven by the realization that some quantum behaviors could be harnessed to enhance our information processing capabilities, and led to the emergence of a new field, *quantum information processing*. Leveraging quantum entanglement, quantum communication promises cryptographic proofs based on the fundamental law of physics, while quantum computing suggests exponential performance gains for some tasks. Moreover, quantum sensing enables the resolution of physical properties with an unprecedented precision and quantum simulators will help us solve open questions that are beyond reach to our current computing capacity. In this scope, national and international alliances are pooling resources to develop and scale up quantum technologies. On the long-term, we could see the apparition of a quantum internet, connecting quantum computers, simulators and sensors, and secured by quantum communication.

In the quest towards a complex networks of quantum technologies, the capacity to reliably certify quantum technologies comes as a necessity. Certification of resources would enable the quick detection of errors and provide guarantees on the behaviour of quantum devices, crucial for security-sensitive applications. Interestingly, certification protocols can be formulated in a *device-independent* manner, i.e. without assumption on the behaviour of quantum devices. *Self-testing* is a particularly noteworthy protocol that provides a guarantee on the presence of specific states and measurements. Alternatively, for certain quantum applications,

protocols can be devised so that they only succeed if resources requirements are met. A prime example is *Device-independent quantum key distribution* (DIQKD), allowing two parties to share a secret key, with a security proof that does not rely on assumptions on the quantum devices. In the presence of interferences, whether from adversarial attacks or from faulty quantum devices, DIQKD protocols will simply abort.

In this thesis, we focus on these device-independent protocols, with an emphasis on enabling their experimental implementations. Indeed, while these protocols are promising, their realization necessitates meeting high requirements. Therefore, we begin by quantifying the resources necessary for their successful implementation. We then improve the robustness of these protocols, ultimately lowering the requirements for their implementations. Finally, we propose a method to generate new experimental designs which led to proposals well-suited for their successful realization.

0.2 . Summary of the contributions

Device-independent certification of quantum resources Self-testing enables the certification of quantum resources from observed measurement statistics. We focus on robust singlet self-testing, the self-test of two-qubit maximally entangled states in the presence of losses and noises.

Article 1 [Val+20]: We quantify resources that are necessary for robust self-testing protocols to apply. We focus on self-tests based on a single condition on the measurement statistics; the violation of the CHSH inequality. Our work lead to the discovery of a no-go condition, a minimal violation below which these robust self-tests fail. This fundamental limit improves our understanding of self-testing, shows clear experimental requirements and suggests directions for future robust singlet self-testing protocols.

Article 2 [Val+22]: From a refined analysis of the measurement statistics, we derive new robust singlet self-tests. The new protocol we propose provides a better robustness to losses and thus eases experimental realization of singlet self-testing.

Device-independent quantum key distribution Device-independent quantum key distribution protocols allow two parties to share a key in a provably secure way. Their security proof relies on conditions on the observed measurement statistics.

Article 3 [Sek+21]: We introduce a new security proof, bounding more tightly the information an eavesdropper could gather on the key. Our proof is based on two correlations functions instead of a linear combination of all correlators. The resulting key rate is higher for realistic photonic implementations and partially entangled states but does not provide a better critical efficiency.

Article 4 [Val+23]: We automatise the design of photonic experiments by combining machine learning and a custom-made simulation framework [Val21]. Applied to DIQKD, our method results in new realistic experimental blueprints, yielding both a higher key rate and a higher tolerance to losses compared to known photonic proposals.

Synthèse en français

0.3 . Motivations et contexte

La physique a connu un changement radical de paradigme au début du XXe siècle. La perspective d'un monde continu décrit à la fois par les équations différentielles de la mécanique Newtonienne et par les équations de Maxwell-Boltzmann, fut confrontée à un monde discret, dépeint par la quantification de l'énergie postulée par Max Planck. De plus, notre compréhension intuitive des objets physiques, caractérisés de manière locale et déterministe dans l'espace et le temps, a été balayée par la nature fondamentalement probabiliste de la théorie quantique. Cela engendra de nombreux débats philosophiques sur l'interprétation de la physique quantique, dont certains sont encore d'actualité aujourd'hui. Par ailleurs, de nouveaux modèles furent construits à partir de la physique quantique, nous permettant d'étendre notre compréhension du monde. De la chimie quantique au modèle standard de la physique des particules, ces modèles ont connu un succès éclatant pour la prédiction des phénomènes naturels de l'Univers. En parallèle, une myriade de nouvelles technologies issues de la mécanique quantique virent le jour. Le laser, les transistors ou encore les IRMs sont des exemples connus parmi ces applications. Ces nouveaux modèles et technologies ont marqué la *première révolution quantique*.

Dans les années 80, une nouvelle direction fut prise : nous ne cherchions plus seulement à comprendre les objets quantiques, mais à les construire et à les contrôler. Ce changement advint lorsque nous avons compris que certaines propriétés quantiques peuvent être utilisées pour augmenter nos capacités de calcul et de communication. En exploitant l'intrication quantique, la communication quantique promet des preuves de cryptographie basées sur les lois fondamentales de la physique, tandis que l'informatique quantique suggère des gains exponentiels de performance pour la réalisation de certaines tâches. De plus, les capteurs quantiques permettent d'obtenir une précision jamais atteinte pour la résolution de certaines grandeurs physiques, et les simulateurs quantiques nous aideront à résoudre des problèmes au-delà de nos capacités de calcul actuelles. Dans ce contexte, des organisations nationales et internationales réunissent les ressources nécessaires au développement et à l'évolution de ces technologies quantiques. À long terme, nous pourrions voir apparaître un internet quantique reliant ordinateurs, capteurs et simulateurs quantiques, le tout communiquant de manière sécurisée grâce à la communication quantique.

Pour la réalisation d'un réseau complexe de technologies quantiques, la capacité de certifier ces technologies quantiques apparaît comme primordiale. La certification de ressources quantiques devrait permettre de détecter rapidement des

erreurs et d'attester du comportement des appareils quantiques, ce qui est critique pour les tâches sensibles en matière de sûreté. Certains protocoles de certification peuvent être réalisés dans une approche «boîte noire», c'est-à-dire sans hypothèse sur le fonctionnement interne des appareils quantiques, considérés comme des boîtes noires. L'exemple le plus notable est le *self-testing*, un protocole permettant de garantir la présence d'états quantiques et de mesures spécifiques. Pour certaines applications quantiques, il est également possible de concevoir des protocoles «boîte noire» dont leur succès est conditionné à la présence de ressources particulières. La distribution quantique de clé de type «boîte noire» est un exemple caractéristique de ce type de protocoles. Elle permet à deux parties de partager une clé secrète de chiffrement dont la preuve de sécurité ne dépend pas des appareils utilisés. Une attaque par une partie adverse ou des défauts dans les appareils utilisés engendrent inévitablement des interférences détectables par le protocole, qui s'interrompra.

Dans cette thèse, nous étudions ces protocoles «boîte noire», avec une attention particulière portée sur la facilitation de leur réalisation expérimentale. Bien que ces protocoles soient prometteurs, leur mise en œuvre nécessite le respect de nombreuses conditions. Nous commençons par déterminer les ressources fondamentales nécessaires à leur réalisation, puis nous améliorons ces protocoles pour les rendre plus résistants aux pertes, ce qui réduit les exigences sur leur réalisation expérimentale. Enfin, nous proposons une méthode pour automatiser la conception d'expériences d'optique quantique. Cela nous permettra d'obtenir de nouveaux designs bien adaptés à la réalisation de ces protocoles.

0.4 . Présentation des protocoles «boîte noire»

0.4.1 . Certification «boîte noire» de ressources quantiques

Le *self-testing*, proposé par Mayer et Yao [MY04], est la pierre angulaire des protocoles «boîte noire». Ce protocole permet à un client, disposant de ressources uniquement classiques, de certifier que des «boîtes noires», interconnectées, effectuent exactement des mesures spécifiques sur un état quantique particulier, partagé entre ces boîtes. Pour ce faire, le client choisit librement une entrée pour chacune de ces boîtes, puis enregistre les résultats en sortie. En répétant cette étape plusieurs fois, le client obtient des statistiques de mesures ou *correlations* entrées-sorties, à partir desquelles la certification peut être stipulée. En effet, il existe des conditions sur ces corrélations qui ne peuvent être satisfaites que pour un unique modèle quantique – un ensemble de mesures et d'un état. Autrement dit, il est possible de certifier la présence d'un modèle quantique si des conditions adéquates sont remplies par les statistiques de mesures, Dans cette thèse, nous nous intéressons à la certification d'un état quantique particulier, l'état de deux qubits maximalement intriqués, une ressource clé pour de nombreuses technologies quantiques. La certification de cet état quantique est réalisée à partir de la satura-

tion d'une inégalité de Bell, l'inégalité Clauser-Horne-Shimony-Holt (CHSH). Nous présentons ce protocole ainsi qu'une preuve de cette certification dans le Chap. 4.

La réalisation expérimentale du self-testing apporte de nombreuses problématiques. Dans un cas pratique, les statistiques de mesures diffèrent inévitablement de celles nécessaires à la certification de ressources quantiques. Cela est dû à différents bruits et pertes, des imperfections naturellement présentes lors de la création, de la distribution et de la mesure de l'état quantique. De plus, la collection de statistiques en un nombre fini de répétitions de l'expérience ne permet qu'une estimation des corrélations, à un intervalle près. Il apparait donc comme nécessaire d'adapter les protocoles de self-testing à ces limitations ; c'est ainsi que furent proposés les protocoles de *robust self-testing*. Cette nouvelle famille de protocole certifie une limite sur la similitude entre la ressource testée et la ressource cible. Après avoir défini la notion de similitude entre états quantiques, dans le Chap. 5, nous présentons un protocole pour la certification de l'état de deux qubits maximalement intriqués en présence d'imperfections. Nous exposons ensuite deux de nos contributions portant respectivement sur les limites de ce protocole et sur un nouveau protocole plus robuste à certaines imperfections.

0.4.2 . Distribution quantique de clé de type «boîte noire»

Les récentes avancées en informatique quantique menacent nos systèmes de chiffrement actuels. Les ordinateurs quantiques ont le potentiel de briser rapidement les algorithmes de chiffrement classiques, mettant ainsi en danger la sécurité des données sensibles. Face à cette menace, deux approches sont envisagées. La première approche est la cryptographie post-quantique, qui propose de nouveaux algorithmes résistants aux attaques quantiques connues. Cette approche présente l'avantage de ne pas nécessiter de nouvelles infrastructures, mais simplement une mise à jour de nos normes de chiffrement. Cependant, elle comporte des risques à long terme. Par exemple, un attaquant pourrait enregistrer des messages chiffrés avec ces nouveaux algorithmes en attendant une future avancée technologique ou mathématique permettant de nouvelles attaques. La seconde approche est la distribution quantique de clés (QKD), une famille de protocoles de communication quantique permettant à deux utilisateurs reliés par un canal quantique de communication, de créer et partager une clé symétrique de chiffrement. Dans ce cas, la sécurité ne dépend pas des ressources dont dispose un attaquant, mais repose sur les lois de la physique. Cette approche offre ainsi une solution aux risques à long terme.

Si la distribution quantique de clé apparait comme une approche prometteuse, son application pratique comporte des risques. La preuve de sécurité d'une implémentation de QKD repose sur un modèle physique spécifique à cette réalisation. Or, des imperfections dans les systèmes utilisés pour cette implémentation peuvent entrainer des divergences au modèle physique pris en compte, rendant ainsi la preuve de sécurité caduque. Exploitant ces imperfections, des attaques ont déjà

été menées avec succès contre des systèmes de QKD.

La distribution quantique de clé de type «boîte noire» (DIQKD) offre une solution pour éliminer la dépendance de la preuve de sécurité en l'hypothèse que l'implémentation soit conforme à un modèle physique spécifique. En effet, les protocoles de DIQKD permettent d'obtenir une preuve de sécurité dérivée uniquement à partir de statistiques de mesures. Ces protocoles sont de type «boîte noire» car ils ne nécessitent aucune hypothèse sur les systèmes quantiques à l'origine de ces statistiques – ces systèmes peuvent être donc vus comme des boîtes noires.

Dans le Chap. 6, nous présentons les ressources nécessaires à l'implémentation d'un protocole de DIQKD, puis nous détaillons les différentes étapes d'un protocole type, de l'obtention des statistiques de mesures à la production de la clé de chiffrement. Les preuves de sécurité sous forme de taux de clé sont ensuite exposées dans le Chap. 7. Nous revenons sur l'expression fondamentale de ce taux de clé, ainsi que sur son expression pour différents protocoles. Au sein de ce même chapitre, nous commentons une de nos contributions sur la DIQKD ; un nouveau protocole offrant un taux de clé avec une meilleure résistance aux pertes. Finalement, dans le Chap. 8 nous nous intéressons à la réalisation expérimentale de la DIQKD. Nous comparons d'abord les différentes plateformes privilégiées pour les expériences de DIQKD, avant d'exposer une expérience photonique servant de modèle de référence. Enfin, nous présentons la dernière de nos contributions, une nouvelle méthode permettant de générer automatiquement des designs d'expériences photoniques. Avec cette méthode appliquée à la DIQKD, nous mettons en avant deux nouveaux schémas d'expériences photoniques de DIQKD, facilitant la réalisation d'expériences de DIQKD.

0.5 . Résumé des contributions

Certification «boîte noire» de ressources quantiques

Article 1 [Val+20]: Nous quantifions les ressources nécessaires pour appliquer des protocoles de self-testing en présence d'imperfections. Nous nous concentrons sur le self-testing basé sur une seule condition que doivent respecter les statistiques de mesures ; la violation de l'inégalité CHSH. Ce travail conduit à la découverte d'une condition nécessaire : une violation minimale en dessous de laquelle le robust self-testing échoue. Cette limite fondamentale améliore notre compréhension du self-testing, définit des exigences expérimentales claires et suggère des orientations pour de futurs protocoles.

Article 2 [Val+22]: À partir d'une analyse affinée des statistiques de mesure, nous dérivons de nouveaux self-tests robustes pour le singlet. Le nouveau protocole que nous proposons offre une meilleure robustesse aux pertes et facilite ainsi la réalisation expérimentale du self-testing du singlet.

Distribution quantique de clé de type «boîte noire»

Article 3 [Sek+21]: Nous formulons une nouvelle preuve de sécurité d'un protocole DIQKD, qui limite plus justement l'information qu'un adversaire peut obtenir sur la clé distribuée. Notre preuve est basée sur deux fonctions de corrélation au lieu d'une seule combinaison linéaire de toutes les statistiques. Le taux de clé qui en découle est plus élevé pour les implémentations réalistes basées sur l'optique quantique et pour les états partiellement intriqués. Cependant, notre approche ne fournit pas une meilleure efficacité critique.

Article 4 [Val+23]: En combinant l'apprentissage machine et un framework de simulation de circuits photoniques [Val21], nous automatisons la conception d'expériences photoniques. Appliquée à la distribution quantique de clé de type «boîte noire», notre méthode propose de nouveaux designs d'expériences réalistes, offrant à la fois un taux de clé plus élevé et une tolérance plus élevée aux pertes par rapport aux propositions photoniques précédemment connues.

Organisation of the manuscript

In Part I of this thesis, we introduce key concepts of quantum information. This allows us to present the two device-independent protocols that are the focus of this thesis: self-testing and device-independent quantum key distribution (DIQKD).

Part II focuses on self-testing. In Chap. 4 we recall a method to self-test two-qubit maximally entangled states and maximally incompatible measurements from the maximal violation of the CHSH inequality. We then explore a more practical scheme in Chap. 5, robust self-testing, enabling the certification of a singlet-fraction in a noisy and lossy regime, relevant for real world applications. After introducing the core concept of extractabitliy in Sec 5.1, we focus on quantifying the fundamental resources that are required for such robust self-tests. In Sec 5.2.3, we explain how we derived a lower-bound on the CHSH-score below which robust singlet self-testing fails, assessing the need for new robust self-tests. In this scope, in Sec.5.3 we briefly review an original self-testing protocol based on a more refined analysis of the correlations, that we formulated.

Part III of the manuscript covers device-independent quantum key distribution (DIQKD). In Chap. 6, we present the steps involved in a typical DIQKD protocol. Security proofs, in the form of key rates, are then reviewed in Chap. 7. This includes the fundamental key rate expression, and a practical key rate expression that has been derived from the CHSH score. We then show some improvements that have been built on top of this key rate, notably fine-grained error-correction and noisy pre-processing. In order to ease concrete experimental realizations of DIQKD, we proposed a new security proof based on generalized-CHSH inequalities, that we briefly review in Sec. 7.3.1. Finally, a recent work that has introduced key rate based on the full statistics, yielding the best rate and robustness, is discussed in Sec 7.3.2. After reviewing the different experimental platforms that can be used to implement DIQKD, in Chap. 8 we present how we combined reinforcement learning and a custom-made simulation framework to automatise the design of photonic experiments. The results of this method when applied DIQKD is discussed in 8.3.3. Leveraging the flexibility of our approach, a new setup for the experimental violation of the CHSH inequality are presented in Sec. 8.3.4.

Finally, in Part IV, we present some conclusions on both self-testing and DIQKD and devise some perspectives for the future of these two protocols. We then suggest how these two device-independent methods should fall within the framework of a quantum internet.

Publications

This thesis is based on the following contributions.

Publications:

1. *What is the minimum CHSH score certifying that a state resembles the singlet?*
   Xavier Valcarce, Pavel Sekatski, Davide Orsucci, Enky Oudot, Jean-Daniel Bancal, and Nicolas Sangouard.
   Quantum, volume 4, page 246.

2. *Self-testing two-qubit maximally entangled states from generalized Clauser-Horne-Shimony-Holt tests*
   Xavier Valcarce, Julian Zivy, Nicolas Sangouard, and Pavel Sekatski.
   Phys. Rev. Research 4, 013049.

3. *Device-independent quantum key distribution from generalized CHSH inequalities*
   Pavel Sekatski, Jean-Daniel Bancal, Xavier Valcarce, Ernest Y.-Z. Tan, Renato Renner, and Nicolas Sangouard.
   Quantum, volume 5, page 444.

4. *Automated design of quantum optical experiments for device-independent quantum key distribution*
   Xavier Valcarce, Pavel Sekatski, Elie Gouzien, Alexey Melnikov, Nicolas Sangouard.
   Phys. Rev. A 107, 062607.

Codes:

5. QuantumOpticalCircuits.jl — Julia framework for the simulation of photonic circuits.
   https://github.com/xvalcarce/QuantumOpticalCircuits.jl

6. SPDCStats.jl — Julia package to compute statistics arising from a SPDC source and non photon-number resolving photodetectors.
   https://github.com/xvalcarce/SPDCStats.jl

I – Overview and definitions

1 - Quantum Entanglement

Quantum entanglement is often thought as one of the most bizarre feature of quantum mechanics. In 1935, it puzzled Einstein, Podolsky and Rosen (EPR) who described the phenomena in [EPR35]. The same year, Schrödinger, in his seminal paper [Sch35], coined the term *entanglement* and portrayed it as not "*one* but rather *the* characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought.".

An entangled system is described in opposition to a separable system, i.e. a system that can be fully described from the state of its individual components. Such an entangled system is allowed by the *superposition* principle and the structure of the space of joint quantum systems.

A pure quantum state $|\psi\rangle$ is represented by a vector in a Hilbert space $\mathscr{H}$. Given two pure states $|\psi^A\rangle$ and $|\psi^B\rangle$ and their respective Hilbert space $\mathscr{H}^A$ and $\mathscr{H}^B$, a separable system composed of these states can be written as the tensor product of its components

$$|\psi\rangle = |\psi^A\rangle \otimes |\psi^B\rangle \tag{1.1}$$

associated with the Hilbert space $\mathscr{H}^{AB} = \mathscr{H}^A \otimes \mathscr{H}^B$. Conversely, a state in $\mathscr{H}^{AB}$ that can not be written in the previous form is said to be entangled. The two-qubit maximally entangled states

$$\begin{aligned} |\psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ |\psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \\ |\phi^+\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ |\phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \end{aligned} \tag{1.2}$$

are famous examples of such entangled states and are known as Bell states.

More generally, convex sum of pure states, or *mixed state*, are described by the density matrix

$$\rho = \sum_i c_i |\psi_i\rangle \langle\psi_i| \qquad \text{with} \quad \sum_i c_i = 1, \quad c_i \geq 0. \tag{1.3}$$

A mixed bipartite state ρ_{AB} is said to be entangled if it can not be decomposed in a convex sum of product states

$$\rho_{AB} = \sum_i c_i \rho_i^A \otimes \rho_j^B. \tag{1.4}$$

The concept of entanglement leads to counter-intuitive predictions. Most notably, the fact that a property measured on one part of an entangled system can determine the measurement outcome of that property on the other part of such system, even if both parties are far apart. This was famously referred as a "spooky action at distance" by Einstein, and it leads to a paradox, the EPR paradox.

Quantum mechanics imposes that the values of two non-commuting observables can not be known simultaneously. For example, it is impossible to both exactly know the spin value in the x-direction and in the z-direction of a system, since these two spin observables do not commute. The EPR paradox occurs when measuring such non-commuting observables on an entangled system. Consider the entangled state $|\phi^+\rangle$, described above, to be shared between Alice and Bob. If Alice were to measure the spin in the z-direction and obtain the value $1/2$, she can assume that if Bob were to measure his system in the same manner he would also obtain $1/2$. So it seems that if Bob measures his system in the x-direction and ask Alice for the outcome of her measurement in the z-direction, he would precisely access the values of two non-commuting observables, which is paradoxical.

Believing in the complete local determination of the outcomes, Einstein, Podolsky and Rosen proposed the existence of *hidden variables* to solve this paradox.

Discussions about entanglement were at first left by physicists as a purely fundamental and philosophical problem of quantum mechanics. In 1964, John Bell devised a test to prove that quantum mechanics can not be explained by a physical theory of *local-hidden variable*, under the assumption of *free will* [Bel64]. Based on the work of John Bell, Clauser, Horne, Shimony and Holt (CHSH) made a convincing proposal for an experimental protocol to implement Bell's test [Cla+69]. This proposal was soon followed by a first experimental realisation showing evidence towards Bell's non locality [FC72], i.e. the idea that quantum correlations cannot be explained by local-hidden variable. Over time, increasingly convincing implementations of Bell's test have been reported, including the seminal experiments conducted by Alain Aspect and his colleagues in the early 1980's [ADR82; AGR82] and the experiment carried out by the Zeilinger group in the late 1990's [Wei+98]. These works were ultimately recognized by the 2022 Nobel Prize, awarded to John Clauser, Alain Aspect and Anton Zeilinger.

The work of Bell followed by experimental evidences brought back interest on entanglement. In particular, the capability to generate entangled pairs of particles led into thinking of entanglement as a quantum resource. This allowed for a variety of new technologies and the creation of a subfield of physics today known as *quantum information* (see Chap. 3). Entanglement-based technologies include quantum key distribution [Eke91], quantum computing [Pre18], quantum random numbers generators [AM16], quantum machine learning [Bia+17], and much more.

2 - Bell nonlocality

2.1 . Bell game

In order to prove the existence of correlations not compatible with a local hidden variable theory, John Bell introduced a game, known today as a *Bell game* [Bel64]. This game consists of a particle pair source and two space-like separated players, Alice and Bob, each having a measurement apparatus.

When a particle is received, Alice chooses a measurement to perform and records the outcome of that measurement. We label x her *measurement choice* or *setting*, A_x the corresponding measured observable, and a the outcome. Similarly, when he receives a particle, Bob makes a measurement choice y and obtains the outcome b from the observable B_y. This Bell game is sketched in Fig. (2.1).

The outcomes a, b are not necessarily deterministically determined by the inputs x, y. We are thus interested in the joint probability $p(ab|xy)$ of having outcomes a and b given the measurement choices x and y. For a given game, one can arrange the probabilities for every possible outcomes and inputs in a vector $\mathbf{P} = \{p(ab|xy)\}$ also refer to as *correlations*. These correlations form a set whose boundaries depend on which assumptions are fulfilled by the Bell game and which resources are considered.

Note that a spatial separation between players ensures that there is no influence between the two measurement devices while the game is played.

2.2 . Non-signalling correlations

Non-signalling correlations are correlations respecting a single assumption: the measurement choice of one party can not influence the outcome of the other party's measurement. When Alice and Bob are space-like separated, this assumption is trivially enforced by special relativity, i.e. no information can be transmitted faster-than-light.

Formally, non-signalling correlations are correlations for which the local marginals of a party are independent of the other party's measurements choice. Mathematically, such correlations satisfy

$$\begin{aligned} \sum_b p(ab|xy) = \sum_b p(ab|xy') = p(a|x), \quad \forall\, a, x, y, y' \\ \sum_a p(ab|xy) = \sum_a p(ab|x'y) = p(b|y), \quad \forall\, b, x, x', y. \end{aligned} \tag{2.1}$$

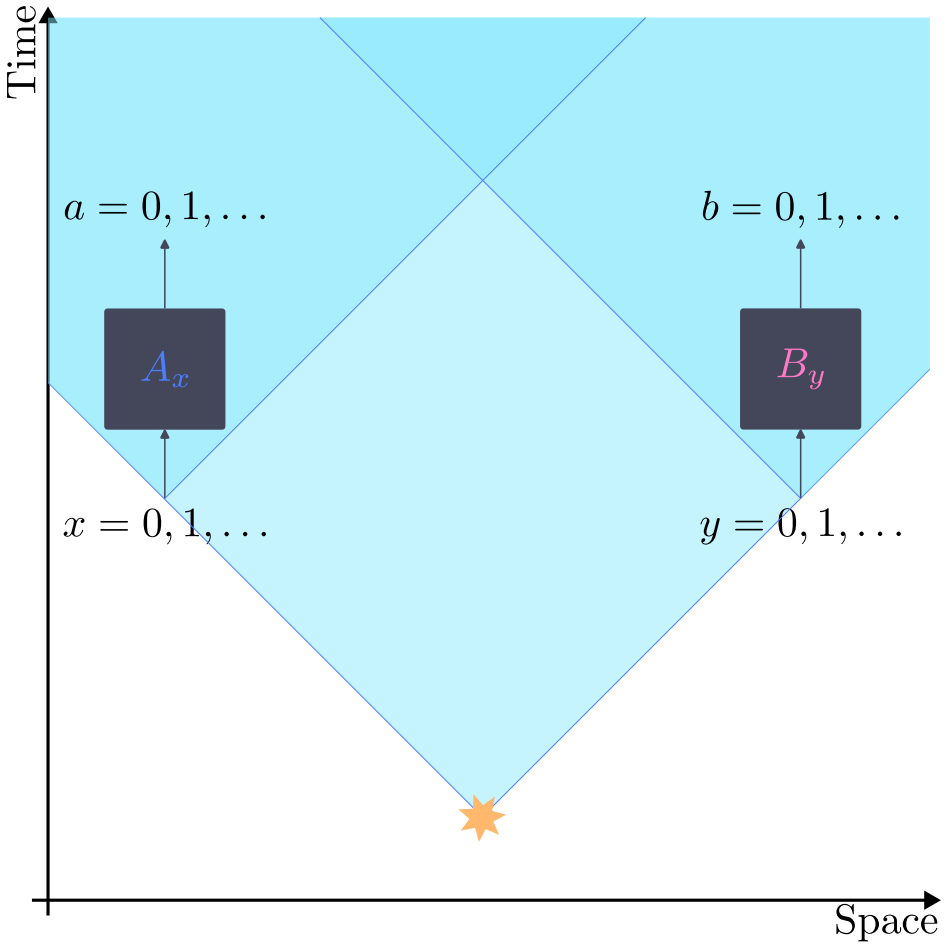


Figure 2.1: Bell game. A source (yellow star) emits a particle-pair, one send to Alice (left) and one to Bob (right). Alice chooses an input x and obtains an output a. Bob selects an input y and records the output b. The blue areas represent light-cones of different events. For a Bell test to be valid, the measurement outcome of a party has to be recorded outside the light-cone triggered by the other party's choice of setting.

2.3 . Local and non-local correlations

Local correlations are fully characterised from the local system of Alice and Bob, i.e. they are not influenced by actions outside the light cone. This type of correlation accounts for some hypothetical shared hidden information between the two parties. Since Alice and Bob's particles were in contact in the past, outcomes of their measurements can be influenced by some past factors, available locally to both parties' systems but possibly unobservable, i.e. *hidden*. These past factors are often called *local-hidden variables* and are represented by λ. Given that λ can be distributed according to $q(\lambda)$ we formally defined local correlations as any correlation that can be decomposed as

$$p(ab|xy) = \int_\lambda \mathrm{d}\lambda\, q(\lambda) p(a|x,\lambda) p(b|y,\lambda). \tag{2.2}$$

One assumption we made in writing this decomposition is the *freedom of choice* of both parties' measurements, that is x and y are independent of λ.

Interestingly, any local correlation can be written as a convex sum of deterministic local strategies, $p_D(ab|xy) = p_D(a|x)p_D(b|y)$, for which the output only depends on the input, following

$$p(ab|xy) = \sum_{p_D \in \mathcal{L}_{\mathsf{Det}}} c_{p_D} p_D(ab|xy) \tag{2.3}$$

with $c_{p_D} \geq 0$ and $\sum c_{p_D} = 1$. Here $\mathcal{L}_{\mathsf{Det}}$ is the set of all deterministic local strategies. From the previous decomposition, it follows that the convex sum of local strategies is also local. Geometrically, the set of local correlations is the convex hull of a finite number of deterministic strategies, which is a convex polytope, the *local polytope*.

Non-local correlations are defined as any correlation that does not admit a decomposition in the form of Eq. (2.2). Such correlations can thus not be explained by means of local-hidden variables. Note that this is the case for some non-signalling correlations as correlations satisfying Eq. (2.1) do not necessarily admit a decomposition of the form Eq. (2.2). However, local correlations fulfill the non-signalling assumption. See [Bru+14; Sca19] for a review on Bell nonlocality.

2.4 . Quantum correlations

Quantum correlations occur when Alice and Bob's particles are described by a quantum state ρ_{AB}. Generally, this quantum state is a mixed state laying in the Hilbert space $\mathcal{L}(\mathscr{H}^{AB} = \mathscr{H}^A \otimes \mathscr{H}^B)$. For measurement choices x, y, quantum correlations are given by the Born rule

$$p(ab|xy) = \mathrm{tr}\left[\rho_{AB} M_x^a \otimes M_y^b\right] \quad \forall\, a, b, x, y \tag{2.4}$$

where M_x^a are the positive operator-valued measurement (POVM) elements of the observable A_x associated with outcome a, and similarly for Bob with the POVM M_y^b for the observable B_y and the outcome b.

Quantum correlations satisfy the non-signalling assumption, but are not necessarily local. In order to obtain non-local quantum correlations, Alice and Bob must share an entangled state as the correlation produced by a separable state $\rho_{AB}^{\text{sep}} = \sum_i c_i \rho_i^A \otimes \rho_i^B$,

$$\begin{aligned} p(ab|xy) &= \text{tr}\left[\rho_{AB}^{\text{sep}}\, M_x^a \otimes M_y^b\right] \\ &= \sum_i c_i \ \text{tr}\left[(\rho_i^A \otimes \rho_i^B)(M_x^a \otimes M_y^b)\right] \\ &= \sum_i c_i \ \text{tr}\left[\rho_i^A M_x^a \otimes \rho_i^B M_y^b\right] \\ &= \sum_i c_i \, p_i(a|x) \, p_i(b|y) \end{aligned} \tag{2.5}$$

is of the form Eq. (2.3) and thus local. Entanglement can therefore be detected solely from the observations of non-local correlations, given that the non-signalling assumption is enforced.

2.5 . Bell inequalities

In his 1964 paper, John Bell proposed bounds satisfied by correlations that can be described with local-hidden variables theories [Bel64]. Today, these bounds are known as *Bell inequalities*. Facets of the local polytopes are examples of such Bell inequalities. When a Bell inequality is not satisfied by some correlations, we observe a *Bell violation*. Consequently, violating a Bell inequality proves the presence of non-locality and, therefore, of entanglement.

The most general expression of a Bell inequality $\mathcal{I}$ on some correlation $\mathbf{P}$ is

$$\mathcal{I}(\mathbf{P}) = \sum_{a,b,x,y} c_{abxy} p(ab|xy) \leq \beta_L \tag{2.6}$$

where β_L is the *local bound*, i.e. the maximum Bell score such that $\mathbf{P}$ satisfies Eq. (2.2).

2.6 . CHSH inequality

Clauser-Horne-Shimony-Holt (CHSH), in a effort to experimentally test Bell's theorem, proposed a more specific version of Bell's game and inequality [Cla+69]. The game, today known as the *CHSH game*, limits Alice and Bob to two dichotomic measurements, A_0, A_1 for Alice and B_0, B_1 Bob, with outcomes $a, b \in \{\pm 1\}$. A

well-suited Bell inequality for this game is the CHSH inequality

$$S = |\langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle| \leq 2 \tag{2.7}$$

where S is the *CHSH score*, and $\langle A_x B_y \rangle = \sum_{a,b} ab\, p(ab|xy)$ expresses a *correlator* – quantifying how correlated are the outcomes of two measurements. Note that correlators of a quantum state ρ_{AB} are defined using the Born rule, $\langle A_x, B_y \rangle = \mathrm{tr}\left[(A_X \otimes B_y)\rho_{AB}\right]$. It is convenient to define the CHSH operator, a Bell operator,

$$\mathcal{B}_{\mathrm{CHSH}} = A_0 \otimes (B_0 + B_1) + A_1 \otimes (B_0 - B_1) \tag{2.8}$$

from which the CHSH score can be obtain using $S = |\mathrm{tr}\left[\mathcal{B}_{\mathrm{CHSH}}\, \rho_{AB}\right]|$.

The inequality Eq. (2.7) can be used to prove the non-local nature of quantum mechanics. Consider the $|\psi^-\rangle$ Bell state, also known as the *singlet* state, shared between Alice and Bob, and the measurements

$$\begin{aligned} A_0 &= \sigma_z, & A_1 &= \sigma_x \\ B_0 &= \frac{\sigma_z + \sigma_x}{2}, & B_1 &= \frac{\sigma_z - \sigma_x}{2}. \end{aligned} \tag{2.9}$$

Computing the CHSH score from these resources yield $S = 2\sqrt{2}$ which violates the inequality. It can also be proven that $2\sqrt{2}$ is the maximum CHSH violation achievable using quantum resources [Tsi80].

3 - Quantum information

The emergence of quantum information and the second quantum revolution can be attributed to the discovery of quantum entanglement. Indeed, if quantum mechanics revolutionized technology by leveraging quantum proprieties to process classical information, mostly thanks to the invention of the transistor, there is now a shift to control individual quantum objects and use them as carrier of information. Quantum information already have numerous technological applications, from quantum computing to quantum cryptography, quantum simulation or quantum sensing to name a few. For an introduction on most quantum information concepts see [NC12].

3.1 . Device-independent quantum information processing

Quantum information processing relies heavily on quantum entanglement. It is then necessary to certify that a proposed implementation carries out some form of entanglement. A possible approach is to use quantum state tomography, which allows to reconstruct the density matrix of a quantum state [DPS03]. Another possibility is to use entanglement witnesses, characterizing the *closeness* of state to a target quantum state using specific operators, see e.g. [Bru+02]. On the downside, these two methods require precisely calibrated measurement devices, which is a major experimental challenge.

To circumvent this problem, one can use a *device-independent* approach, in which all the quantum devices used, both sources and measurement apparatus, are considered as black-boxes, i.e. no assumption is made on their inner working. As we saw in the previous chapter, a Bell inequality violation certifies the non-local nature of tested correlations and asserts the presence of entanglement . Hence, a Bell violation is a device-independent certification of entanglement, as it does not require any assumption on how the tested correlations were obtained, i.e. the inputs x, y and outputs a, b are treated as pure mathematical objects with no specific physical nature. Notice however, that such certification still requires some assumption on the Bell test itself, as measurement independence and a space-like separation between the parties' measurement events are required.

The device-independent approach advances beyond the simple certification of entanglement and is at the core of complex quantum information technologies. In this thesis we focus on two device-independent protocols. First, we study self-testing, the most fundamental device-independent protocol, enabling the device-independent certification of specific states and measurements. Then, we focus on device-independent quantum key distribution (DIQKD), one of the most peculiar application of the device-independent framework, allowing two parties to

share a secret key whose secrecy is guaranteed without making assumptions on the quantum devices used to produce that key. Another notable device-independent protocol outside the scope of this thesis is the device-independent generation of random numbers of certified quantum origin [AM16; Liu+18].

3.2 . Self-testing

Introduced by Mayers and Yao [MY04], self-testing is the cornerstone of device-independent protocols. It finds its use when a classical client, with access to multiple black-boxes, would like to certify that these boxes performed specific measurements on a specific shared quantum state producing non-local correlations. Each boxes has some inputs the client can choose freely, and some outputs they can record, that together form some correlations, similarly to a Bell game. Self-testing protocols test these correlations against a Bell inequality crafted to certify the presence of a specific state and measurements. More precisely, the maximum violation of some Bell inequalities can only be achieved by a particular family of correlations, that necessary originates from a specific state and measurements. The first self-testing protocol uses the CHSH inequality to certify the presence of maximally entangled two-qubit states [MY04]. New protocols then extended self-testing, notably to all pure bipartite entangled two-qubit states [YN13; BP15], and even to any pure bipartite entangled state [CGS17]. For a in-depth review on self-testing, see [ŠB20].

This device-independent approach is crucial when the devices used to generate the state and perform the measurement for a quantum information processing task are partially unknown, uncharacterised or untrusted. Therefore, self-testing was extended to device-independent quantum key distribution [MY04], verifiable blind quantum computing [RUV13; HPF15; McK16], certify blocks of quantum computers [Mag+06; Sek+18], or certify a quantum network link [Ban+21]. However, it is worth noting that for some device-independent protocols, correlations can be directly and more efficiently used, without resorting to self-testing.

Originally, self-testing aims at certifying exactly a given state and measurements thanks to the maximum violation of a Bell inequality, only achievable by specific correlations [MY04]. Experimentally, this is challenging as noises and losses introduce errors. Moreover, finite number of repetition rounds lead to statistical uncertainties on the correlations. To circumvent these issues, *robust self-testing* has been introduced as a mean to approximate a self-test certificate [Kan16]. Robust self-testing guarantees that if a sufficiently high Bell violation is observed, the state and measurements are *close* to the ones we want to certify. More precisely, from a high enough violation, one can expect to *extract*, from the actual state, a state close to the target one. Robust self-testing protocols were developed to decrease the requirement on the Bell violation while maintaining a certain closeness to the state to certify [Ban+15; Kan16; Kan17; Val+22].

3.3 . Device-independent quantum key distribution

As recent advances in quantum computing threaten the security of our current encryption algorithm [Sho94; GS21; Gou+23], more-than-ever is the need for stronger cryptographic protocols.

One approach is *post-quantum cryptography* (PQC), new classical cryptography protocols that are resistant to known quantum attacks. PQC is convenient as it does not require a new infrastructure, i.e. classical computers and communication links are sufficient. However, a major drawback is a poor long-term security; information encrypted using PQC can be stored for years until new quantum attacks that can break the encryption scheme are developed. Furthermore, mathematical flaws in these protocols can be discovered, ruling out their security. This recently happened to a protocol short-listed by the NIST as a candidate for PQC [CD22]. For an overview on the current state of PQC see e.g. the recent report by the European Union Agency for Cybersecurity [Cyb21].

Another approach is quantum key distribution (QKD), allowing two parties connected by a quantum channel to share a secret key [BB84; Eke91; Gis+02; Sca+09]. An important aspect of QKD is that it does not rely on computational assumptions. Instead, it leverages the fundamental laws of physics to guarantee, in principle, an unconditional security [SP00; May01]. Moreover, the no-cloning theorem forbids a malicious actor to create an independent and identical copy of the information send during a QKD protocol. This gives QKD an infinite long-term security. It is worth noting that quantum key distribution and PQC are not in competitions with each other as replacements for classical cryptography, rather, they are complementary [1].

First QKD protocols were *prepare and measure* protocols [BB84; GG02; Gro+03]. In these protocols Alice would send information encoded in a quantum state to Bob. Thanks to the no-cloning theorem and to the uncertainty principle, attacks performed by an eavesdropper to gain information on the encoded message would unavoidably lead to detectable disturbances. Alice and Bob could thus detect the eavesdropper and abort the protocol.

Another approach to QKD is entanglement-based protocols [Eke91]. In this case, Alice and Bob generate a key from the outcomes of measurements they perform on a shared entangled signal they receive. Intuitively, when using a bipartite maximally entangled state, the outcomes of Alice and Bob are fully correlated and completely random. Therefore, as the generated outcomes are identical and unpredictable on both side, they can be used to define a key.

The security of QKD protocols relies on the following assumptions

- 1. The devices used to generate the key and to attack the protocol behave

[1] QKD protocols require an authenticated channel of communication. PQC is a natural candidate to perform this authentication.

according to quantum theory,

- 2. There is no information leakage out of Alice and Bob systems, e.g. Alice and Bob are each in a hermetic laboratory,
- 3. Alice and Bob have access to random numbers,
- 4. The classical devices used to process classical information are trusted,
- 5. The quantum devices used to prepare the state and perform measurements are perfectly calibrated and behave predictably.

The level of trust in cryptography is inherently limited by the trust we place on the assumptions our cryptographic protocols rely on. To address this limitation, it is highly desirable to remove the assumption that quantum devices are trustworthy. Indeed, the devices or the apparatus composing these devices may be compromised by third-party producers. A famous example of such interference on classical system is the cryptographic devices sold by Crypto AG which were bugged by the Central Intelligence Agency [Mil20]. However, even considering an honest manufacturer, the quantum devices implementing QKD are hard to build and will always contain noises and losses [Dia+16; Xu+20]. Subsequently, QKD implementations inevitably mismatch with the theoretical models on which the security proofs are based. Moreover, imperfections, especially the ones occurring in single-photon detectors, have been successfully exploited to attack QKD protocols [Fun+07; Lyd+10; Ger+11; Wei+11]. For a review on quantum hacking, with attack examples, refer to [LCT14].

To overcome all of these implementation-related challenges, device-independent quantum key distribution (DIQKD) has been developed [Ací+07; VV14; Arn+18]. DIQKD is a family of more secure quantum key distribution protocols in which the assumption on the inner working of the quantum devices is dropped. Instead, DIQKD security proofs rely solely on the classical outcomes of measurements on a shared system, both of which are considered as *black-boxes*. Crucially, DIQKD protocols will simply abort in the presence of exploitable imperfections, which are always appearing in the collected outcomes.

From a maximal violation of the CHSH inequality the singlet state and specific measurements can be self-tested, and therefore, guaranteeing that two parties can have correlated outcomes, unknown to a third party. Intuitively, DIQKD can be built on top of self-tests; one could first assess the presence of the required resources from the CHSH score, and then compute a security proof on the distributed key. However, this self-tests-based approach leads to performance far from practical applications [FM18; KST22]. Hence, for better efficiency, the security proof of most protocols is directly computed from the CHSH score, or, for even better performance, directly from the observed correlations [Pir+09; Ho+20; Sek+21; WAP21; BFF21].

II – Self-testing for device-independent certification

4 - Self-testing two-qubit maximally entangled states

In this chapter we discuss the self-test of two-qubit maximally entangled states in a fully device-independent scope. Specifically, we here present an ideal self-testing protocol based on correlations leading to a maximal CHSH score, i.e. the certification is solely based on that CHSH score.

We consider the CHSH game in the quantum framework, where Alice and Bob receive copies of an unknown state $\rho_{AB} \in \mathcal{L}(\mathscr{H}^A \otimes \mathscr{H}^B)$ from an unknown source. Alice has access to the subsytem that lays in the Hilbert space $\mathscr{H}^A$ while Bob has access to the one in $\mathscr{H}^B$, both of unknown dimension. Each party has a measurement device with two inputs, $x, y = \{0, 1\}$, respectively corresponding to observables A_x acting on $\mathscr{H}^A$, for Alice, and B_y on $\mathscr{H}^B$, for Bob. These measurements only have two possible outcomes $(a, b) = \pm 1$. For each copies of the unknown share state, Alice and Bob randomly select a measurement and record that measurement outcome. This allows Alice and Bob to learn the statistics $p(ab|xy)$, from which can be computed the correlators $\langle A_x B_y \rangle = p(a = b|xy) - p(a \neq b|xy)$ and the CHSH score S following Eq. (2.7). We here focus on the ideal-case where the maximal CHSH score is obtained, $S = 2\sqrt{2}$ and from which we want to deduce the characteristics of the quantum realization $\{\rho_{AB}, A_x, B_y\}$.

Let us first show that A_x and B_y fully specify the quantum model of the measurements. As the measurements we consider have two outcomes $\{\pm 1\}$, the quantum model of each observable is a positive operator-valued measurement (POVM) with two elements $\{M^{+1}, M^{-1}\}$. We label $\{M_x^{+1}, M_x^{-1}\}$ the POVM of A_x and $\{M_y^{+1}, M_y^{-1}\}$ the one of B_y. Elements of these POVM satisfy

- Hermitianity, $(M^{\pm 1})^\dagger = M^{\pm 1}$,
- Positivity, $M^{\pm 1} \succeq 0$, that is $\langle\psi| M^{\pm 1} |\psi\rangle$ for all ψ,
- Completeness, $M^{+1} + M^{-1} = \mathbb{1}$.

Alice and Bob's observables can be directly constructed from their respective POVM following

$$\begin{aligned} A_x &= \sum_a a M_x^a = M_x^{+1} - M_x^{-1}, \\ B_y &= \sum_b b M_y^b = M_y^{+1} - M_y^{-1}. \end{aligned} \tag{4.1}$$

Using Eq. (4.1) and completeness, we can also show that each POVM element is

fully described by the operator they correspond to, following

$$\begin{aligned} M_A^{+1} &= \frac{1}{2}(\mathbb{1} + A_x), \qquad M_A^{-1} = \frac{1}{2}(\mathbb{1} - A_x) \\ M_B^{+1} &= \frac{1}{2}(\mathbb{1} + B_y), \qquad M_B^{-1} = \frac{1}{2}(\mathbb{1} - B_y). \end{aligned} \tag{4.2}$$

From the violation of the CHSH inequality, the first property of the quantum model we can deduce is that ρ_{AB} is entangled. Indeed, if the shared state is separable, then there exists weights $p_\lambda \geq 0$ and system states $\{\rho_A^\lambda\}$ and $\{\rho_B^\lambda\}$ such that

$$\rho_{AB}^{\mathsf{sep}} = \sum_\lambda p_\lambda \, \rho_A^\lambda \rho_B^\lambda. \tag{4.3}$$

Therefore, the statistics $p(ab|xy)$ can be obtained by a local strategy where Alice and Bob's measurement devices first prepare the state ρ_A^λ and ρ_B^λ, respectively, from the random variable λ, distributed according to p_λ, before measuring it according to M_x^a, M_b^y. Formally, that is

$$\begin{aligned} p(ab|xy) &= \mathrm{tr}\left[\left(M_x^a \otimes M_y^b\right) \rho_{AB}^{\mathsf{sep}}\right] \\ &= \sum_\lambda p_\lambda \ \mathrm{tr}\left[\left(M_x^a \otimes M_y^b\right)\left(\rho_A^\lambda \otimes \rho_B^\lambda\right)\right] \\ &= \sum_\lambda p_\lambda \ \mathrm{tr}\left[M_x^a \rho_A^\lambda\right] \mathrm{tr}\left[M_x^b \rho_B^\lambda\right] \\ &= \sum_\lambda p_\lambda \, p(a|x,\lambda) p(b|y,\lambda). \end{aligned} \tag{4.4}$$

From these statistics, a maximum CHSH score of $S = 2$ can be expected. Hence, a CHSH score $S > 2$ rules out the possibility that the measured state is separable.

Another aspect we can deduce from a CHSH score $S > 2$ is that the measurements are locally incompatible, i.e. $[A_0, A_1] \neq 0$ and $[B_0, B_1] \neq 0$. To demonstrate this, let us focus on Alice's observables. If her measurements commute, then there would exist a basis $\{|k\rangle\}$, with $|k\rangle \in \mathscr{H}_A$, where both operators are diagonal and in particular

$$A_x = \sum_k |k\rangle\langle k| \, A_x \, |k\rangle\langle k| \, . \tag{4.5}$$

Using this basis, we construct an entanglement breaking quantum channel Λ_A projecting the received state in Alice's local basis $\{k\}$ and discarding the measurement results. Formally, this channel acts on ρ_{AB} as follows

$$\begin{aligned} \Lambda_A[\rho_{AB}] &= \sum_k \left(|k\rangle\langle k|_A \otimes \mathbb{1}_B\right) \rho_{AB} \left(|k\rangle\langle k|_A \otimes \mathbb{1}_B\right) \\ &= \sum_k p_k \, |k\rangle\langle k|_A \otimes \rho_B^{(k)} \\ &= \tilde{\rho}_{AB} \end{aligned} \tag{4.6}$$

where p_k is the probability to project ρ_{AB} on $|k\rangle$. Let us now compute the correlators appearing in the CHSH score on the state $\tilde{\rho}_{AB}$

$$\begin{aligned}
\langle A_x B_y \rangle_{\tilde{\rho}_{AB}} &= \mathrm{tr}\left[\tilde{\rho}_{AB}(A_x \otimes B_y)\right] \\
&= \mathrm{tr}\left[\sum_k \left(|k\rangle\langle k|_A \otimes \mathbb{1}_B\right) \rho_{AB} \left(|k\rangle\langle k|_A \otimes \mathbb{1}_B\right) (A_x \otimes B_y)\right] \\
&= \mathrm{tr}\left[\rho_{AB} \sum_k \left(|k\rangle\langle k|_A \otimes \mathbb{1}_B\right) (A_x \otimes B_y) \left(|k\rangle\langle k|_A \otimes \mathbb{1}_B\right)\right] \\
&= \mathrm{tr}\left[\rho_{AB} \left(\sum_k |k\rangle\langle k| A_x |k\rangle\langle k|\right) \otimes B_y\right] \\
&= \mathrm{tr}\left[\rho_{AB} (A_x \otimes B_y)\right].
\end{aligned} \tag{4.7}$$

This shows the equivalence between correlations computed using locally compatible measurements and correlation computed using a separable state. Therefore, a violation of the CHSH inequality, only possible for entangled states, is a proof of locally anticommuting measurements.

If entanglement and locally incompatible measurement are solely deduced from a CHSH score $S > 2$, there is, however, more to deduce from a maximal CHSH score $S = 2\sqrt{2}$. More specifically, a maximal CHSH violation can only be achieved by a specific quantum model of a maximally entangled state and some locally maximally incompatible measurements, i.e. measurement with a zero joint measurability region [SW87; PR92; Tsi93]. Therefore, a maximal CHSH violation is a good criterion for a self-testing statement.

To formulate this statement, we first define the relevant Hilbert spaces. We start by introducing $\mathscr{H}_{AB} = \mathscr{H}_A \otimes \mathscr{H}_B$, the basis in which the shared state is diagonal

$$\rho_{AB} = \sum_i p_i |\psi_i\rangle\langle\psi_i| . \tag{4.8}$$

As the observed statistics only depends on the support of ρ_{AB}, i.e. the states $\{|\psi_i\rangle\}$ for which $p_i \neq 0$, we define the relevant space

$$\mathscr{H}_{AB}^{\star} = \mathrm{span}\left\{|\psi_i\rangle \mid p_i \neq 0\right\}. \tag{4.9}$$

Similarly, we construct the relevant space for each parties' subsytem as

$$\begin{aligned}
\mathscr{H}_A^{\star} &= \mathrm{span}\left\{|\psi_i\rangle_A \mid p_i \neq 0\right\} \\
\mathscr{H}_B^{\star} &= \mathrm{span}\left\{|\psi_i\rangle_B \mid p_i \neq 0\right\}.
\end{aligned} \tag{4.10}$$

Since the observables we consider have eigenvalues ± 1, we can deduce the useful relation

$$A_0^2 |\psi\rangle_A = A_1^2 |\psi\rangle_A = |\psi\rangle_A . \tag{4.11}$$

Then, we recall the expression of the CHSH operator

$$\mathcal{B}_{\text{CHSH}} = A_0 \otimes (B_0 + B_1) + A_1 \otimes (B_0 - B_1) \tag{4.12}$$

which is Hermitian by construction. From the sum-of-square decomposition of the CHSH operator $2\sqrt{2}\mathbb{1}_{AB} - \mathcal{B}_{\text{CHSH}}$ we can show that

$$A_0 A_1 \left|\psi\right\rangle_A = -A_1 A_0 \left|\psi\right\rangle_A \tag{4.13}$$

for all state $\left|\psi\right\rangle_A \in \mathscr{H}_A^\star$ [PNA10; ŠB20].

We label $\left|0_k\right\rangle \in \mathscr{H}_A^\star$ any eigenstates of A_0 satisfying $A_0 \left|0_k\right\rangle = \left|0_k\right\rangle$. We then introduce $\left|1_k\right\rangle = A_1 \left|0_k\right\rangle$. From Eq. (4.11) and Eq. (4.13), we can check that the basis $\{\left|0_k\right\rangle, \left|1_k\right\rangle\}$ is an orthonormal basis for which

$$\begin{aligned} A_0 \left|0_k\right\rangle &= \left|0_k\right\rangle \qquad & A_0 \left|1_k\right\rangle &= -\left|1_k\right\rangle \\ A_1 \left|0_k\right\rangle &= \left|1_k\right\rangle \qquad & A_1 \left|1_k\right\rangle &= \left|0_k\right\rangle . \end{aligned} \tag{4.14}$$

Therefore, on the two-dimensional subspace spanned by $\left|0_k\right\rangle, \left|1_k\right\rangle$, the operator A_0 and A_1 act as the Pauli operators σ_z and σ_x, respectively. Repeating this process for all k eigenvectors, we can write Alice's observables as a block-diagonal matrix with block of size 2×2

$$A_0 = \bigoplus_k \sigma_z^{(k)}, \qquad A_1 = \bigoplus_k \sigma_x^{(k)}. \tag{4.15}$$

Following the same steps for Bob, we find that his observables have the same block diagonal structure

$$B_0 = \bigoplus_l \frac{\sigma_z^{(l)} + \sigma_x^{(l)}}{\sqrt{2}}, \qquad B_1 = \bigoplus_l \frac{\sigma_z^{(l)} - \sigma_x^{(k)}}{\sqrt{2}}. \tag{4.16}$$

This suggests that $\mathscr{H}_A^\star$ can be written as a tensor space of a qubit subspace $\mathbb{C}_A^2$ with basis $\{\left|0\right\rangle, \left|1\right\rangle\}$ and a Hilbert space $\mathscr{H}_{k,A}$ of unknown dimension and carrying the label k. Formally, this allows us to write the decomposition

$$\begin{aligned} \left|0_k\right\rangle &= \left|0, k\right\rangle = \left|0\right\rangle \left|k\right\rangle \\ \left|1_k\right\rangle &= \left|1, k\right\rangle = \left|1\right\rangle \left|k\right\rangle , \end{aligned} \tag{4.17}$$

and, therefore

$$\begin{aligned} \sigma_z^{(k)} &= \left|0, k\right\rangle\!\left\langle 0, k\right| - \left|1, k\right\rangle\!\left\langle 1, k\right| = \sigma_z \otimes \left|k\right\rangle\!\left\langle k\right| \\ \sigma_x^{(k)} &= \left|0, k\right\rangle\!\left\langle 1, k\right| + \left|1, k\right\rangle\!\left\langle 0, k\right| = \sigma_x \otimes \left|k\right\rangle\!\left\langle k\right| \end{aligned} \tag{4.18}$$

where σ_z, σ_x act solely on $\mathbb{C}_A^2$. These expressions help us to decompose Alice's observables following

$$\begin{aligned} A_0 &= \bigoplus_k \sigma_z^{(k)} = \sum_k \sigma_z \otimes \left|k\right\rangle\!\left\langle k\right| = \sigma_z \otimes \sum_k \left|k\right\rangle\!\left\langle k\right| = \sigma_z \otimes \mathbb{1}_{A'} \\ A_1 &= \bigoplus_k \sigma_x^{(k)} = \sum_k \sigma_x \otimes \left|k\right\rangle\!\left\langle k\right| = \sigma_x \otimes \sum_k \left|k\right\rangle\!\left\langle k\right| = \sigma_x \otimes \mathbb{1}_{A'}. \end{aligned} \tag{4.19}$$

where $\mathbb{1}_{A'}$ is the identity matrix on $\mathscr{H}_{k,A}$. Following the same logic for Bob's observables we have

$$\begin{aligned} B_0 &= \frac{\sigma_z + \sigma_x}{\sqrt{2}} \otimes \mathbb{1}_{B'} \\ B_1 &= \frac{\sigma_z - \sigma_x}{\sqrt{2}} \otimes \mathbb{1}_{B'}. \end{aligned} \tag{4.20}$$

where the Pauli operators σ_z, σ_x act on the qubit space $\mathbb{C}^2_B$, and $\mathbb{1}_{B'}$ is the identity matrix acting on $\mathscr{H}_{l,B'}$.

From the derived form of both parties observables, we can write the CHSH operator as

$$\begin{aligned} \mathcal{B}_{\mathsf{CHSH}} &= \sqrt{2} \bigoplus_{k,l} \left(\sigma_z^{(k)} \otimes \sigma_z^{(l)} + \sigma_x^{(k)} \otimes \sigma_x^{(l)} \right) \\ &= \sqrt{2} \underbrace{\left(\sigma_z \otimes \sigma_z + \sigma_x \otimes \sigma_x \right)}_{\mathcal{B}^{\text{2-qubit}}_{\mathsf{CHSH}}} \otimes \mathbb{1}_{A',B'}. \end{aligned} \tag{4.21}$$

which only acts non-trivially, according to $\mathcal{B}^{\text{2-qubit}}_{\mathsf{CHSH}}$, on the two qubit space of Alice and Bob. The two-qubit operator $\mathcal{B}^{\text{2-qubit}}_{\mathsf{CHSH}}$ has two non-zero eigenvalues, 2 and -2, with corresponding eigenvectors $|\phi^+\rangle$ and $|\psi^-\rangle$ respectively. These eigenvectors are Bell states and their expression can be found in Eq. (1.2). This allows us to formulate the CHSH operator as

$$\mathcal{B}_{\mathsf{CHSH}} = 2\sqrt{2} \left(|\phi^+\rangle\langle\phi^+| - |\psi^-\rangle\langle\psi^-| \right) \otimes \mathbb{1}_{A',B'} \tag{4.22}$$

Therefore, for a CHSH score of $2\sqrt{2}$ we have

$$\begin{aligned} 2\sqrt{2} &= \operatorname{tr}\left[\mathcal{B}_{\mathsf{CHSH}} \rho_{AB}\right] \\ &= 2\sqrt{2} \operatorname{tr}_{\mathbb{C}^2_A, \mathbb{C}^2_B} \operatorname{tr}_{\mathscr{H}_{k,A}, \mathscr{H}_{l,B}} \left[\rho_{AB} \left(\left(|\phi^+\rangle\langle\phi^+| - |\psi^-\rangle\langle\psi^-| \right) \otimes \mathbb{1}_{A',B'} \right) \right] \\ &= 2\sqrt{2} \operatorname{tr}_{\mathbb{C}^2_A, \mathbb{C}^2_B} \left[\underbrace{\operatorname{tr}_{\mathscr{H}_{k,A}, \mathscr{H}_{l,B}} [\rho_{AB}]}_{\rho'_{AB}} \left(|\phi^+\rangle\langle\phi^+| - |\psi^-\rangle\langle\psi^-| \right) \right] \\ &= 2\sqrt{2} \operatorname{tr}_{\mathbb{C}^2_A, \mathbb{C}^2_B} \left[\rho'_{AB} \left(|\phi^+\rangle\langle\phi^+| - |\psi^-\rangle\langle\psi^-| \right) \right] \end{aligned} \tag{4.23}$$

which directly implies that

$$\rho'_{AB} = |\phi^+\rangle\langle\phi^+| . \tag{4.24}$$

Note that using the same demonstration, a score of $-2\sqrt{2}$ leads to $\rho'_{AB} = |\psi^-\rangle\langle\psi^-|$. Because the two-qubit state ρ'_{AB} is pure, the global state is the product state

$$\rho_{AB} = \rho'_{AB} \otimes \varrho_{\mathsf{junk}} \tag{4.25}$$

with $\varrho_{\mathsf{junk}} \in \mathscr{H}_{k,A} \otimes \mathscr{H}_{l,B}$.

From the CHSH score $S = 2\sqrt{2}$, we can hence conclude that there is a basis in which the shared state ρ_{AB} is of the form Eq. (4.25) and that the measurement are orthogonal Pauli measurements as in Eq. (4.19) and Eq. (4.20).

Since the observed correlations would be unchanged by considering another basis in which the state and measurements would be mapped to

$$\begin{aligned} \rho_{AB} &\to (U_A \otimes U_B)\, \rho_{AB}\, (U_A \otimes U_B)^\dagger \\ A_x &\to U_A A_x U_A^\dagger \\ B_y &\to U_B B_y U_B^\dagger, \end{aligned} \tag{4.26}$$

for some unitaries U_A, U_B, it is only relevant to consider self-testing up to local unitaries. Hence, we can formulate the following self-testing statement for the two-qubit maximally entangled state:

Theorem 1 *For any quantum realization $\{\rho_{AB}, A_x, B_y\}$ compatible with a CHSH score of $2\sqrt{2}$ there exists local isometries f_A, f_B such that a two-qubit maximally entangled state can be extracted following*

$$(f_A \otimes f_B)\,[\rho_{AB}] = \left|\phi^+\right\rangle\!\left\langle\phi^+\right| \otimes \varrho_{\mathit{junk}},$$

and such that measurements are orthogonal Pauli measurements on that state

$$\begin{aligned} f_A[A_0] &= \sigma_z \otimes \mathbb{1}_{A'} \\ f_A[A_1] &= \sigma_x \otimes \mathbb{1}_{A'} \\ f_B[B_0] &= \frac{\sigma_z + \sigma_x}{2} \otimes \mathbb{1}_{B'} \\ f_B[B_1] &= \frac{\sigma_z - \sigma_x}{2} \otimes \mathbb{1}_{B'}. \end{aligned}$$

5 - Robust self-testing of two-qubit maximally entangled states

In the previous chapter, we examined the self-test of two-qubit maximally entangled states from correlations achieving a maximal violation of the CHSH inequality. However, such correlations can hardly be observed experimentally. Indeed, imperfections such as noise and loss in creating, distributing and measuring the quantum state, will unavoidably lead to non-ideal correlations, i.e. not maximally violating the Bell inequality. Furthermore, since any self-testing experiment can only collect a limited sample of Bell game rounds, the correlations are only estimated up to a certain confidence interval. Acknowledging such limitations, there is the need for self-testing protocols robust to the presence of imperfections in the correlations, also known as *robust self-testing*.

There are multiple approaches to robust self-testing. Chronologically, the Mayers-Yao self-test was made robust in [Mag+06] while robust self-testing based on CHSH was introduced in [Bar+09]. A framework for the robust self-testing of the singlet was presented in [MYS12]. Since then, numerous improvement were made to improve the robustness of self-testing, and to extend it to different scenario, e.g. Bell scenarios with more inputs or outputs.

Here we present a numerical method, using Jordan's lemma, relevant for the robust self-test of the singlet. Two notable methods than will not be discussed here are the analytical method based on operator inequalities presented in [Kan16] and the numerical SWAP method [Ban+15]. We then expose some fundamental limitations on robust self-testing based on the CHSH inequality. Finally, we present a method that we developed, overcoming some of these limitations by extending robust self-testing of the singlet beyond the CHSH inequality.

5.1 . Extractability

In robust self-testing, the goal is to use the correlations observed in a Bell game to bound the *closeness* of the shared state, ρ_{AB} to the target state $|\psi_{AB}\rangle$ that we here consider pure. Similarly to ideal-case self-testing, Alice and Bob can craft local isometries, f_A and f_B, to identify the relevant degree of freedom from the shared state encoding the target state. Taking into account local isometries, a possible notion of *closeness* is the so-called *extractability* expressed as

$$\Xi[\rho_{AB} \to \psi_{AB}] = \sup_{\{f_A, f_B\}} F((f_A \otimes f_B)[\rho_{AB}], \psi_{AB} \otimes \varrho_{\text{junk}}) \tag{5.1}$$

where $F(\rho_0, \rho_1) = \left(\operatorname{tr}\left[\sqrt{\rho_0^{1/2}\rho_1\rho_0^{1/2}}\right]\right)^2$ is the square of the Uhlmann fidelity, which reduces to the squared overlap $F(\rho_0, \rho_1) = \operatorname{tr}[\rho_0\,\rho_1]$ if any of the two states

is pure. The separable state $\psi_{AB} \otimes \varrho_{\text{junk}}$ consists of $\psi_{AB} = |\psi_{AB}\rangle\langle\psi_{AB}|$, the target state, and ϱ_{junk} containing all remaining degrees of freedom which can be traced out. As an isometry mapping a state from one Hilbert space $\mathscr{H}_1$ to $\mathscr{H}_2 \otimes \mathscr{H}_2'$ can be thought of as a map from $\mathscr{H}_1$ to $\mathscr{H}_2$ by tracing out the ancillary space $\mathscr{H}_2'$, we can rewrite the extractability as

$$\Xi[\rho_{AB} \to \psi_{AB}] = \sup_{\{\Lambda_A, \Lambda_B\}} F((\Lambda_A \otimes \Lambda_B)[\rho_{AB}], \psi_{AB}). \tag{5.2}$$

where Λ_A, Λ_B are completely-positive trace-preserving (CPTP) maps. A detailed proof of the equivalence of these two extractability definitions in case the target state is pure can be found in [Sek+18].

Note that the extractability is lower bounded by $1/2$ as it is always possible for Alice and Bob to construct maps discarding the received state and preparing a new one with a fidelity of $1/2$ with respect to the target one. For example, if the target state is the singlet $|\psi^-\rangle$, we can build maps acting as

$$(\Lambda_A \otimes \Lambda_B)\left[\rho_{AB}\right] = |1\rangle\langle 1| \otimes |0\rangle\langle 0|\,. \tag{5.3}$$

Therefore, a non-trivial self-testing statement can be made if and only if $\Xi[\rho_{AB}] > 1/2$.

5.2 . Robustness of CHSH-based singlet self-tests

5.2.1 . Robust self-testing with two binary measurements

As a device-independent protocol, no assumption is made on the dimension of the shared quantum state and the measurements in self-testing. Interestingly, in the particular case of a Bell game where Alice and Bob own two dichotomic measurements – with two outcomes – we can use Jordan's lemma to define a basis where local observables are block diagonal. Indeed, Jordan's lemma states that for two Hermitian operators with eigenvalues ± 1 there exists a basis in which both operators are block-diagonal, with blocks of dimension 2×2. To simplify further calculations, we consider these blocks to be in the (σ_x, σ_z)-plane. This is done without loss of generality as Alice and Bob can always perform local rotations of their basis to recover that plane. Alice and Bob's observables can thus be written as a direct sum over these blocks

$$\begin{aligned} A_x &= \bigoplus_i A_x^i = \bigoplus_i \cos(\alpha_i)\sigma_h + (-1)^x \sin(\alpha_i)\sigma_m, \\ B_y &= \bigoplus_j B_y^j = \bigoplus_j \cos(\beta_j)\sigma_z + (-1)^y \sin(\beta_j)\sigma_x, \end{aligned} \tag{5.4}$$

with $\sigma_{m,h} = (\sigma_z \pm \sigma_x)/\sqrt{2}$ and for some measurement angles $\alpha_i, \beta_j \in [0, \pi/2]$ for each block, indexed by i and j. Trivially, the CHSH operator defined in Eq. (2.8)

inherits the same block structure and can be express following

$$\mathcal{B}_{\mathsf{CHSH}} = \bigoplus_{i,j} \mathcal{B}^{i,j}_{\mathsf{CHSH}} = \bigoplus_{i,j} A^i_0 \otimes (B^j_0 + B^j_1) + A^i_1 (B^j_0 - B^j_1). \tag{5.5}$$

The shared quantum state ρ_{AB} does not necessarily have a block diagonal structure. However, before measuring this state, Alice and Bob can always project it in their respective local basis to obtain the state

$$\tilde{\rho}_{AB} = \bigoplus_{i,j} p_{i,j} \rho^{i,j}_{AB} \tag{5.6}$$

where $p_{i,j}$ is the success probability to project ρ_{AB} in the (i,j)-block. Note that the state $\tilde{\rho}_{AB}$ achieves the same CHSH score as ρ_{AB} thanks to the block structure of the CHSH operator

$$S = \mathrm{tr}\left[\mathcal{B}_{\mathsf{CHSH}} \rho_{AB}\right] = \sum_{i,j} p_{i,j} \,\mathrm{tr}\left[\mathcal{B}^{i,j}_{\mathsf{CHSH}} \rho^{i,j}_{AB}\right]. \tag{5.7}$$

In the previous chapter, we have seen that in order to complete a self-testing statement we need to construct local maps $\Lambda = \Lambda_A \otimes \Lambda_B$. These local maps can be constructed using the same block diagonal recipe

$$\Lambda = \bigoplus_{i,j} \Lambda^i_A \otimes \Lambda^j_B \tag{5.8}$$

with the isometry in each block acting as

$$\Lambda^i_A : \mathcal{L}(\mathbb{C}^2) \to \mathcal{L}(\mathbb{C}^2), \qquad \Lambda^j_B : \mathcal{L}(\mathbb{C}^2) \to \mathcal{L}(\mathbb{C}^2). \tag{5.9}$$

From this block structure, the singlet extractability defined in (5.2) reads

$$\Xi[\rho_{AB} \to \psi^-] = \sup_{\{\Lambda^i_A, \Lambda^j_B\}} \sum_{i,j} p_{i,j} F((\Lambda^i_A \otimes \Lambda^j_B)[\rho^{ij}_{AB}], \psi^-). \tag{5.10}$$

Given that the probabilities $p_{i,j}$ are non-negative real numbers that sum up to 1, by definition, the singlet extractability is given by a convex sum of the singlet extractability on two-qubit blocks.

To obtain a CHSH-based robust self-test of the singlet, we need to lower bound the singlet extractability with respect to all quantum realisation achieving a given CHSH score S. In order to do so, we can first obtain a lower bound on this extractability over all two-qubit blocks. This can be done by first fixing the dependence of the maps on the block indexes (i,j), i.e. the expression of the maps would be a fixed function of the local measurement angle, $\Lambda^i_A = \Lambda_A(\alpha_i)$ for Alice and $\Lambda^j_B = \Lambda_B(\beta_j)$ for Bob. Note that the resulting isometries might not maximize the singlet extractability. Therefore, we will obtain a lower bound on Eq. (5.10) in

this way. The minimum singlet fidelity over all two-qubit states and measurement choices compatible with a score S is obtained by solving the optimisation

$$\begin{aligned} O_{\min}(S) = \min_{\alpha_i,\beta_j,\tau} \; & F(\Lambda_A^i \otimes \Lambda_B^j[\tau], \psi^-) \\ \text{s.t. } & \operatorname{tr}\left[\mathcal{B}_{CHSH}^{i,j}\,\tau\right] \geq S, \\ & \tau \geq 0, \\ & \operatorname{tr}[\tau] = 1, \\ & \tau^\dagger = \tau. \end{aligned} \tag{5.11}$$

The optimisation over all two-qubit states τ can be solved to arbitrary precision using semi-definite programming [SC23]. Therefore, a strategy to solve Eq. (5.11) is to minimize over the angles (α_i, β_j) the singlet-fidelity minimized over τ.

Using the convex structure of Eq. (5.10), the convex roof of $O_{\min}(S)$ over all CHSH scores, $f(S)$, gives a lower bound on the singlet-extractability with respect to the CHSH score [Sek+18]. Hence, from a CHSH score S, one can hope to extract a singlet fidelity of at most

$$\Xi[\rho_{AB} \to \psi^-] \geq \mathcal{F}(S) = \max\left(1/2, f(S)\right). \tag{5.12}$$

5.2.2 . Robustness bounds

To assess the performance of robust self-testing, we are interested in the evolution of the extractability with respect to the CHSH score. In particular, the minimum score for which a non-trivial fidelity to the target state can be extracted is called the *robustness bound*. This bound is crucial as any implementation of a self-testing protocol is required to have the capability to achieve a Bell violation at least as high as the robustness bound.

To glean the robustness bound with the method presented in the previous section, we first need to choose the local maps Λ_A^i and Λ_B^i appearing in Eq. (5.11). These maps are completely-positive trace-preserving maps acting on qubit space and parametrised by Alice and Bob measurement choice, respectively. A relevant pick for such maps has been reported in [Kan16]. For the block i, let Alice's map be a dephasing map of the form

$$\Lambda_A^i(\alpha_i)[\rho_{AB}] = \left(\frac{1+g(\alpha_i)}{2}\mathbb{1}\rho_{AB}\mathbb{1} + \frac{1-g(\alpha_i)}{2}\Gamma(\alpha_i)\rho_{AB}\,\Gamma(\alpha_i)\right), \tag{5.13}$$

with a dephasing strength

$$g(\alpha_i) = (1+\sqrt{2})(\cos\alpha_i + \sin\alpha_i - 1) \tag{5.14}$$

and a dephasing direction

$$\Gamma(\alpha_i) = \begin{cases} \sigma_h, & \text{if } \alpha_i \leq \frac{\pi}{4} \\ \sigma_m, & \text{otherwise.} \end{cases} \tag{5.15}$$

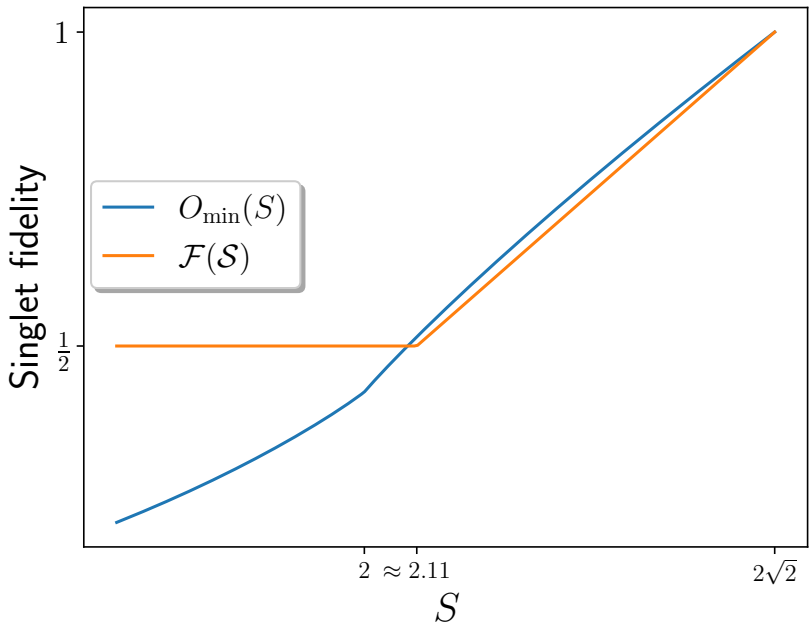


Figure 5.1: Lower bound on the singlet extractability with respect to the CHSH score S.

For the block j and the corresponding measurement angle β_j, Bob's map is of the same form, but with a dephasing direction given by

$$\Gamma(\beta_j) = \begin{cases} \sigma_h, & \text{if } \beta_j \leq \frac{\pi}{4} \\ \sigma_m, & \text{otherwise.} \end{cases} \tag{5.16}$$

We can now solve the optimisation Eq. (5.11) to get $O_{\min}(S)$ and, from the convex roof, obtain $\mathcal{F}(S)$, the lower bound on the singlet extractability as a function of the CHSH score. These functions are depicted in Fig. (5.1). A non-trivial fidelity is achieved for any CHSH violation greater than $S \approx 2.11$, the robustness bound.

It is worth noting that, using an analytical approach [Kan16], this bound has been found at $S = (16 + 14\sqrt{2})/17 \approx 2.11$, compatible with the numerical result we present here.

5.2.3 . Limits of CHSH-based singlet self-testing

While continuous efforts are made to improve the robustness bound of CHSH-based self-testing, another approach focuses on finding the *threshold CHSH score* below which no self-testing statement can be made. Surprisingly, it has been demonstrated [CKS19] that this threshold does not coincide with the local bound

$S = 2$. The demonstration is based on an example of a state achieving a CHSH score of $S = 2.0014$ while having a singlet extractability of $1/2$.

There is thus a threshold CHSH score higher than the local bound 2 and lower than 2.11, below which it is not possible to get a non-trivial self-testing statement. This raises numerous questions. First, as photonic implementations seems more desirable for technological applications of self-testing, most photonic loophole free Bell test realisation are based on polarization entangled photons for which detection efficiencies of $\approx 90\%$ are required to achieve a score higher that 2.11 [Viv+15]. Such detection efficiencies are beyond the realm of current possibilities. Therefore, if the threshold CHSH score is close to 2.11, self-testing the singlet will be hard to perform experimentally with photonic realisation. Secondly, if that threshold is close to the local bound, efforts are needed to craft better local maps than the ones proposed in Ref. [Kan16]. Thirdly, and more fundamentally, it raises the question of the type of resources needed for self-testing.

The CHSH threshold proves that under local operations (LO) only, singlet-extraction is not possible from any CHSH score. However, if Alice and Bob can share classical information (LOCC), a singlet state can always be extracted from the slightest CHSH violation [Bar+09]. Therefore, it would be interesting to explore if this threshold still occurs under other regimes such as local operations and share randomness (LOSR).

In an attempt to answer some of these question, in Article 1 [Val+20] we search for the quantum realisation achieving a maximum CHSH score while resulting in a trivial singlet extractability. Using Jordan's lemma, this problem corresponds to the optimisation

$$\begin{aligned} \sup_{\{\rho_{AB}, A_x, B_y\}} \quad & S = \sum_{i,j} p_{i,j} \operatorname{tr}\left(\mathcal{B}^{i,j}_{\mathsf{CHSH}} \rho^{i,j}_{AB}\right) \\ \text{s.t.} \quad & \Xi[\rho_{AB} \to \psi^-] \leq \frac{1}{2} \\ & \rho_{AB} = \bigoplus_{i,j} \rho^{i,j}_{AB} = \sum_{ij} |i\rangle\langle i| \otimes |j\rangle\langle j| \otimes \rho^{i,j}_{AB} \\ & A_x = \bigoplus_i A^i_x = \sum_i |i\rangle\langle i| \otimes A^i_x \\ & B_y = \bigoplus_j B^j_y = \sum_j |j\rangle\langle j| \otimes B^j_y \end{aligned} \tag{5.17}$$

This problem is hard to tackle as the number of two-qubit blocks (i, j) is unbounded. Furthermore, even when considering a relaxation of the problem to a fixed amount of two-qubit blocks, we would need to obtain a certified upper-bound on the singlet extractability. Since the extractability consists of a non-linear optimisation over CPTP maps, the certification of a tight upper-bound can not be guaranteed.

Therefore, as the proof can be constructive, we choose to limit ourselves to a subset of this problem. First, following the intuition behind [CKS19], we limit ourselves to the case of three two-qubit blocks per party, i.e. $i, j = \{1, 2, 3\}$. We consider observables with 2×2 blocks defined as

$$\begin{aligned} A_0^i &= \sigma_z, \quad A_1^i \in \{\sigma_z, \sigma_x, -\sigma_z\}_{i=1}^3 \\ B_0^j &= \sigma_h, \quad B_1^j \in \{\sigma_h, \sigma_m, -\sigma_h\}_{j=1}^3 \end{aligned} \tag{5.18}$$

where $\sigma_{h,m} = (\sigma_z \pm \sigma_x)/\sqrt{2}$. We focus on a family of state that are a mixture between the singlet state and separable states build from the structure of the Bell operator

$$\rho_{AB} = \nu \left(|2\rangle\langle 2| \otimes |2\rangle\langle 2| \otimes \rho_{AB}^{2,2} \right) + (1-\nu) \sum_{i,j \neq \{2,2\}} p_{i,j} \, |i\rangle\langle i| \otimes |j\rangle\langle j| \otimes \rho_{AB}^{i,j} \tag{5.19}$$

with

$$\begin{aligned} \rho_{AB}^{2,2} &= |\psi^-\rangle\langle\psi^-| \\ \rho_{AB}^{3,2} &= \frac{1}{4}(\mathbb{1} \otimes \mathbb{1} + \sigma_z \otimes \sigma_m) \\ \rho_{AB}^{3,3} &= \frac{1}{4}(\mathbb{1} - \sigma_z) \otimes (\mathbb{1} + \sigma_h) \\ \rho_{AB}^{1,1} = \rho_{AB}^{1,3} = \rho_{AB}^{3,1} &= \frac{1}{4}(\mathbb{1} + \sigma_z) \otimes (\mathbb{1} + \sigma_h), \end{aligned} \tag{5.20}$$

and with $p_{i,j} = 0$ for all other values of i, j. Conveniently, this family of states yield a CHSH score of $S = 2 + (2\sqrt{2} - 2)\nu$.

A relaxation of all separable two-qubit maps on these specific states, which we detailed in our article, allows us to obtain an upper bound on the singlet extractability given as a non-linear maximisation of only five real parameters. To obtain a CHSH threshold, we minimized this upper-bound over the weights of the states of the family we consider, for a gradually increasing CHSH score, i.e. for a higher ν. This approach gave us a state with a parameter $\nu = 0.061$, hence achieving a CHSH violation of ≈ 2.05, below which no singlet can be extracted. Our result pushed the CHSH threshold by an order of magnitude. Importantly, this shows the limitation of CHSH-based self-testing as the *CHSH threshold* lays in the $[2.05, 2.11]$ range.

5.3 . Robust singlet self-testing beyond CHSH

In an attempt to make robust self-testing more accessible to experimental implementations, there is the need for protocols more resistant to noises and losses. In the previous section, we saw that robust CHSH-based self-testing has been only proven for a CHSH score higher than $S \approx 2.11$ and can not be made for score below 2.05. These relatively high CHSH scores are hardly in reach experimentally, and,

as such, a very few self-testing experiments have been reported so far [Tan+17; Ban+21].

It is in this scope that in Article 2 we propose a new protocol for robust self-testing. Our approach is based on a more refined analysis of the correlations which are needed to compute the CHSH score, i.e. our protocol does not require any additional data. Instead of using a single Bell inequality, our protocol relies on a family of *generalized CHSH inequalities*

$$S_\theta = \sqrt{2}(\cos(\theta)\underbrace{\langle A_0(B_0+B_1)\rangle}_{X} + \sin(\theta)\underbrace{\langle A_1(B_0-B_1)\rangle)}_{Y} \tag{5.21}$$

parametrised by an angle $\theta \in [0, \pi/2]$, for which we derived robust self-testing statements.

As our approach applies to a Bell game with two dichotomic measurements, we prove self-testing statements from Jordan's lemma, following the steps explained in the previous section. Analogously to the CHSH-case, we obtained the robustness bound by minimizing the singlet fidelity over all state and measurement choices, for fixed maps. We crafted maps with a dependency in both the local measurement choice and θ. More specifically, these maps are inspired by the one presented in Eq. (5.13), with a couple of tweaks, notably a dephasing strength depending on θ, and for one party, an additional rotation along σ_y as well as a dephasing direction depending both on the angle of measurement and θ.

We then provide a robust self-testing statement recipe for any given correlator pair (X, Y). From a list of parameters θ and their corresponding robustness bound S_θ^{bound} that we provide, one can hope to obtain a singlet-extractability of

$$\max_\theta \mathcal{F}(S_\theta) = \max_\theta \left[\begin{cases} \frac{1}{2}, & \text{if} S_\theta \leq S_\theta^{\text{bound}}, \\ \frac{1}{2}\left(1 + \frac{S_\theta - S_\theta^{\text{bound}}}{2\sqrt{2} - S_\theta^{\text{bound}}}\right), & \text{otherwise} \end{cases} \right]. \tag{5.22}$$

Note that the argument θ maximizing this optimisation directly gives the best Bell inequality of the family Eq. (5.21) to self-test the considered correlator pair (X, Y). The maximum singlet-extractability over all θ, as a function of correlators pair (X, Y) is depicted in Fig. (5.2).

Comparing to CHSH-based self-testing, our protocol achieves higher singlet-extractability for any correlator $X \neq Y$. Furthermore, our protocol can be used to perform self-tests for correlation leading to CHSH scores below the robustness bound of $S \approx 2.11$, below which no self-testing statement has been proven, and even below the currently known CHSH threshold of 2.05, provided enough imbalance between the correlators, e.g. $X \gg Y$. Therefore, this protocol makes self-testing implementations more accessible, especially in a case of imbalanced correlators.

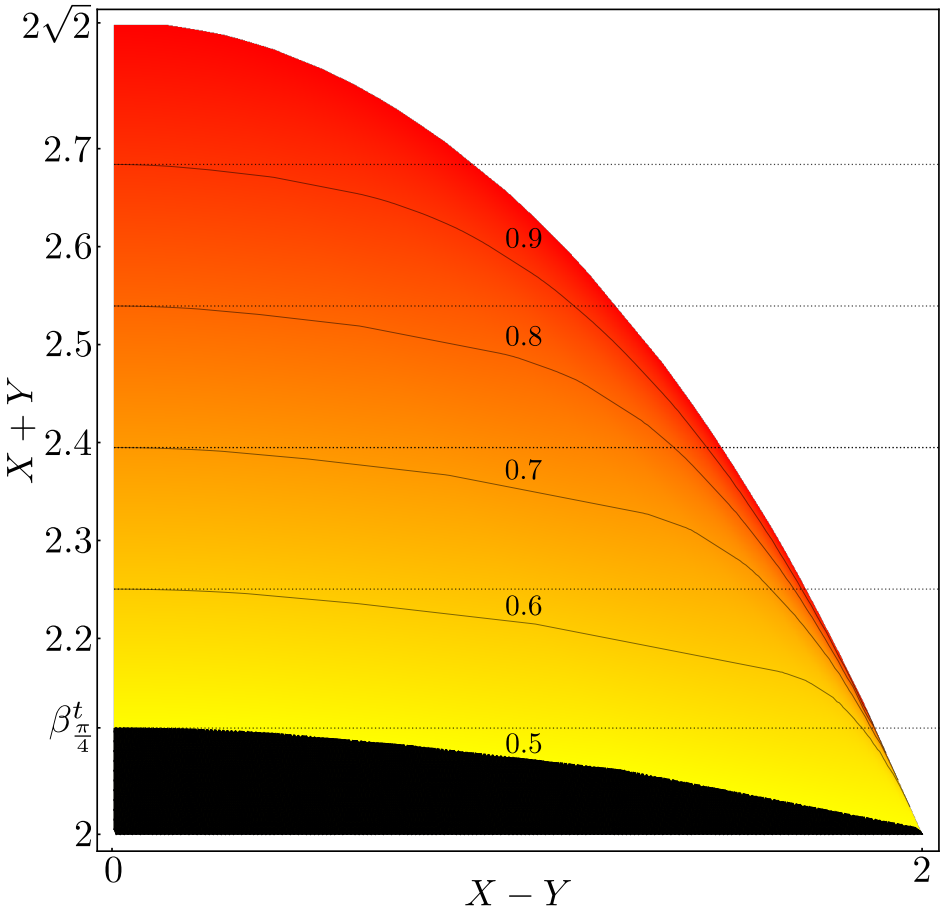


Figure 5.2: Solution to Eq. (5.22) for all pairs of correlators (X, Y). The dashed lines represent different singlet-extractabilities using CHSH, while the solid line shows the singlet-extractability achieved using the most fitting generalized CHSH inequality. Correlators in the black zone can not be used to make self-testing statement with our method.

Article 1

What is the minimum CHSH score certifying that a state resembles the singlet?

Xavier Valcarce[1], Pavel Sekatski[1], Davide Orsucci[1], Enky Oudot[1,2], Jean-Daniel Bancal[1,2], and Nicolas Sangouard[1]

[1] Departement Physik, Universität Basel, Klingelbergstraße 82, 4056 Basel, Schweiz
[2] Département de Physique Appliquée, Université de Genève, 1211 Genève, Suisse

Quantum, volume 4, page 246
arXiv preprint: 1910.04606

Abstract

A quantum state can be characterized from the violation of a Bell inequality. The well-known CHSH inequality for example can be used to quantify the fidelity (up to local isometries) of the measured state with respect to the singlet state. In this work, we look for the minimum CHSH violation leading to a non-trivial fidelity. In particular, we provide a new analytical approach to explore this problem in a device-independent framework, where the fidelity bound holds without assumption about the internal working of devices used in the CHSH test. We give an example which pushes the minimum CHSH threshold from ≈ 2.0014 to ≈ 2.05, far from the local bound. This is in sharp contrast with the device-dependent (two-qubit) case, where entanglement is one-to-one related to a non-trivial singlet fidelity. We discuss this result in a broad context including device-dependent/independent state characterizations with various classical resources.

Article 2

Self-testing two-qubit maximally entangled states from generalized Clauser-Horne-Shimony-Holt tests

Xavier Valcarce[1, 2], Julian Zivy[1, 2], Nicolas Sangouard[1, 2], and Pavel Sekatski[2]

[1] Université Paris-Saclay, CEA, CNRS, Institut de Physique Théorique, 91191 Gif-sur-Yvette, France

[2] Departement Physik, Universität Basel, Klingelbergstraße 82, 4056 Basel, Schweiz

Phys. Rev. Research 4, 013049
arXiv preprint: 2011.03047

Abstract

Device-independent certification, also known as self-testing, aims at guaranteeing the proper functioning of untrusted and uncharacterized devices. For example, the quality of an unknown source expected to produce two-qubit maximally entangled states can be evaluated in a bi-partite scenario, each party using two binary measurements. The most robust approach consists in deducing the fidelity of produced states with respect to a two-qubit maximally entangled state from the violation of the CHSH inequality. In this paper, we show how the self-testing of two-qubit maximally entangled states is improved by a refined analysis of measurement statistics. The use of suitably chosen Bell tests, depending on the observed correlations, allows one to conclude higher fidelities than ones previously known. In particular, nontrivial self-testing statements can be obtained from correlations that cannot be exploited by a CHSH-based self-testing strategy. Our results not only provide novel insight into the set of quantum correlations suited for self-testing, but also facilitate the experimental implementations of device-independent certifications.

III – Device-independent quantum key distribution

6 - Device-independent key distribution protocols

Alice and Bob wants to share a cryptographic key, unknown to an eavesdropper, Eve, which has access to unlimited physical and computational resources. Both parties are each in a closed lab such that no information is leaked, and each have access to a trusted source of randomness. These labs are interconnected by a quantum channel as well as by an authenticated classical channel. The classical channel is public, all the information transmitted over it is openly disclosed, however authentication prevents Eve from tampering with the transiting information.

In her lab, Alice has two measurements $\hat{A}_x$, with $x \in \{0, 1\}$. In his lab, Bob has three measurements $\hat{B}_y$, with $y \in \{0, 1, 2\}$. The outcomes of the measurements $\hat{A}_0, \hat{A}_1, \hat{B}_0$ and $\hat{B}_1$ are used to guarantee the secrecy of the generated key. The extra measurement $\hat{B}_2$ is chosen so that it correlates with $\hat{A}_0$ as much as possible. Notice that, in general, the outcomes are not binary.

In the following, we make no assumption on the quantum channel and the measurements, i.e. Eve is considered to have full control over the quantum channel and can have bugged the measurement devices beforehand. A setup to perform DIQKD is depicted in Fig. (6.1).

With this setup, a typical DIQKD protocol has the following steps

1. Measurements: For each round, a source generates and distributes a shared quantum state $|\psi_{ABE}\rangle \in \mathscr{H}_a \otimes \mathscr{H}_B \otimes \mathscr{H}_E$ to Alice and Bob over the quantum channel. Alice randomly picks an input $x \in \{0, 1\}$ and preform the corresponding measurement $\hat{A}_x$. Bob decides if the round is a *test round*, used to test the quantum devices, or a *generation round*, used to create the key. He then measures with either $\hat{B}_0$ or $\hat{B}_1$, chosen randomly, in case of a test round, or with $\hat{B}_2$ for a generation round. Alice records the obtained outcomes in a string $\mathbf{A}$. Similarly, Bob fills a string $\mathbf{B}$ from his outcomes.

2. Sifting: Alice and Bob share the string of their input choices, $\mathbf{X}$ and $\mathbf{Y}$, respectively. To indicate the type of rounds chosen, Bob will also send to Alice a binary string $\mathbf{T}$ with bits set to 0 for test rounds and 1 for generation rounds. Alice and Bob may erase the outcomes of some generation rounds. This is particularly relevant for basis choice leading to poorly correlated outcomes. Here, this is all generation rounds in which Alice measured $\hat{A}_1$.

3. Error correction: Alice communicates publicly a syndrome of her outcomes string. This allows Bob to either reconstruct a string $\mathbf{A}' = \mathbf{A}$ or abort the protocol.

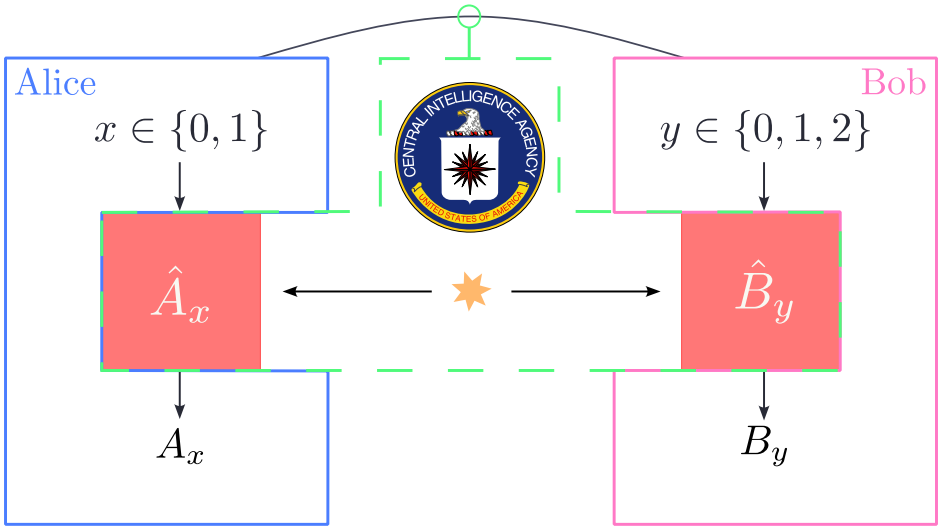


Figure 6.1: DIQKD Setup. Alice's lab (delimited by the blue line) and Bob's lab (delimited by the pink line) are linked by an authenticated classical channel of communication (gray craved line), and by a quantum channel (green dashed rectangle). A source (yellow star) generates a bipartite state with one part send to Alice while the other is sent to Bob. Alice selects an input x, to perform the measurement $\hat{A}_x$ and obtain the outcome A_x. Similarly, Bob chooses an input y, to measure his received state with respect to $\hat{B}_y$ and obtain B_y. Eve, represented by the CIA logo, has full access on the quantum channel, the classical channel, and may have compromised the measurement devices.

4. Parameter estimation: From $\mathbf{A}', \mathbf{B}, \mathbf{X}$ and $\mathbf{Y}$ Bob can compute the correlations $p(ab|xy)$. If these correlations fail to satisfy some requirements, e.g. a given CHSH score, the protocol abort.

5. Privacy amplification: Alice and Bob run a privacy amplification process on $\mathbf{A}$ and $\mathbf{A}'$, to yield the final key.

Some extra steps can be included to further enhance the performance of DIQKD protocols. Notably, following insights on QKD, Alice can add noise by shifting the outcomes of $\hat{A}_0$ with a probability fixed before the protocol starts [Ho+20]. The protocol can also be slightly modified by including an extra measurement for Bob, B_3, that is randomly chosen instead of B_2 during key generation rounds [Sch+21]. Recently, a protocol for which the key is generated using a randomly post-selected subset of the key generation round has been proposed [Xu+22]. For a general review on the different DIQKD protocols, see [Pri+23].

7 - Entropy bounds

7.1 . Key rate

To benchmark the performance of DIQKD protocols we need to compute the *key rate*, labelled r, corresponding to the amount of key bit that can be extracted per round. We here solely focus on asymptotic key rates, which are key rates derived in the limit of an infinite number of rounds. If asymptotic key rates are fundamentally inaccessible, they are a handy tool to assess the quality of a DIQKD protocol. In particular, avoiding finite size effects greatly simplifies the computation of key rates. However, by not including these finite size effects, the asymptotic regime yield key rates higher that the ones obtained for a finite number of rounds. These finite size effects are beyond the scope of this thesis, more details can be found in [Tan21; Tan+22; Pri+23].

Extracted key bits must be secret, i.e. provably unknown to Eve, and correct, i.e. identical for Alice and Bob. Therefore, the computation of a key rate must take into account all attacks that can be implemented by Eve, and specific error-correction protocol. In the following, we discuss key rates that were first derived with the assumption that quantum devices are independent and identically distributed (IID) over the rounds of the protocols, i.e. that the devices are memoryless, measurements $\hat{A}_x, \hat{B}_y$ are the same through the protocol and the distributed state for n-round is of the form $|\psi\rangle_{ABE}^{\otimes n}$. This assumption limits Eve's range of attacks to what is known as collective attacks. However, using the *entropy accumulation theorem* [DF19; DFR20], it has been shown that the key rates we present here, up to some finite corrections, hold under general attacks, known as coherent attacks, allowing to drop the need for the IID assumption [ARV19]. Note that in the asymptotic regime, there exists a choice of protocol parameters that renders the cost of these the finite corrections negligible.

Intuitively, the key rate is given by the mutual information between the outcomes of the generation rounds, A_0 and B_2, used to generate the key (correctness) and is limited by the amount of information Eve has on A_0 (secrecy). In the asymptotic limit, where one-way error correction from Alice to Bob is used and where the correlations $p(ab|xy)$ can be computed exactly, the key rate is lower-bounded by the Devetak-Winter bound [DW05]

$$r \geq r_{\mathrm{DW}} = I(A_0 : B_2) - \chi(A_0 : E) \tag{7.1}$$

where I is the mutual information, χ corresponds to the Holevo bound and E denotes the quantum-side information Eve stored during the protocol. Note that the key rate can be expressed using conditional von Neumann entropies $H(\blacksquare|\blacksquare)$

following

$$\begin{aligned} r_{\mathrm{DW}} &= I(A_0 : B_2) - \chi(A_0 : E) \\ &= H(A_0) - H(A_0|B_2) - (H(A_0) - H(A_0|E)) \\ &= H(A_0|E) - H(A_0|B_2). \end{aligned} \tag{7.2}$$

The remaining challenge is to bound these two terms, and in particular to upper-bound the Holevo quantity directly from the correlations $p(ab|xy)$, as no assumption can be made on Eve's system and the quantum devices. In the following two sections we will describe two methods to tackle this bound, the first one utilize the CHSH score, while the second one is based on a more refined analysis of the correlations.

7.2 . CHSH-based security

7.2.1 . Key rate from the CHSH score

In [Pir+09], the first upper-bound on the Devetak-Winter bound has been derived. This approach makes use of an additional symmetrisation step in the protocol presented in the previous chapter. The symmetrisation step allows Alice and Bob to obtain uniform marginals, which result in $H(A_x) = H(B_y) = 1$. In order to do so, Alice and Bob can simply XOR their key bits with a public random string that is shared over the classical channel.

Let's consider uniform noise, i.e. noise affecting symmetrically the outcomes of Alice and Bob's measurements. Such type of noise naturally occurs when a state goes through a depolarizing channel or through a phase-covariant cloner. In that case, the mutual information between Alice and Bob's raw key simply reads

$$I(A_0 : B_2) = H(A_0) - H(A_0|B_2) = 1 - h(Q) \tag{7.3}$$

where $Q = p(a = b|xy) - p(a \neq b|xy)$ is the quantum bit error rate (Qber) and h is the binary entropy $h(x) = -x \log_2(x) - (1-x)log_2(1-x)$.

From the parameter estimation step of the protocol presented above, Bob can compute the CHSH score $S = \langle \hat{A}_0 \hat{B}_0 \rangle + \langle \hat{A}_0 \hat{B}_1 \rangle + \langle \hat{A}_1 \hat{B}_0 \rangle - \langle \hat{A}_1 \hat{B}_1 \rangle$. From this score and using Jordan's lemma, an upper-bound on the Holevo quantity appearing in Eq. (7.1) is derived

$$\chi(A_0 : E) \leq h\left(\frac{1 + \sqrt{(S/2)^2 - 1}}{2}\right). \tag{7.4}$$

Finally, from these two results, a lower bound on the DIQKD key rate is given by

$$r \geq r_{\mathrm{P}} = 1 - h\left(\frac{1 + \sqrt{(S/2)^2 - 1}}{2}\right) - h(Q). \tag{7.5}$$

7.2.2 . Fine-grained error-correction

When presenting the protocol in the previous chapter, we assumed that Alice and Bob have binary measurements with outcomes ± 1. A more general approach would allow both parties to have measurements with more outcomes, that could ultimately be binned to form the raw key. Non-binary outcomes naturally occur in the presence of loss, as loss might lead to no measurement outcomes, which can be accounted as an extra outcome. Interestingly, Bob can use the extra information of the non-binned or *fine* outcomes of B_2 to reduce the cost of error-correction [ML12]. This *fine-grained error correction* is given by

$$\begin{aligned} I(A_0 : B_2) &= 1 - H(A_0|B_2) \\ &= 1 - H(A_0, B_2) - H(B_2) \\ &= 1 - \sum_b \left(\sum_{a=\pm 1} -p(ab|02) \log_2(p(ab|02)) \right) \\ &\quad - p(b|02) \log_2(p(b|02)). \end{aligned} \tag{7.6}$$

Note that, in the presence of uniform noise, this error-correction trivially reduces to $1 - h(Q)$ in case Bob has only two outcomes.

Therefore, a tighter lower-bound on the key rate is

$$r \geq r_{\mathrm{ML}} = 1 - h\left(\frac{1 + \sqrt{(S/2)^2 - 1}}{2} \right) - H(A_0|B_2). \tag{7.7}$$

7.2.3 . Noisy Preprocessing

Following insights from device-dependent QKD [RGK05; KGR05; RS07], it can be advantageous for Alice to include a *noisy-preprocessing* step following the measurement step of the DIQKD protocol we consider here [Ho+20]. This noise acts as a bit-flip operation on the binned outcome of $\hat{A}_0$, used for key generation, occurring with a probability q, fixed by Alice. Formally, this is the transformation

$$p(a|0y) \to (1 - q)\, p(a|0y) + q\, p(-a|0y). \tag{7.8}$$

We denote A_0' the raw key bit of Alice after noisy pre-processing.

For a CHSH score S and a noisy preprocessing probability q, the Holevo quantity is upper bounded by

$$\begin{aligned} \chi(A_0' : E) \leq I_q(S) = & h\left(\frac{1 + \sqrt{(S/2)^2 - 1}}{2} \right) \\ & - h\left(\frac{1 + \sqrt{1 - q(q-1)(8 - S^2)}}{2} \right), \end{aligned} \tag{7.9}$$

which is equivalent to Eq. (7.4) when $q = 0$, and smaller otherwise.

Combined with the fine-grained error-correction term Eq. (7.6), we obtain the following lower bound on the key rate

$$r \geq r_{\mathrm{Ho}} = 1 - I_p(S) - H(A_0'|B_2). \tag{7.10}$$

7.2.4 . Robustness of CHSH-based security

To grasp the requirements for experimental implementations of DIQKD, we need to study the behaviour of the key rate for some specific quantum model and losses.

Intuitively, it is worth exploring the behaviour of the key rate when the source sends a singlet state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, as this state saturate the CHSH inequality and thus should yield a key rate of 1 in the absence of losses.

We consider measurements to be as general as possible on the $(\sigma_x - \sigma_z)$-plane. This is, measurements characterized by the POVMs associated with outcomes $\{+1, -1\}$

$$\begin{aligned} \hat{A}_x &: \{M(\alpha_x),\, \mathbb{1} - M(\alpha_x)\} \\ \hat{B}_y &: \{M(\beta_y),\, \mathbb{1} - M(\beta_y)\} \end{aligned} \tag{7.11}$$

with $M(\theta) = \frac{1}{2}\left(\mathbb{1} + \cos(\theta)\sigma_z + \sin(\theta)\sigma_x\right)$ and the angles $\alpha_x, \beta_y \in [0, \pi/2]$. To verify our intuition in the absence of loss, without noisy preprocessing $q = 0$, and with the optimal angles $(\alpha_0, \alpha_1) = (0, \pi/2)$ and $(\beta_0, \beta_1, \beta_2) = (\pi/4, -\pi/4, 0)$, we indeed obtain a key rate of

$$r \geq 1 - h\left(\frac{1 + \sqrt{(S/2)^2 - 1}}{2}\right) - h(Q) = 1 - h(1) - h(0) = 1. \tag{7.12}$$

In the presence of loss, we need to address the possibility of the shared state being lost before the measurement, which would result in the absence of outcome. We label $\eta \in [0, 1]$ the efficiency of the quantum devices, i.e. the shared state is lost with probability $1 - \eta$. If the state is lost, Alice and Bob can recover binary outcomes by binning the no-outcome event as $+1$. Thus, their POVMs becomes

$$\{M^{+1},\, M^{-1}\} \to \{\eta M^{+1} + (1-\eta)\mathbb{1},\, \mathbb{1} - \big(\eta M^{+1} + (1-\eta)\mathbb{1}\big)\}. \tag{7.13}$$

However, for his measurement B_2, Bob can simply consider all three outcomes, with the corresponding POVM

$$B_2 : \{\eta M(\beta_2),\, \eta(\mathbb{1} - M(\beta_2)),\, (1-\eta)\mathbb{1}\}, \tag{7.14}$$

since exploiting fine-grained outcomes can reduce the cost of error-correction as explained in Sec. 7.2.2.

To study the robustness of CHSH-based key rates, we optimise the different key rates Eq. (7.5), Eq. (7.7) and Eq. (7.10), over all measurement angles α_x, β_y on the singlet state, for a decreasing efficiency η. When considering noisy preprocessing, we also optimise the key rate over the parameter q of Eq. (7.10). These key rates are shown in figure Fig. (7.1a). Most interestingly, using noisy preprocessing and fine-grained error-correction, we obtain a critical efficiency of $\eta \approx 0.903$, below which no key can be extracted.

For a more general approach, we study the robustness of the CHSH-based key rates for all partially entangled pure two-qubit states of the form

$$|\psi\rangle_\theta = \frac{1}{2}\left(\cos(\theta)\,|00\rangle + \sin(\theta)\,|11\rangle\right) \tag{7.15}$$

with $\theta \in [0, \pi]$. This is done by adding the parameter θ as an optimisation parameter when optimising for the key rate. The results are given in Fig. (7.1b). As expected from [Ebe93], the key rate is more tolerant to loss for these states, and the critical detection efficiency drop to $\eta \approx 0.826$.

7.3 . DIQKD security proof beyond CHSH

In the previous section, we presented how provably secure key bits can be extracted from the CHSH score. If improvement on the key rate has been made by including fine-grained error-correction and noisy preprocessing, the security proof is still fundamentally limited by the CHSH score. To improve the resistance to losses, a natural approach is to derive a security statement from a more refined analysis of the observed statistics $\{p(ab|xy)\}$. Conveniently, since the CHSH score is computed from these correlations, no extra step or assumption on the DIQKD protocol are required.

7.3.1 . Security statement from the generalized-CHSH score

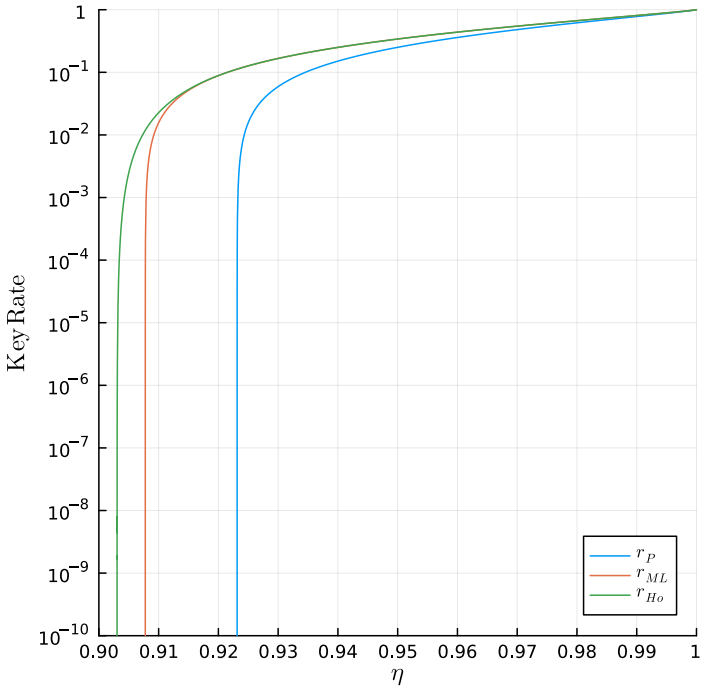
The generalized CHSH score $S_\theta = \sqrt{2}(\cos(\theta)X + \sin(\theta)Y)$, obtained from the generalized CHSH operator $\mathcal{B}_\theta$, allows to leverage the knowledge of the correlator pair

$$\begin{aligned} X &= \langle A_0 \otimes (B_0 + B_1)\rangle, \\ Y &= \langle A_1 \otimes (B_0 - B_1)\rangle. \end{aligned} \tag{7.16}$$

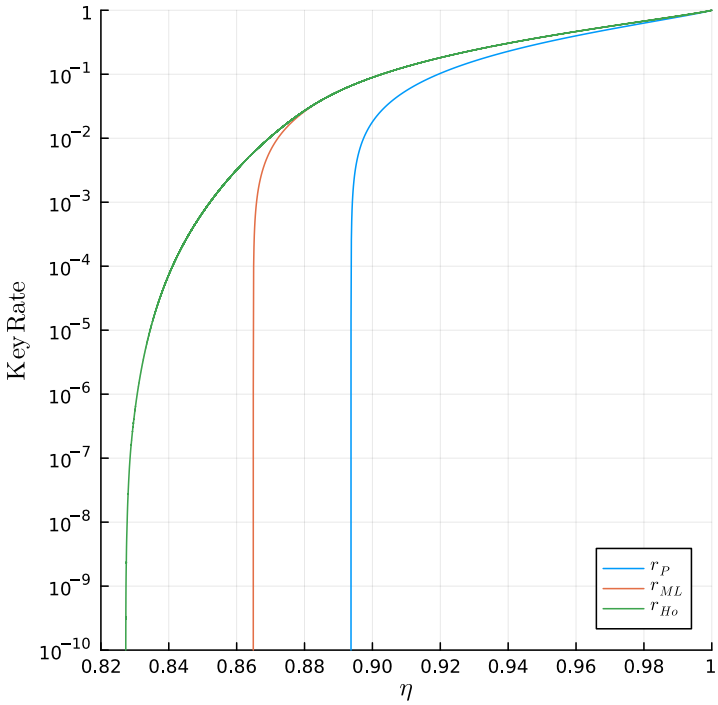
We have seen in the previous part that generalized CHSH inequalities, compared to CHSH, can be advantageous for a device-independent protocol that is self-testing [Val+22]. Intuitively, these inequalities can be useful for DIQKD as well. The intuition comes from the correlator pair (X, Y) allowing to differentiate between the contributions of measurements $\hat{A}_0$, used for key generation, and $\hat{A}_1$ solely used to test the quantum devices. Therefore, this extra degree of freedom could allow us to bound Eve's entropy on the outcome A_0 more tightly.

In Article 3, we investigate this intuition, paving the way for DIQKD security proofs beyond the CHSH score. We here provide a sketch of the proof, for more detail please refer to [Sek+21] or, alternatively, to [WAP21].

The critical part of the security analysis consists in bounding Eve's information on the key directly from the correlator pair X, Y. This requires to analyze the entropy $H(A_0'|E)$ of Eve on the key A_0' obtained after a noisy preprocessing with



(a) Two-qubit maximally entangled state



(b) Two-qubit partially entangled state

Figure 7.1: Evolution of different key rates with efficiency η. r_P is given by Eq. (7.5), r_{ML} by Eq. (7.7) and r_{Ho} by Eq. (7.10). The key rates are optimised over Alice and Bob measurement angles, and for insert b) over the parameter θ of Eq. (7.15).

probability q, in a more refined way compared to the CHSH case. This entropy can be expressed as

$$H(A_0'|E) = H(A_0') - \underbrace{\left(H(\rho_E) - \sum_{a'=\pm 1} p(a') H(\rho_{E|a'}) \right)}_{I_{\theta,q}(X,Y)} \tag{7.17}$$

where ρ_E is the reduced state of Eve, and where $\rho_{E|a'}$ is Eve's state conditioned on the key bit $A_0' = a'$, occurring with probability $p(a')$. Using the symmetrisation step explained in Sec 7.2.1, we have $H(A_0') = 1$. We show in [Sek+21] that, using Jordan's lemma, the quantity $I_{\theta,q}(X,Y)$ reduced on two-qubit states, $I'_{\theta,q}(X,Y)$, can be obtained by solving the maximization problem

$$\begin{aligned} I'_{\theta,q}(X,Y) = \max_{L,\alpha_0,\alpha_1,\beta_0,\beta_1} & H(\mathbf{L}) + H(\rho_{E|a'=+1}(L,\alpha_0,q)) \\ \text{s.t.} \quad & \mathcal{B}_\theta(\mathbf{L},\alpha_0^i,\alpha_1^i,\beta_0^j,\beta_1^j) \geq S_\theta, \end{aligned} \tag{7.18}$$

where $\rho_{E|a'=+1}(\mathbf{L},\alpha_0,q)$ is a two-qubit states shared between Alice and Eve, with a fixed dependency in $\alpha_0, \mathbf{L}$ and q, and where $\mathcal{B}_\theta(\mathbf{L},\alpha_0,\alpha_1,\beta_0,\beta_1)$ is the generalized CHSH operator parametrized by θ and Alice and Bob's measurement angles $(\alpha_0,\alpha_1,\beta_0,\beta_1)$ applied on states of the form

$$|\psi\rangle_{AB} = \sum_k \sqrt{L_k}\, |\phi_k\rangle\,, \tag{7.19}$$

with $|\phi_k\rangle = \{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$, characterized by $\mathbf{L} = (L_1, L_2, L_3, L_4)$. In [Sek+21] we further explain how to solve this optimisation, and how to obtain an upper bound $\tilde{I}_{\theta,q}(X,Y) \geq I'_{\theta,q}(X,Y)$ concave in S_θ.

In Article 3, we solve the minimization for all $\theta \in [0, \pi/2]$. This gave us the bound on the conditional entropy $1 - \min_\theta \tilde{I}_{\theta,q}(X,Y) \leq H(A_0|E)$ and, hence, the lower bound on the key rate

$$r \geq r_{\text{Sek}} = 1 - \min_\theta \tilde{I}_{\theta,q}(X,Y) - H(A_0'|B_2). \tag{7.20}$$

Interestingly, this approach achieves higher key rate than CHSH-based key rates, except when correlators satisfy $X(X+Y) = 4$, in which case the obtained key rates are equal. When considering optimal noisy preprocessing, the gap in improved key rate diminishes but is still non-negligible. Applied to the concrete case of a singlet state as explained in 7.2.4, the critical detection efficiency drops from ≈ 0.903 to ≈ 0.900 when using generalized CHSH security proof. However, for partially entangled two-qubit states, there is no improvement in critical detection efficiency. Note that, independently to our results, [WAP21] reported on similar results. In particular, a DIQKD security proof has also been derived from the generalized CHSH score and the reported advantages in key rate and critical efficiencies are identical to the ones found using our method.

7.3.2 . Security statement from all correlations

In [BFF21] a device-independent lower bound on the von Neumann entropy has been derived based on all the correlations $\{p(ab|xy)\}$. This approach introduces a sequence of optimisation problems which ultimately converges to the conditional von Neumann entropy, for states which lay in tensor product Hilbert spaces. Each optimisation problem can be solved using a NPA hierarchy [NPA07; PNA10], producing a certified bound from semi-definite programming, and tightly converging with the order of the hierarchy. As this method is more general than the scope of this thesis, we here briefly introduce the optimisation problem and the result of this method when applied to DIQKD key rate.

Consider a state $\rho_{ABE} \in \mathscr{H}_{\mathcal{A}} \otimes \mathscr{H}_{\mathcal{A}} \otimes \mathscr{H}_{\mathcal{E}}$ shared between Alice, Bob and Eve. The shared state reduced on Alice and Eve subsystems is given by $\rho_{AE} = \mathrm{tr}_B[\rho_{ABE}]$. We label $\{M_a^0\}$ the POVM corresponding to the outcomes $\{a\}$ for Alice's measurement $\hat{A}_0$. For some $m \in \mathbb{N}$, lemma 3.1 of [BFF21] states that Eve's entropy on Alice's raw key is lower bounded by

$$\begin{aligned} c_m + \sum_{i=1}^{m-1} \frac{w_i}{t_i \ln(2)} \sum_a \inf_{Z_a \in \mathcal{L}(\mathscr{H}_E)} \mathrm{tr}\Big[\rho_{AE} \\ \big(M_a^0 \otimes (Z_a + Z_a^* + (1-t_i) Z_a Z_a^* + t_i (\mathbb{1}_A \otimes Z_a Z_a^*)\big)\Big] \\ \text{s.t.} \quad ||Z_a|| \leq \nu_i = \frac{3}{2} \max\left\{\frac{1}{t_i}, \frac{1}{1-t_i}\right\} \end{aligned} \tag{7.21}$$

where $c_m = \frac{-1}{m^2 \ln(2)} + \sum_{i=1}^{m} \frac{w_i}{t_i \ln(2)}$ and where w_i and t_i are the nodes and weights of the m-order Gauss-Radau quadrature in the range $[0, 1]$. Eq. (7.21) converges to $H(A_0|E)$ when m converges to infinity.

To obtain a device-independent lower bound on the conditional von Neumann entropy, we can constraint Eq. (7.21) to all quantum models compatible with the observed correlations. In particular, we define r constraints as inequalities of linear combinations of the observed correlations

$$\sum_{abxy} c^i_{abxy} p(ab|xy) \geq \gamma_i \quad \forall i \in \{1, ..., r\}. \tag{7.22}$$

Adding these constraints and relaxing Eq. (7.21) by commuting the sum and the infinimum as well as by replacing the tensor product structure of the space of ρ_{AE} by introducing commutation relations on the relevant variables, one obtains the

problem

$$
\begin{aligned}
c_m + \inf \sum_{i=1}^{m-1} \frac{w_i}{t_i \ln(2)} \sum_a \langle\psi| M_a^0 (Z_{a,i} + Z_{a,i}^* + (1-t_i) Z_{a,i} Z_{a,i}^* + t_i (\mathbb{1}_A \otimes Z_{a,i} Z_{a,i}^*) |\psi\rangle \\
\text{s.t.} \quad \sum_{abxy} c_{abxy}^i \langle\psi| M_a^x N_b^y |\psi\rangle \geq \gamma_i \qquad & \forall i \in \{1 \ldots, r\} \\
\sum_a M_a^x = \sum_b N_b^y = \mathbb{1} \qquad & \forall x, y \\
M_a^x \geq 0 \qquad & \forall a, x \\
N_b^y \geq 0 \qquad & \forall b, y \\
Z_{a,i} Z_{a,i}^* \leq \nu_i \qquad & \forall a,\ i \in \{1, \ldots, m-1\} \\
Z_{a,i}^* Z_{a,i} \leq \nu_i \qquad & \forall a,\ i \in \{1, \ldots, m-1\} \\
[M_a^x, N_b^y] = [M_a^x, Z_{b,i}] = [N_b^y, Z_{a,i}] = 0 \qquad & \forall a, b, x, y, i
\end{aligned}
\tag{7.23}
$$

where the minimum is taken over all collections $(|\psi\rangle, \{M_a^x\}, \{N_B^y\}, \{Z_{a,i}\})$. Using the NPA hierarchy, this problem can be relaxed into a converging sequence of semi-definite program, which can be solved exactly.

This method, when applied to correlations compatible with a two-qubit partially entangled state shared between Alice and Bob, gives the most advantageous key rate. We find that the critical detection efficiency, in particular, drops to ≈ 0.805, considering a $(m = 8)$-order Gauss-Radau quadrature. This critical detection efficiency for two-qubit partially entangled states is close to the optimal one, as it has been proven that no key rate can be obtained from efficiency below ≈ 0.7904[Łuk+22].

Note, however, that this method requires heavy computational resources. It is, henceforth, not convenient for a quick benchmark of a DIQKD implementation proposal. In this scope, solving Eq. (7.23) more efficiently is desired, this could be achieved by choosing better monomial sets or by exploiting symmetries to reduce the size of the SDPs [RMB21].

8 - Implementing device-independent quantum key distribution

8.1 . Platform comparison

DIQKD protocols relies on entanglement to generate a provably secure key. Before practical considerations such as distance between parties or noise resistance, the key rate of protocol, asserting the amount of secure key bit that can be extracted per experiment rounds, is arguably the first reference benchmark to compare DIQKD implementations. As the key rates presented in Sec. 7.3.1 and Sec. 7.3.2 are recent and were not easily exploitable at the time of preparing this thesis, we here focus on key rates based on the CHSH score to compare DIQKD implementations.

In order to implement DIQKD, a first requirement is to be able to entrust all assumptions made on the protocol. Specifically, the no-leakage assumption needs particular attention. In a Bell test, no information about the input of a party should influence the outcome of the other party's measurement. This locality loophole is often closed by using a space-like separation between Alice and Bob's measurement events, see e.g. [Hen+15; Giu+15; Sha+15]. When it comes to DIQKD, this is however more complex as we need to ensure that there is no information leakage to Eve. Indeed, any information about the inputs or outputs of the parties would open up a new range of attacks beyond coherent attacks. Therefore, DIQKD experiment proposals have to address this assumption by suggesting a relevant way to isolate Alice and Bob's lab.

CHSH based key rates increase with the CHSH score. Subsequently, proposed DIQKD experiments should be based on a platform known to be able to generate highly entangled states leading to a high CHSH score in a detection loophole-free manner.

A critical factor in implementing DIQKD is the ability for the experiment to operate at a high repetition rate. Indeed, as the product of the repetition rate with the key rate gives the key rate per unit of time, a high repetition rate is necessary for practical applications. Furthermore, as key rates drop with losses, a high repetition rate enables mildly lossy implementations by maintaining their practicality.

In the rest of this section, we will examine two common platforms for implementing DIQKD: one utilizing heralded entanglement and the other based on purely photonic circuits. We will provide a brief overview of the advantages and disadvantages of each approach.

8.1.1 . Heralded entanglement

The objective of heralded entanglement experiments is to generate a strong entanglement between two quantum systems, held by Alice and Bob. Such quantum systems can be of different nature, and notably include NV-centers, single atoms in cavities and trapped ions. A particularity of these systems is that they are capable of emitting photons that are entangled with the inner state of the system. Therefore, by sending these photons to a central station that performs Bell-state measurements, Alice and Bob can entangle their quantum systems through a process known as *entanglement swapping*.

Combining the capability of creating highly entangled state with high detection efficiencies, high CHSH score can be achieved with heralding experiments. Such experiments have thus been successfully used to perform loophole-free Bell experiments [Hen+15; Ros+17]. Importantly for DIQKD, heralded entanglement systems are scalable by nature as the transmission loss is managed thanks to the heralding process.

On the downside, heralded entanglement realizations run at a low repetition rate. This is mainly due to resetting the system between measurements. Furthermore, this approach requires heavy machineries which can not easily be embedded or minimized to work in data centers or on satellites as desired for industrial DIQKD applications. As such, while heralded entanglement systems are a great tool for proof-of-concept experiments, they may not be the ideal candidate for long-term applications.

A first DIQKD experiment, making use of trapped ions, has been reported in [Nad+22]. This was made possible from the strong entanglement between two ions separated by $2\mathrm{m}$, yielding a high CHSH score of $S \approx 2.677$ and having a low quantum bit error rate of $Q \approx 0.0144$ This experiment generated a key of $95\,884$ bits out of $1\,500\,000$ repetitions, achieving a key rate of $r \approx 0.0639$. This was obtained with an effective repetition rate of $\approx 60Hz$ over 7.9h. Around the same time, another DIQKD experiment using neutral atoms separated by a distance two orders of magnitude larger demonstrated parameters compatible with a positive key rate in the limit of large repetition [Zha+22]. However, no key could be generated, illustrating the challenge of extending DIQKD at large distances.

8.1.2 . Photonic setups

The thoroughly studied photonic setups can produce photons which are entangled in various degree-of-freedom, with polarization-entangled photons being the most commonly used approach. Leveraging the entanglement production capabilities of these setups, experimental loophole-free Bell tests have been successfully conducted [Giu+15; Sha+15; Li+18].

Photonic setups offer numerous advantages over the heralded entanglement approach. Firstly, they provide a high repetition rate which can be orders of magnitude higher than what has been achieved with trapped ions. Additionally, on

a more long term aspect, the photonic platform has a promising potential for commercial applications, mainly thanks to integrated photonic circuits which enable the implementation of complex circuits that can be embedded on a chip. In fact, photonic device-dependent QKD realization has been performed with system embedded on satellite [Lia+17], and rack unit for data centers are already commercially available [PS18].

For the implementation of DIQKD protocols, photonic setups have two main limitations. First, photonic sources used in most Bell test demonstrations produce states which are far from ideal two-qubit states, resulting in a low CHSH score. For example, photon entangled in polarization, generated by a SPDC source can only achieve a CHSH score of $S \approx 2.35$ [Viv+15]. Furthermore, photonic implementations are highly susceptible to losses, mainly from distribution in optical fibers and from non-unit efficiency of single-photon detectors. This leads to low CHSH scores, e.g. the highest score that has been reported in a loophole-free Bell test using a SPDC source is of $S \approx 2.02$ [Liu+21], as well as a challenging scalability with respect to longer transmission distances. In particular, the low Bell violation seriously reduces the expected key rate, even in the presence of a high repetition rate. However, these limitations can be mitigated. Recent theoretical advances in DIQKD protocols coupled with more efficient quantum optical devices can lead to possible photonic DIQKD realizations. Furthermore, heralded qubit amplifiers could help transmit photons over long distances without breaking entanglement [GPS10].

Photonic setups are hence a natural candidate for DIQKD experiments and more long-term applications [Zap+23]. Encouragingly, a first proof-of-concept realization of DIQKD with photons entangled in polarization has been reported, where parameters compatible with a positive key rate in the limit of large repetition were remonstrated [Liu+22]. Several improvements are still required to obtain a first photonic DIQKD produced key following this proposal, including the implementation of random basis switching and a proof of security valid against the most general type of attacks in case where random postselection is applied.

More efforts are therefore needed in order to see a photonic DIQKD realization. Complementary to protocol improvements we detailed in Chap. 7, it is also worth exploring new photonic experiment designs. In the next section, we present a common approach to photonic DIQKD, based on photons entangled in polarization. The key rate obtained with this setup is used as a benchmark to newly suggested experimental designs. Then, in the last section of this chapter, we show how photonic experiments can be designed in an automated manner, as we proposed in Article 4. Applied to DIQKD, this led to new setups which are promising candidates for photonic DIQKD implementations.

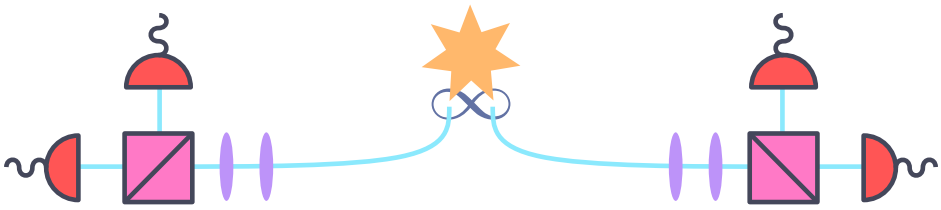


Figure 8.1: SPDC setup. A SPDC source (yellow star) sends photons entangled in polarization (blue lines), with one part send to Alice and one send to Bob. Locally, each party disposes of wave plates (purple ellipses) used to choose the measurement basis according to the measurement setting. This is followed by a polarising beamsplitter (pink sliced square) with each of the two outputs measured by NPNR detectors.

8.2 . DIQKD with polarization-entangled photons

A standard approach to implement DIQKD with photons is to use polarization entangled photons generated by a spontaneous down-conversion source (SPDC) and measured in different polarization basis thanks to wave plates, polarization beam-splitters and single-photon detectors. This typical setup, here referred as the *SPDC setup*, is depicted in Fig. (8.1). This approach is the one chosen in the results reported in [Liu+22] and is often used to benchmark theoretical key rate improvements [Ho+20; Sek+21].

Let us briefly describes the statistics obtained from this implementation. An SPDC source is implemented with a non-linear crystal used to emit photons in coupled modes, with mode a sent to Alice and mode b sent to Bob. Note that here we only consider a single mode per party, whereas, in practice, multiple modes can be created. We denote $a, a_\perp$ the two orthogonal polarizations of Alice's mode, and, similarly $b, b_\perp$ for Bob. The state emitted is given by

$$|\psi\rangle = \sqrt{1-T_g}\sqrt{1-T_{g'}}\exp\left(T_g a^\dagger a_\perp^\dagger - T_{g'} b^\dagger b_\perp^\dagger\right)|00\rangle \tag{8.1}$$

with $T_g = \tanh(g)$ and $T_{g'} = \tanh(g')$, and where g and g' are the squeezing parameters given by the non-linear susceptibility of the crystal and by the power of the pump [Viv+15].

For each measurement input, Alice rotates her measurement basis with the help of wave plates. Formally, for angles (α_x, ϕ_x) corresponding to the input choice x, the two orthogonal polarizations change following

$$\begin{aligned} a &= \cos(\alpha_x)\tilde{a} + e^{i\phi_x}\sin(\alpha_x)\tilde{a}_\perp, \\ a_\perp &= e^{-i\phi_x}\sin(\alpha_x)\tilde{a} - \cos(\alpha_x)\tilde{a}_\perp. \end{aligned} \tag{8.2}$$

where $(\tilde{a}, \tilde{a}_\perp)$ form a new polarization basis. Similarly, Bob obtains a new polarization basis $(\tilde{b}, \tilde{b}_\perp)$ from angles (β_y, φ_y) for input y.

Finally, each polarizing beam-splitter outputs two modes, one for each polarization basis, that are measured using single-photon detectors. For Alice, the detectors will measure the modes $\tilde{a}, \tilde{a}_\perp$, respectively, while for Bob they will resolve $\tilde{b}$ for one and $\tilde{b}_\perp$ for the other. Such detectors are non photon-number resolving (NPNR) detectors with outcomes $+1$, or *click*, when a photonic signal is detected and -1, or *no-click*, otherwise. These detectors have an efficiency η, i.e. in the presence of photons the outcome should be $+1$ with probability η. Formally, an η-efficient NPNR detector on a mode $\tilde{a}$, is characterized by the POVM $\{M^{\tilde{a}}_{-1}, \mathbb{1} - M^{\tilde{a}}_{-1}\}$ where

$$M^{\tilde{a}}_{-1} = (1-\eta)^{\tilde{a}^\dagger \tilde{a}}. \tag{8.3}$$

To obtain binary outcomes, Alice and Bob have to bin their four potential outcomes $\{p_H, p_V\} = \{\pm 1, \pm 1\}$. For an outcome pair $\{p_H, p_V\}$, the binning choice

$$p = \begin{cases} +1, & \text{if } \{p_H, p_V\} = \{+1, -1\} \\ -1, & \text{otherwise} \end{cases} \tag{8.4}$$

has been shown to be optimal [Viv+15].

Combining the expression of the state, the measurement basis choices and the detection operators, one can compute the statistics $p(ab|xy)$ as a function of the squeezing parameters, Alice and Bob's measurements angles and detector efficiencies. The full derivation of these statistics can be found in [Viv+15] and [Ho+20].

The statistics computed from the SPDC setup allow to study its application for DIQKD. This is achieved by optimising the key rate over the squeezing parameters and measurement angles. With this method, we compute the critical detection efficiency by repeating the optimisation for progressively smaller efficiency η until no positive key rate is obtained.

Using the key rate Eq. (7.10), with fine-grained error correction and noisy preprocessing, the mono-mode SPDC setup have a key rate of $r \approx 0.2552$ for the ideal case $\eta = 1$. When allowing for more modes, the key rate goes up to ≈ 0.295. This setup also requires a detection efficiency of at least $\eta \approx 0.826$ to yield a positive key rate. This critical efficiency is achieved for single-mode SPDC sources, as the multimode regime only produces CHSH score that are advantageous for efficiency higher that 0.9 [Viv+15]. The evolution of the key rate with the detection efficiency, in the mono-mode regime, is shown in Fig. (8.2).

8.3 . Automatic design of photonic experiments

If photonic setups are a promising platform for quantum information processing and, in particular for DIQKD, finding a suitable photonic experiment design is

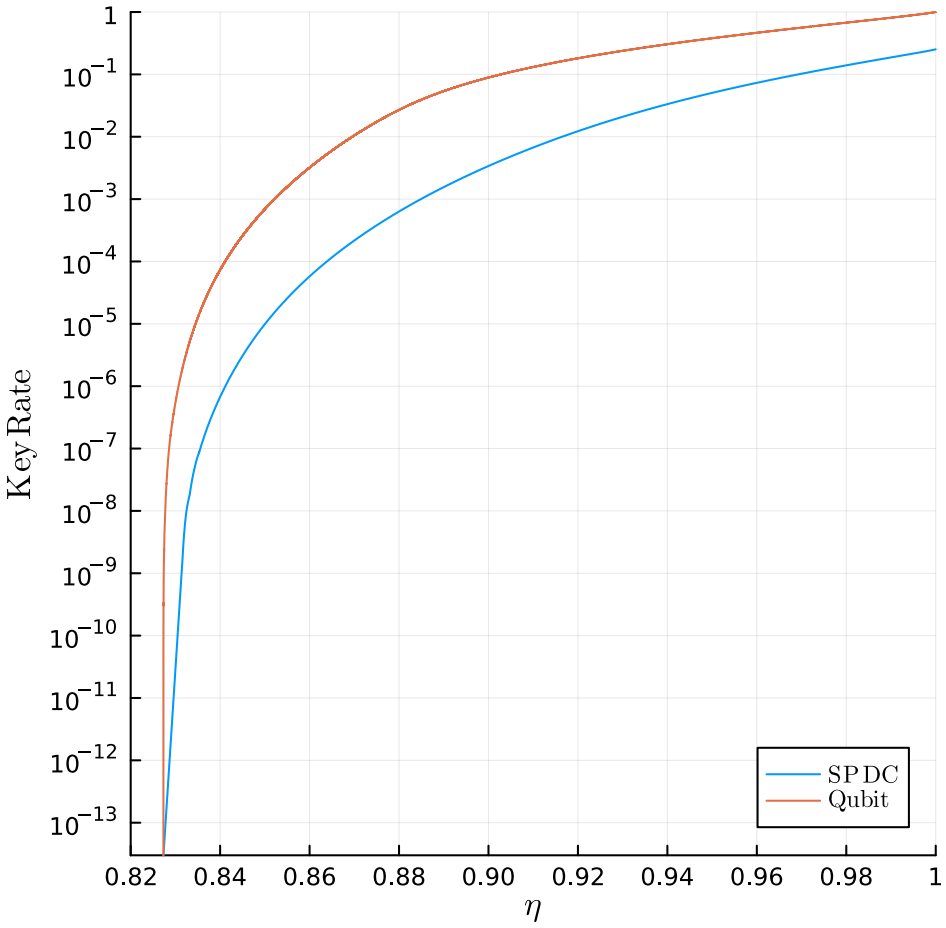


Figure 8.2: Key rate with respect to the detection efficiency. The blue line correspond to the key rate obtained from a mono-mode SPDC setup when all source and measurement parameters are optimized. The orange curve gives the key rate obtained for two-qubit partially entangled state, as a reference.

cumbersome. Indeed, thanks to integrated photonic [Pel+21] there is the possibility to implement complex circuits, combining numerous optical devices. Therefore, a systematic search through all possible implementations seems unrealistic. Furthermore, for each photonic setup, carrying the computation of the measurement statistics by hand is a time-consuming task while using numerical analysis based on available Fock-representation framework quickly turn resource heavy when precise computation and more optical modes are considered. Finally, with a constant evolution of DIQKD protocols, new implementations need to be proposed continuously.

To circumvent these issues, in Article 4 [Val+23], we propose an approach using machine learning and an efficient custom-made photonic simulation framework

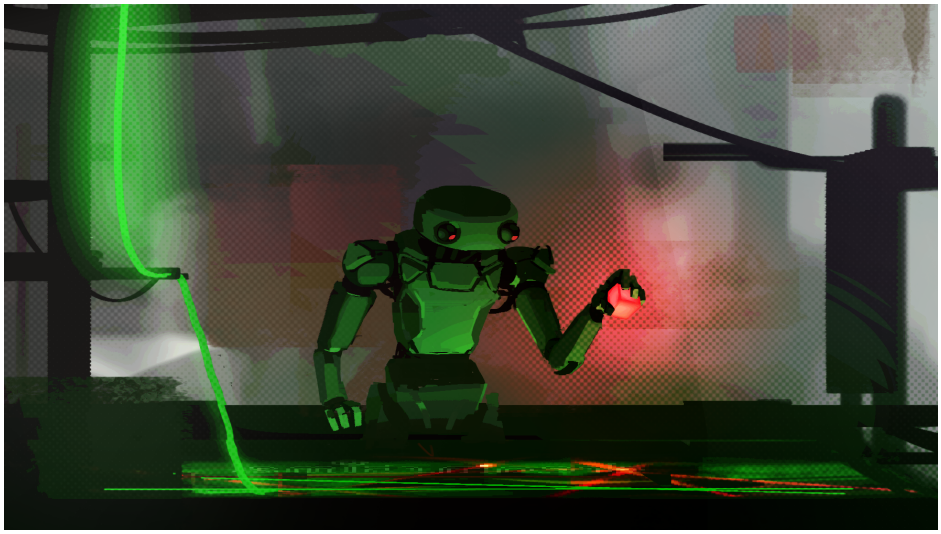


Figure 8.3: Artist's impression of the automated design of photonic experiments. © Dowinson Nguyen.

which, together, can propose photonic design matching a given figure of merit, e.g. a DIQKD key rate. In the next two subsections, we give an overview of this method. Then, we show how our method performs for the design of DIQKD experiments as well as for another figure of merit.

8.3.1 . Simulating quantum optical circuits

Photonic circuits can be seen as quantum circuits where each mode i is a bosonic mode characterized by the bosonic operators $a_i, a_i^\dagger$, and where gates are transformations of these modes. We restrict ourselves to optical transformations that are commonly available in quantum optics laboratory : single- and two-modes squeezers, displacements, phase-shifters and beam-splitters. To measure these bosonic modes, we focus on non photon-number resolving (NPNR) detectors sometimes called single-photon detectors, which have outcome $+1$ or *click*, when a signal is detected and -1, or *no-click*, otherwise. In addition to these operations, we also include heralding operations, conditioning the state of the circuit to the presence of a signal in the heralded mode.

In order to efficiently explore these photonic setups, there is the need for a fast and accurate simulation framework. We address this need with an approach based on the Gaussian representation of states and operations. This representation has the advantage of allowing for an exact and memory-efficient representation of circuits. Concretely, we develop a numerical framework using this representation to efficiently evaluate any given photonic circuit.

Gaussian Quantum optics Consider a n-mode bosonic system. Each mode i can be described in terms of quadrature operators; the position $x_i = (a_i^\dagger + a_i)/2$ and the momentum $p_i = i(a_i^\dagger - a_i)/2$ operators. The entire circuit is thus characterized by the vector $\mathbf{q} = (q_1, \ldots, q_{2n}) = (x_1, p_1, \ldots, x_n, p_n)$.

Gaussian states, such as the vacuum state, are fully characterized by a displacement vector μ and a covariance matrix Σ. Elements of these two object are functions of $\mathbf{q}$. More precisely, they are given by

$$\mu = (\mu_1, \ldots, \mu_{2n}), \qquad \text{with} \quad \mu_i = \langle q_i \rangle = \mathrm{tr}\left[\rho q_i\right] \tag{8.5}$$

$$\Sigma = \begin{pmatrix} \Sigma_{11} & \ldots & \Sigma_{1,2n} \\ \vdots & \ddots & \vdots \\ \Sigma 2n, 1 & \ldots & \Sigma_{2n,2n} \end{pmatrix}, \qquad \text{with} \quad \Sigma_{i,j} = \frac{\langle q_i q_j + q_j q_i \rangle}{2} - \mu_i \mu_j. \tag{8.6}$$

This representation is compact as it only needs $2n(n+1)$ real parameters to fully characterized a n-mode bosonic system.

Gaussian transformations are transformations which conserve the Gaussian properties of Gaussian states. These include

- single-mode and two-modes squeezers,
- displacements,
- beam-splitters,
- phase shifters.

Such transformation are represented by a vector $\mathbf{d}$ of size $2n$ and by a symplectic matrix M of size $2n \times 2n$. Applied on a Gaussian state (μ, Σ), such transformations output

$$(\mu, \sigma) \;\mapsto\; (M\mu + d,\; M\Sigma M^T). \tag{8.7}$$

The no-click probability $p_{\circ,i}$ of a NPNR detector on mode i with efficiency η, is computed from the displacement vector and covariance matrix of a Gaussian state following

$$p_{\circ i} = \frac{2}{2-\eta} \sqrt{\frac{(\det \Sigma)^{-1}}{\det(\Sigma^{-1} + F)}} e^{-\frac{1}{2}\mu^T \left(\Sigma^{-1} - \Sigma^{-1}(\Sigma^{-1}+F)^{-1}\Sigma^{-1}\right)\mu} \tag{8.8}$$

where

$$F = \begin{pmatrix} \frac{4\eta}{2-\eta} & 0 \\ 0 & \frac{4\eta}{2-\eta} \end{pmatrix}_{2i-1,2i} \oplus 0_{2n-2}. \tag{8.9}$$

Trivially, the click probability in mode i is given by $p_{\bullet,i} = 1 - p_{\circ,i}$.

Heralded operations are non-Gaussian operations. However, the state $\rho_{\bullet,i}$resulting of an n-mode Gaussian state conditioned on a click in a mode i, can be expressed,

up to a renormalization factor, as the difference of two $(n-1)$-modes Gaussian state

$$\rho_{\bullet,i} = \frac{\rho_{\neg,i} - p_{\circ,i}\rho_{\circ,i}}{1 - p_{\circ,i}} \tag{8.10}$$

where $\rho_{\neg,i}$ is the Gaussian state with the mode i traced out and where $\rho_{\circ,i}$ is the Gaussian state after a no-click event. Therefore, we can represent an n-mode photonic circuits undergoing $n-m$ heralding operations with $2^{n-m}(2m^2+3m+1)$ real parameters.

More details on the exact expression of Gaussian transformation for each optical devices, on the expression used to obtain the statistics of joined NPNR detections, and their derivations can be found in Appendix A of Article 4.

QuantumOpticalCircuits.jl Using the Julia programming language [Bez+17], we developed QuantumOpticalCircuits.jl, a package to simulate efficiently and accurately photonic setups [Val21]. This package relies on the Gaussian representation to store states in a compact form and to compute accurately the effect of optical gates and the outcomes of single photon detectors. It includes all the optical devices we listed above as well as NPNR detectors and heralded operations.

Our package makes extensive use of the multiple-dispatch paradigm of the Julia programming language. Hence, it can easily be extended to include other operations and measurements. Furthermore, we design this package with ease-of-use in mind, so that simulating photonic setups is programmatically simple. Finally, even if it is less efficient, we also provide a Fock representation back-end, as this representation is more common in the community. A simple example using this framework can be seen in Fig. (8.4).

8.3.2 . Reinforcement Learning

Reinforcement learning (RL) is a machine learning paradigm that involves an intelligent agent learning to perform a task by interacting with an environment [SB18]. Schematically, from the current state of an environment, an agent chooses an action to be performed. Feedback is then provided in the form of the new state of the environment as well as a *reward*, designed to quantify the quality of the selected action, with respect to the goal task. From this feedback, the agent updates the way actions are chosen in order to maximize the reward received. The definition of an RL scheme thus amounts to specifying its environment, agent, actions and reward function.

One of the key advantage of RL is that it does not require pre-generated data to be trained on, unlike supervised and unsupervised learning. This is particularly beneficial when generating data is costly as it is the case with the simulation of optical circuits.

RL has seen numerous successful applications to a great variety of tasks, from learning to play games [Mni+15; Sil+17; Vin+19] to finding new algorithm for

Figure 8.4: Example usage of QuantumOpticalCircuits.jl in the Julia REPL; the simulation of a two-mode photonic circuits where the first mode is squeezed after which a balanced beam splitter mixes the mode 1 and 2, and, finally a NPNR detector with efficiency $\eta = 0.8$ measures mode 1. Note that the probability of a *click* outcome slightly differs between the Gaussian, $p = 0.05495903420401427$ and the Fock back-end $p = 0.054904814588312534$. This is due to the necessary cut-off, here set at 5 photons, of the Fock representation which introduces some error compare to the exact value obtained when using the Gaussian representation.

matrix multiplications [Faw+22]. In the field of quantum physics, RL has been applied to design quantum error correction algorithms [And+19; Nau+19; Swe+20], quantum gates [Niu+19], or new quantum experiments [Mel+18; Kre+16; KEZ20; Kre+21], in particular to design photonic Bell test experiments [MSS20].

Motivated by these past works, in Article 4, we propose an approach that combines reinforcement learning with our photonic circuit simulation framework to generate new photonic experiment designs. As an agent we use proximal-policy optimization (PPO), a deep reinforcement learning algorithm, known to be sample efficient [Sch+17]. A fixed number of photonic modes constitute the environment. Actions that can be chosen from are optical devices that act on a specific mode or pair of modes. After appending a chosen action to the photonic circuit, an optimisation over the optical devices' parameters is run in order to maximize a given function of the statistics, e.g. a DIQKD key rate. This defines the reward function. From past experiences – state, chosen action, new state and reward – the PPO algorithm updates its policy so that future chosen actions maximize the reward obtained.

8.3.3 . Application to DIQKD

We used this automated approach to the design of DIQKD experiments where Alice and Bob each have access to a single bosonic mode. In order to ensure that our photonic setups are complete, we systematically finish the circuits by placing a pair of heterodyne measurements, i.e. a displacement operation followed by a NPNR detector on Alice's and on Bob's modes. We allow the agent to explore circuits that use an auxiliary mode, and place a NPNR detector on this mode in order to herald the state measured by Alice and Bob. We then consider two different rewards.

First, we pick the key rate Eq. (7.10) achieved in an ideal scenario, i.e. in the absence of losses and noises, as the reward to be maximized by the agent. In other words, for every photonic circuit considered by the agent, we compute the maximum key rate that can be achieved by this circuit by optimizing over all the circuit parameters. After training a PPO agent on that task, the best circuit we obtain is a fairly complex photonic circuit, composed of 12 elements. In the ideal case, this setup achieves a key rate of $r_{Ho} \approx 0.914$, outperforming the benchmark implementation detailed in Sec. 8.2. However, this setup seems not so robust to losses as we were able to obtain positive key rate for $\eta \gtrsim 0.874$ only.

Then, we craft a reward to maximize the robustness of the key rate to losses. We do this by first optimising the key rate in the ideal scenario. We then progressively lower the efficiency, re-optimizing the circuit's parameters for each new efficiency, until $\eta_{\approx \mathrm{crit}}$, the lowest efficiency such that $r \geq 10^{-4}$, is reached. The reward is directly proportional to $1 - \eta_{\approx \mathrm{crit}}$. Our method provides a simple circuit of only 7 optical devices, more robust than the reference implementation. Indeed, this setup output key rate $r_{Ho} \geq 10^{-8}$ for efficiency $\gtrsim 0.8245$. Furthermore, the obtained key rate are consistently higher than the one achieved by the benchmark

setup. These setups as well as their key rates as the function of the efficiency can be found in Article 4.

8.3.4 . Application toward continuous-variable DIQKD

Our automated approach for designing photonic experiments can be readily extended to implement any task that can be expressed as a function of measurements. An interesting task for quantum cryptography is *continuous-variable* DIQKD; DIQKD implementations in which Alice and Bob perform homodyne measurements, resolving the quadratures x, p of bosonic modes. These measurements are particularly relevant as they are known to be efficient and can be performed at a high repetition rate. However, if a violation of the CHSH inequality – the first step towards DIQKD – can be obtained in this regime, the implementation with the highest violation that has been proposed so far yield a score of $S \approx 2.046$ [Gar+04; GFC05]. From this low score, current DIQKD protocols provide a mere positive key rates, e.g. even considering the unrealistic case of $H(A'_0|B_2) = 0.0$, Eq. (7.10) gives only $r_{Ho} \approx 10^{-2}$. To improve on this violation, a proposal combining homodyne and NPNR detectors has shown an expected violation of $S \approx 2.25$ [Cav+11]. Note that a CHSH score of $S \approx 2.35$ with homodyne measurements has been reported, however, as it fails to close any loophole this setup has to be excluded for DIQKD [The+18].

It is in this context that we apply our automated method with the task of maximizing the CHSH violation using solely homodyne measurements, heralding operations, and the optical devices listed above. We limit our selves to the measurement settings proposed in [GFC05] and to a sign binning of the homodyne measurement outcomes. After learning, our intelligent agent proposed the circuit depicted in Fig. (8.5). Interestingly, this circuit attains a CHSH score of $S \approx 2.068$.

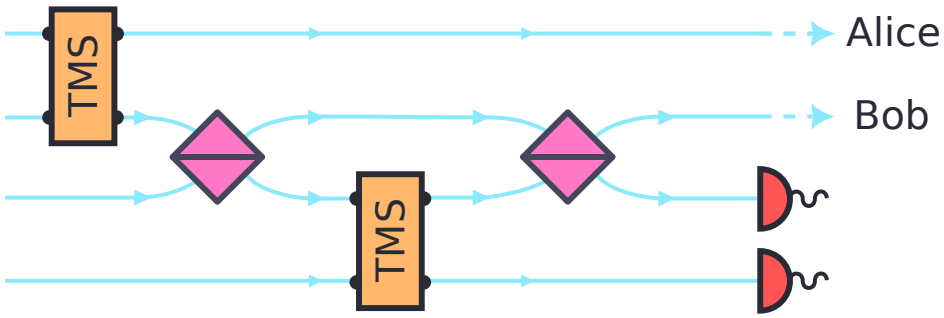


Figure 8.5: Circuit achieving a CHSH score $S \approx 2.068$. The blue lines are bosonic modes. The yellow rectangle labeled TMS represent two-mode squeezer, with optimal squeezing parameters $g_1 = 0.44689$ and $g_2 = 8.47 \times 10^{-3}$ respectively. The two sliced pink squares are beam-splitters with optimal parameters $\theta_1 = 0.04202$ and $\theta_2 = 0.04338$. The two red half circles represent NPNR detectors heralding the modes 3 and 4. The final prepared state is post-selected on a double click, i.e. in both mode 3 and 4, which occurs with a probability of $p \approx 4.05 \times 10^{-7}$. The first mode is then sent to Alice while the second is sent to Bob.

Article 3

Device-independent quantum key distribution from generalized CHSH inequalities

Pavel Sekatski[1], Jean-Daniel Bancal[2], Xavier Valcarce[3], Ernest Y.-Z. Tan[4], Renato Renner[4], and Nicolas Sangouard[1,3]

[1] Departement Physik, Universität Basel, Klingelbergstraße 82, 4056 Basel, Schweiz
[2] Department of Applied Physics, University of Geneva, Chemin de Pinchat 22, 1211 Geneva, Switzerland
[3] Université Paris-Saclay, CEA, CNRS, Institut de Physique Théorique, 91191 Gif-sur-Yvette, France
[4] Institute for Theoretical Physics, ETH Zürich, 8093 Zürich, Switzerland

Quantum, volume 5, page 444
arXiv preprint: 2009.01784v4

Abstract

Device-independent quantum key distribution aims at providing security guarantees even when using largely uncharacterised devices. In the simplest scenario, these guarantees are derived from the CHSH score, which is a simple linear combination of four correlation functions. We here derive a security proof from a generalisation of the CHSH score, which effectively takes into account the individual values of two correlation functions. We show that this additional information, which is anyway available in practice, allows one to get higher key rates than with the CHSH score. We discuss the potential advantage of this technique for realistic photonic implementations of device-independent quantum key distribution.

Article 4

Automated design of quantum optical experiments for device-independent quantum key distribution

Xavier Valcarce[1], Pavel Sekatski[2], Elie Gouzien[1], Alexey Melnikov[3], Nicolas Sangouard[1]

[1] Université Paris-Saclay, CEA, CNRS, Institut de Physique Théorique, 91191 Gif-sur-Yvette, France
[2] Department of Applied Physics, University of Geneva, Chemin de Pinchat 22, 1211 Geneva, Switzerland
[3] Terra Quantum AG, 9000 St Gallen, Switzerland

Phys. Rev. A 107, 062607
arXiv preprint: 2209.06468

Abstract

Device-independent quantum key distribution (DIQKD) reduces the vulnerability to side-channel attacks of standard QKD protocols by removing the need for characterized quantum devices. The higher security guarantees come however, at the price of a challenging implementation. Here, we tackle the question of the conception of an experiment for implementing DIQKD with photonic devices. We introduce a technique combining reinforcement learning, optimisation algorithm and a custom efficient simulation of quantum optics experiments to automate the design of photonic setups maximizing a given function of the measurement statistics. Applying the algorithm to DIQKD, we get unexpected experimental configurations leading to high key rates and to a high resistance to loss and noise. These configurations might be helpful to facilitate a first implementation of DIQKD with photonic devices and for future developments targeting improved performances.

IV – Conclusion and perspectives

In this thesis we presented our work on device-independent quantum information protocols, improving them with the end goal of easing their experimental implementations, and answering some fundamental questions along the way. As quantum information applications are expected to have an important impact on current technologies, notably revolutionizing computation and communication tasks, the device-independent framework appears as a necessity. Indeed, for quantum information protocols to replace their current classical counterparts, stable and robust implementations are as crucial as improved performances. Moreover, in a global world where communication is key and where manufacturing is scattered across numerous actors, there is the need for cryptographic systems which not only come with the highest security proofs but also with the capability to detect the presence of interferences from the devices they rely on. Device-independent protocols address these concerns by allowing certifications of resources and security guarantees without relying on assumption on their inner working.

Self-testing In the first part of this thesis, we study the most fundamental device-independent protocol, self-testing. Self-testing enables the device-independent certification of certain quantum resources from the presence of specific non-local correlations. In particular, from the maximal CHSH score, it is possible to self-test two-qubit maximally entangled states and maximally incompatible measurements. For real world applications, robust singlet self-testing provides the certification of a singlet-fraction from lower violation of the CHSH inequality, naturally occurring in a noisy and lossy regime. One of our contributions to this topic concerns the quantification of the fundamental resources that are required for robust self-testing of the singlet. Notably, we showed that the CHSH score $S \approx 2.05$ is a threshold below which robust self-testing fails [Val+20]. From the relatively high value of this threshold, we emphasized the need for new robust self-testing protocols which provide certification beyond the CHSH score. To tackle this matter, we formulated an original protocol in [Val+22], leveraging the available information of correlators pair to provide better robustness bounds without changing experimental requirements. Interestingly, in the case of imbalanced noises, our protocol allows for self-tests below the CHSH threshold of $S \approx 2.05$ and even as close as the local bound, $S = 2$, providing an asymmetric enough noise. Our new protocol, henceforth, eases the experimental realization of device-independent protocols based on the certification of singlet states.

Our results on self-testing, show the need for more robust self-testing protocols, point at directions where improvements can be obtained, and raise some more fundamental questions. First, the CHSH-score threshold we derived is still far from the bound $S \approx 2.11$ given by the best known CHSH-based self-testing protocol [Kan16]. Therefore, an improvement is to be expected on the threshold or on the bound $S \approx 2.11$, e.g. by improving on the local isometries proposed in [Kan16], or on both. Then, analogously to what has been done for DIQKD [BFF21], one

can hope for a robust self-testing protocol harnessing all of the available statistics. Insights obtained from our generalized-CHSH based self-test show that such a protocol should help provide self-tests that are robust to any type of noises. This would be a crucial step not only to ease the implementation of self-testing, but also to make self-testing a handy and flexible certification tool, that could be used as a complementary tool with tomography. Finally, better robustness bound could arise when considering a scenario with more than 2 inputs and outputs. However, this would require derivations that do not rely on Jordan's lemma. If the SWAP method provides a numerical solution to self-testing from all the correlations and without relying on Jordan's lemma, its general scope yields suboptimal extractability bound in the case of the singlet [Yan+14; Ban+15]. An improved SWAP method may thus be derived. Elements from the approach [BFF21] may be useful to tackle this problem as well.

More broadly, robust self-testing methods should be extended to enable the certification of not just states, but entire quantum systems. First, the robust self-testing of quantum channels, introduced in [Sek+18], could be extended to certify quantum measurements beyond commutation [Kan17]. A framework for the robust self-testing of joint quantum measurements beyond the Bell-state measurement [BSS18; RKB18] could then be developed. Finally, this may lead to *complete self-tests*, certifying at once both states and measurements. For each of these methods, it is desired to have proofs valid in non-IID scenarios to enable practical applications. Intuitively, the approach based on estimators on the statistics demonstrated in [Ban+21] could be extended to these more complete self-tests.

DIQKD In the second part of this thesis, we focus on device-independent quantum key distribution (DIQKD), the protocol allowing two parties to share a secret key in a provable way. Security proofs are commonly found in the form of a key rate guaranteeing a fraction of secure key bit per protocol run. After the derivation of a first practical key rate from the CHSH score, numerous improvements pushed that key rate to higher values and increased its robustness to losses. On the experimental side, photonic setups seem the most promising platform for long-term DIQKD applications. However, the SPDC setup – the photonic implementation successfully used in Bell tests – only achieves low CHSH score in realistic efficiency regimes, thus yielding key rates that are only slightly positive. Therefore, in order to ease photonic DIQKD realizations, we aimed at improving DIQKD security proofs. In [Sek+21] we propose a new proof which utilizes more information from the available statistics than the sole CHSH score. This refined analysis allows us to more tightly bound the information an eavesdropper can get access to and, therefore, improve the key rate. Considering the SPDC setup, our security proof increases the key rate by 37% in the ideal scenario. However, we did not witness an improvement of the critical efficiency. We thus tackled the problem of enabling photonic DIQKD realizations from another perspective. Using reinforcement learning and a

custom-made simulation framework, we crafted a method to automate the design of photonic experiments [Val+23]. When applied to DIQKD, our method proposed new setups yielding both higher rates and a better robustness to losses compared to the SPDC setup. Additionally, the flexibility of our approach led us to find a setups based on homodyne measurements, achieving CHSH score higher than the local bound.

Together, our works contribute to progress for the first realization of a photonic DIQKD experiment. The higher key rate resulting from our DIQKD protocol lowers requirements on the repetition rate of experiments. Additionally, the new photonic setup designs we propose leads to positive key rate for a reduced constraint on the efficiency.

The recent development of DIQKD protocols are important steps for new proof-of-concept DIQKD experiments. However, for the low efficiency regime that is characteristic of photonic setups, further improvements are required to push the key rate by orders of magnitude. One improvement could come from a more general pre-processing of inputs and outcomes, i.e. an extension of noisy pre-processing [Ho+20]. Indeed, works in non-locality distillation have shown that pre-processing may amplify the non-local nature of correlations [FWW09]. It would be interesting to find out whether a general pre-processing could enable the distillation of better rates from current DIQKD protocols.

Additionally, in this thesis we focused on asymptotic key rates of DIQKD protocols, but finite-size effects need to be taken into account in order to guarantee that a protocol can actually produce a key [Tan21]. In particular, the entropy accumulation theorem (EAT), the main theoretical tool able to produce finite-size security proofs valid under coherent attacks, is costly – resulting in lower key rates. This cost could be mitigated by a modified version of EAT that would yield better bounds, notably on the smooth max entropy of Eve on Bob's outcomes. Furthermore, for given correlations, bounding the adversary's information in terms of a Bell inequality better suited than CHSH could be used as the min-tradeoff function on which the EAT relies. Such an inequality can be extracted from the dual formulation of the problem Eq. (7.21).

For every new security proof and protocol improvement, it is also worth analyzing standard photonic setups, such as the SPDC setup, as well as newly proposed ones. For example, with the currently best known bound on Eve's uncertainty on the key and the capacity to consider all measurements outcomes in the security proof, positive key rates at practical efficiencies from these setups may already be obtained with the protocol introduced in [BFF21].

Finally, it is necessary to develop new experimental designs for the implementation of DIQKD. These new designs should progressively address practical requirements and limitations, e.g. a decent scalability with the distance between parties, the ability to operate at a high rate, or the capacity to transmit photons at telecom

wavelength. Reinforcement learning may help generate new experiments blueprints covering some of these points. Furthermore, progress in other quantum information processing field, such as quantum computing or quantum simulation, may provide new solutions to these challenges. For example, as suggested in [Zap+23], arrays of trapped atoms or ions could help multiplexing the generation of entanglement, helping heralded entanglement systems to operate at a higher rate.

Towards a Quantum Internet While all device-independent protocols possess promising applications, their use in a quantum internet may unlock more powerful and concrete possibilities. The quantum internet is a hypothetical network of classical and quantum devices, connected by links in which both classical and quantum information transit. This upgraded version of the current Internet will provide new functionalities with the two most notable ones being communication secured by quantum cryptography and enhance computational power from quantum computers. If currently many challenges are in the way of a quantum Internet, however, incentives for its realization are flourishing. Indeed, promises in quantum computing, from fault-tolerant quantum computing heading the roadmap of some companies [Goo22; Int22; IBM22] to potential groundbreaking quantum computation advantages [DJ92; Sho94; Gro96] and applications [Bau+20; Pau+22] are pushing for the accessibility of quantum computers via internet [Rie+22]. Securing access to cloud quantum computing seems therefore to be the first key element for a quantum internet.

The ability to process quantum information in the cloud requires new stability and security guarantees. With a minimal set of assumptions, self-testing is a privileged candidate to guarantee the proper functioning of elements involved in cloud quantum computing [Sek+18]. Indeed, self-testing may become the tool of choice for the certification of network links, quantum gates and quantum measurements. Manufacturers and cloud providers could thus use self-testing to reliably identify faulty elements in their systems. Future progress in self-testing could lead to even more general protocol where composite systems could be self-tested, scaling the capacity for error detection.

Furthermore, self-testing can be combined with verifiable blind quantum computing [Fit17; Eis+20] – a line of research providing security protocols guaranteeing the verifiability and integrity of a computation delegated to a quantum computer – to provide device-independent certifications of computations [RUV13; GKW15; HPF15; McK16].

To secure the transit of information, be it classical or quantum, quantum key distribution provides the strongest security guarantee. Nowadays, QKD is however not privileged by the security agencies of numerous countries, such as France [ANS20], the UK [NCS20] and the USA [NSA21]. These agencies unanimously criticize the need for a special infrastructure, the required trust in relay points and the susceptibility to attacks from an eavesdropper. The former might be

covered by infrastructure requirements for quantum computing and encouraged by potential quantum communication applications such as quantum money [Wie83; MVW13]. Furthermore, developing on-chip QKD systems coupled with transmission at telecom wavelength would reduce infrastructure changes to simply adding QKD rack units in data centers. Device-independent quantum key distribution protocols address the last two concerns; the device-independent approach removes the need to trust relays and protocols secure against coherent attacks prevent any type of hacking.

In the perspective of a quantum internet, device-independent protocols could bring solutions to many aspects desired by end-users. Security and privacy, listed as important issues by the Electronic Frontier Foundation [EFFa; EFFb], are among them. The device-independent framework could guarantee the protection of users' data by reducing the level of trust required in external actors. It marks a step towards truly secure communications and may enable the remote processing and long term storage of private data, even by mistrustful third parties. With guarantees obtainable by end users directly, device-independent protocols may also help build a more decentralize world, as the need for central authorities would become obsolete. Finally, one should not forget that even if technologies are developed with good intentions, it should ultimately be up to the people through democratic processes to guide their usage.

Bibliography

[Ací+07] Antonio Acín et al. “Device-Independent Security of Quantum Cryptography against Collective Attacks”. In: *Physical Review Letters* 98.23 (June 2007). doi: 10.1103/physrevlett.98.230501. url: https://doi.org/10.1103/physrevlett.98.230501.

[ADR82] Alain Aspect, Jean Dalibard, and Gérard Roger. “Experimental Test of Bell’s Inequalities Using Time- Varying Analyzers”. In: *Physical Review Letters* 49.25 (Dec. 1982), pp. 1804–1807. doi: 10.1103/physrevlett.49.1804. url: https://doi.org/10.1103/physrevlett.49.1804.

[AGR82] Alain Aspect, Philippe Grangier, and Gérard Roger. “Experimental Realization of Einstein-Podolsky-Rosen-Bohm Gedankenexperiment: A New Violation of Bell’s Inequalities”. In: *Physical Review Letters* 49.2 (July 1982), pp. 91–94. doi: 10.1103/physrevlett.49.91. url: https://doi.org/10.1103/physrevlett.49.91.

[AM16] Antonio Acín and Lluis Masanes. “Certified randomness in quantum physics”. In: *Nature* 540.7632 (Dec. 2016), pp. 213–219. doi: 10.1038/nature20119. url: https://doi.org/10.1038/nature20119.

[And+19] Philip Andreasson et al. “Quantum error correction for the toric code using deep reinforcement learning”. In: *Quantum* 3 (Sept. 2019), p. 183. doi: 10.22331/q-2019-09-02-183. url: https://doi.org/10.22331/q-2019-09-02-183.

[ANS20] ANSSI. “Should Quantum Key Distribution be Used for Secure Communications?” In: *ANSSI - Technical Position Paper: QKD v2.1* (2020). url: https://www.ssi.gouv.fr/uploads/2020/05/anssi-technical_position_papers-qkd.pdf (visited on 05/30/2020).

[Arn+18] Rotem Arnon-Friedman et al. “Practical device-independent quantum cryptography via entropy accumulation”. In: *Nature Communications* 9.1 (Jan. 2018). doi: 10.1038/s41467-017-02307-4. url: https://doi.org/10.1038/s41467-017-02307-4.

[ARV19] Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick. "Simple and Tight Device-Independent Security Proofs". In: *SIAM Journal on Computing* 48.1 (Jan. 2019), pp. 181–225. doi: 10.1137/18m1174726. url: https://doi.org/10.1137/18m1174726.

[Ban+15] Jean-Daniel Bancal et al. "Physical characterization of quantum devices from nonlocal correlations". In: *Physical Review A* 91.2 (Feb. 2015). doi: 10.1103/PhysRevA.91.022115. url: https://link.aps.org/doi/10.1103/PhysRevA.91.022115.

[Ban+21] Jean-Daniel Bancal et al. "Self-testing with finite statistics enabling the certification of a quantum network link". In: *Quantum* 5 (Mar. 2021), p. 401. issn: 2521-327X. doi: 10.22331/q-2021-03-02-401. url: https://doi.org/10.22331/q-2021-03-02-401.

[Bar+09] C.-E. Bardyn et al. "Device-independent state estimation based on Bell's inequalities". In: *Physical Review A* 80.6 (Dec. 2009). doi: 10.1103/PhysRevA.80.062327. url: https://doi.org/10.1103/PhysRevA.80.062327.

[Bau+20] Bela Bauer et al. "Quantum Algorithms for Quantum Chemistry and Quantum Materials Science". In: *Chemical Reviews* 120.22 (Oct. 2020), pp. 12685–12717. doi: 10.1021/acs.chemrev.9b00829. url: https://doi.org/10.1021/acs.chemrev.9b00829.

[BB84] Charles H Bennett and Gilles Brassard. "Quantum cryptography: public key distribution and coin tossing." In: *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (1984), p. 175.

[Bel64] J. S. Bell. "On the Einstein Podolsky Rosen paradox". In: *Physics Physique Fizika* 1.3 (Nov. 1964), pp. 195–200. doi: 10.1103/physicsphysiquefizika.1.195.

[Bez+17] Jeff Bezanson et al. "Julia: A fresh approach to numerical computing". In: *SIAM review* 59.1 (2017), pp. 65–98. url: https://doi.org/10.1137/141000671.

[BFF21] Peter Brown, Hamza Fawzi, and Omar Fawzi. "Device-independent lower bounds on the conditional von Neumann entropy". In: (2021). eprint: arXiv:2106.13692.

[Bia+17] Jacob Biamonte et al. "Quantum machine learning". In: *Nature* 549.7671 (Sept. 2017), pp. 195–202. doi: 10.1038/nature23474. url: https://doi.org/10.1038/nature23474.

[BP15] Cédric Bamps and Stefano Pironio. “Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing”. In: *Phys. Rev. A* 91 (5 May 2015), p. 052111. doi: 10.1103/PhysRevA.91.052111. url: https://link.aps.org/doi/10.1103/PhysRevA.91.052111.

[Bru+02] Dagmar Bruß et al. “Reflections upon separability and distillability”. In: *Journal of Modern Optics* 49.8 (July 2002), pp. 1399–1418. doi: 10.1080/09500340110105975. url: https://doi.org/10.1080/09500340110105975.

[Bru+14] Nicolas Brunner et al. “Bell nonlocality”. In: *Rev. Mod. Phys.* 86 (2 Apr. 2014), pp. 419–478. doi: 10.1103/RevModPhys.86.419. url: https://link.aps.org/doi/10.1103/RevModPhys.86.419.

[BSS18] Jean-Daniel Bancal, Nicolas Sangouard, and Pavel Sekatski. “Noise-Resistant Device-Independent Certification of Bell State Measurements”. In: *Phys. Rev. Lett.* 121 (25 Dec. 2018), p. 250506. doi: 10.1103/PhysRevLett.121.250506. url: https://link.aps.org/doi/10.1103/PhysRevLett.121.250506.

[Cav+11] Daniel Cavalcanti et al. “Large violation of Bell inequalities using both particle andwave measurements”. In: *Physical Review A* 84.2 (Aug. 2011). doi: 10.1103/physreva.84.022105. url: https://doi.org/10.1103/physreva.84.022105.

[CD22] Wouter Castryck and Thomas Decru. *An efficient key recovery attack on SIDH*. Cryptology ePrint Archive, Paper 2022/975. https://eprint.iacr.org/2022/975. 2022. url: https://eprint.iacr.org/2022/975.

[CGS17] Andrea Coladangelo, Koon Tong Goh, and Valerio Scarani. “All pure bipartite entangled states can be self-tested”. In: *Nature Communications* 8.1 (May 2017). doi: 10.1038/ncomms15485. url: https://doi.org/10.1038/ncomms15485.

[CKS19] Tim Coopmans, J ędrzej Kaniewski, and Christian Schaffner. “Robust self-testing of two-qubit states”. In: *Phys. Rev. A* 99 (5 May 2019), p. 052123. doi: 10.1103/PhysRevA.99.052123. url: https://link.aps.org/doi/10.1103/PhysRevA.99.052123.

[Cla+69] John F. Clauser et al. “Proposed Experiment to Test Local Hidden-Variable Theories”. In: *Phys. Rev. Lett.* 23 (15 Oct. 1969), pp. 880–884. doi: 10.1103/PhysRevLett.23.880.

[Cyb21] European Union Agency for Cybersecurity. *Post-quantum cryptography: current state and quantum mitigation.* Publications Office, 2021. doi: 10.2824/92307. url: https://data.europa.eu/doi/10.2824/92307.

[DF19] Frederic Dupuis and Omar Fawzi. "Entropy Accumulation With Improved Second-Order Term". In: *IEEE Transactions on Information Theory* 65.11 (Nov. 2019), pp. 7596–7612. doi: 10.1109/tit.2019.2929564. url: https://doi.org/10.1109/tit.2019.2929564.

[DFR20] Frédéric Dupuis, Omar Fawzi, and Renato Renner. "Entropy Accumulation". In: *Communications in Mathematical Physics* 379.3 (Sept. 2020), pp. 867–913. doi: 10.1007/s00220-020-03839-5. url: https://doi.org/10.1007/s00220-020-03839-5.

[Dia+16] Eleni Diamanti et al. "Practical challenges in quantum key distribution". In: *npj Quantum Information* 2.1 (Nov. 2016). doi: 10.1038/npjqi.2016.25. url: https://doi.org/10.1038/npjqi.2016.25.

[DJ92] David Deutsch and Richard Jozsa. "Rapid solution of problems by quantum computation". In: *Proceedings of the Royal Society of London. Series A: Mathematical and Physical Sciences* 439.1907 (Dec. 1992), pp. 553–558. doi: 10.1098/rspa.1992.0167. url: https://doi.org/10.1098/rspa.1992.0167.

[DPS03] G. Mauro D'Ariano, Matteo G.A. Paris, and Massimiliano F. Sacchi. "Quantum Tomography". In: *Advances in Imaging and Electron Physics*. Elsevier, 2003, pp. 205–308. doi: 10.1016/s1076-5670(03)80065-4. url: https://doi.org/10.1016/s1076-5670(03)80065-4.

[DW05] Igor Devetak and Andreas Winter. "Distillation of secret key and entanglement from quantum states". In: *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences* 461.2053 (Jan. 2005), pp. 207–235. doi: 10.1098/rspa.2004.1372. url: https://doi.org/10.1098/rspa.2004.1372.

[Ebe93] Philippe H. Eberhard. "Background level and counter efficiencies required for a loophole-free Einstein-Podolsky-Rosen experiment". In: *Physical Review A* 47.2 (Feb. 1993), R747–R750. doi: 10.1103/physreva.47.r747. url: https://doi.org/10.1103/physreva.47.r747.

[EFFa] Electronic Frontier Foundation (EFF). *Privacy*. url: https://www.eff.org/issues/privacy.

[EFFb] Electronic Frontier Foundation (EFF). *Security*. url: https://www.eff.org/issues/security.

[Eis+20] Jens Eisert et al. "Quantum certification and benchmarking". In: *Nature Reviews Physics* 2.7 (June 2020), pp. 382–390. doi: 10.1038/s42254-020-0186-4. url: https://doi.org/10.1038/s42254-020-0186-4.

[Eke91] Artur K. Ekert. "Quantum cryptography based on Bell's theorem". In: *Physical Review Letters* 67.6 (Aug. 1991), pp. 661–663. doi: 10.1103/physrevlett.67.661. url: https://doi.org/10.1103/physrevlett.67.661.

[EPR35] A. Einstein, B. Podolsky, and N. Rosen. "Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?" In: *Phys. Rev.* 47 (10 May 1935), pp. 777–780. doi: 10.1103/PhysRev.47.777. url: https://link.aps.org/doi/10.1103/PhysRev.47.777.

[Faw+22] Alhussein Fawzi et al. "Discovering faster matrix multiplication algorithms with reinforcement learning". In: *Nature* 610.7930 (Oct. 2022), pp. 47–53. doi: 10.1038/s41586-022-05172-4. url: https://doi.org/10.1038/s41586-022-05172-4.

[FC72] Stuart J. Freedman and John F. Clauser. "Experimental Test of Local Hidden-Variable Theories". In: *Physical Review Letters* 28.14 (Apr. 1972), pp. 938–941. doi: 10.1103/physrevlett.28.938. url: https://doi.org/10.1103/physrevlett.28.938.

[Fit17] Joseph F. Fitzsimons. "Private quantum computation: an introduction to blind quantum computing and related protocols". In: *npj Quantum Information* 3.1 (June 2017). doi: 10.1038/s41534-017-0025-3. url: https://doi.org/10.1038/s41534-017-0025-3.

[FM18] Honghao Fu and Carl A. Miller. "Local randomness: Examples and application". In: *Physical Review A* 97.3 (Mar. 2018). doi: 10.1103/physreva.97.032324. url: https://doi.org/10.1103/physreva.97.032324.

[Fun+07] Chi-Hang Fred Fung et al. "Phase-remapping attack in practical quantum-key-distribution systems". In: *Physical Review A* 75.3 (Mar. 2007). doi: 10.1103/physreva.75.032314. url: https://doi.org/10.1103/physreva.75.032314.

[FWW09] Manuel Forster, Severin Winkler, and Stefan Wolf. “Distilling Nonlocality”. In: *Physical Review Letters* 102.12 (Mar. 2009). doi: 10.1103/physrevlett.102.120401. url: https://doi.org/10.1103/physrevlett.102.120401.

[Gar+04] R. García-Patrón et al. “Proposal for a Loophole-Free Bell Test Using Homodyne Detection”. In: *Physical Review Letters* 93.13 (Sept. 2004). doi: 10.1103/physrevlett.93.130409. url: https://doi.org/10.1103/physrevlett.93.130409.

[Ger+11] Ilja Gerhardt et al. “Full-field implementation of a perfect eavesdropper on a quantum cryptography system”. In: *Nature Communications* 2.1 (June 2011). doi: 10.1038/ncomms1348. url: https://doi.org/10.1038/ncomms1348.

[GFC05] Raúl García-Patrón, Jaromír Fiurášek, and Nicolas J. Cerf. “Loophole-free test of quantum nonlocality using high-efficiency homodyne detectors”. In: *Physical Review A* 71.2 (Feb. 2005). doi: 10.1103/physreva.71.022105. url: https://doi.org/10.1103/physreva.71.022105.

[GG02] Frédéric Grosshans and Philippe Grangier. “Continuous Variable Quantum Cryptography Using Coherent States”. In: *Physical Review Letters* 88.5 (Jan. 2002). doi: 10.1103/physrevlett.88.057902. url: https://doi.org/10.1103/physrevlett.88.057902.

[Gis+02] Nicolas Gisin et al. “Quantum cryptography”. In: *Reviews of Modern Physics* 74.1 (Mar. 2002), pp. 145–195. doi: 10.1103/revmodphys.74.145. url: https://doi.org/10.1103/revmodphys.74.145.

[Giu+15] Marissa Giustina et al. “Significant-Loophole-Free Test of Bell’s Theorem with Entangled Photons”. In: *Physical Review Letters* 115.25 (Dec. 2015). doi: 10.1103/physrevlett.115.250401. url: https://doi.org/10.1103/physrevlett.115.250401.

[GKW15] Alexandru Gheorghiu, Elham Kashefi, and Petros Wallden. “Robustness and device independence of verifiable blind quantum computing”. In: *New Journal of Physics* 17.8 (Aug. 2015), p. 083040. doi: 10.1088/1367-2630/17/8/083040. url: https://doi.org/10.1088/1367-2630/17/8/083040.

[Goo22] Google. *Our quantum computing journey*. 2022. url: https://quantumai.google/learn/map.

[Gou+23] Élie Gouzien et al. *Computing 256-bit Elliptic Curve Logarithm in 9 Hours with 126133 Cat Qubits*. 2023. eprint: arXiv:2302.06639.

[GPS10] Nicolas Gisin, Stefano Pironio, and Nicolas Sangouard. "Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier". In: *Phys. Rev. Lett.* 105 (7 Aug. 2010), p. 070501. doi: 10.1103/PhysRevLett.105.070501. url: https://link.aps.org/doi/10.1103/PhysRevLett.105.070501.

[Gro+03] Frédéric Grosshans et al. "Quantum key distribution using gaussian-modulated coherent states". In: *Nature* 421.6920 (Jan. 2003), pp. 238–241. doi: 10.1038/nature01289. url: https://doi.org/10.1038/nature01289.

[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 - STOC '96*. ACM Press, 1996. doi: 10.1145/237814.237866. url: https://doi.org/10.1145/237814.237866.

[GS21] Élie Gouzien and Nicolas Sangouard. "Factoring 2048-bit RSA Integers in 177 Days with 13 436 Qubits and a Multimode Memory". In: *Physical Review Letters* 127.14 (Sept. 2021). doi: 10.1103/physrevlett.127.140503. url: https://doi.org/10.1103/physrevlett.127.140503.

[Hen+15] B. Hensen et al. "Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres". In: *Nature* 526.7575 (Oct. 2015), pp. 682–686. doi: 10.1038/nature15759. url: https://doi.org/10.1038/nature15759.

[Ho+20] M. Ho et al. "Noisy Preprocessing Facilitates a Photonic Realization of Device-Independent Quantum Key Distribution". In: *Physical Review Letters* 124.23 (June 2020). doi: 10.1103/physrevlett.124.230502. url: https://doi.org/10.1103/physrevlett.124.230502.

[HPF15] Michal Hajdušek, Carlos A. Pérez-Delgado, and Joseph F. Fitzsimons. "Device-Independent Verifiable Blind Quantum Computation". In: (2015). doi: 10.48550/ARXIV.1502.02563. url: https://arxiv.org/abs/1502.02563.

[IBM22] IBM. *IBM Quantum Roadmap*. 2022. url: https://research.ibm.com/blog/ibm-quantum-roadmap-2025.

[Int22] Intel. *Quantum Computing Backgrounder*. 2022. url: https://download.intel.com/newsroom/2022/new-technologies/quantum-computing-backgrounder.pdf.

[Kan16] Jędrzej Kaniewski. "Analytic and Nearly Optimal Self-Testing Bounds for the Clauser-Horne-Shimony-Holt and Mermin Inequalities". In: *Physical Review Letters* 117.7 (Aug. 2016). doi: 10.1103/physrevlett.117.070402. url: https://doi.org/10.1103/physrevlett.117.070402.

[Kan17] Jędrzej Kaniewski. "Self-testing of binary observables based on commutation". In: *Physical Review A* 95.6 (June 2017). doi: 10.1103/PhysRevA.95.062323. url: https://doi.org/10.1103/PhysRevA.95.062323.

[KEZ20] Mario Krenn, Manuel Erhard, and Anton Zeilinger. "Computer-inspired quantum experiments". In: *Nature Reviews Physics* 2.11 (Sept. 2020), pp. 649–661. doi: 10.1038/s42254-020-0230-4. url: https://doi.org/10.1038/s42254-020-0230-4.

[KGR05] B. Kraus, N. Gisin, and R. Renner. "Lower and Upper Bounds on the Secret-Key Rate for Quantum Key Distribution Protocols Using One-Way Classical Communication". In: *Physical Review Letters* 95.8 (Aug. 2005). doi: 10.1103/physrevlett.95.080501. url: https://doi.org/10.1103/physrevlett.95.080501.

[Kre+16] Mario Krenn et al. "Automated Search for new Quantum Experiments". In: *Physical Review Letters* 116.9 (Mar. 2016). doi: 10.1103/physrevlett.116.090405. url: https://doi.org/10.1103/physrevlett.116.090405.

[Kre+21] Mario Krenn et al. "Conceptual Understanding through Efficient Automated Design of Quantum Optical Experiments". In: *Physical Review X* 11.3 (Aug. 2021). doi: 10.1103/physrevx.11.031044. url: https://doi.org/10.1103/physrevx.11.031044.

[KST22] Srijita Kundu, Jamie Sikora, and Ernest Y.-Z. Tan. "A device-independent protocol for XOR oblivious transfer". In: *Quantum* 6 (May 2022), p. 725. doi: 10.22331/q-2022-05-30-725. url: https://doi.org/10.22331/q-2022-05-30-725.

[LCT14] Hoi-Kwong Lo, Marcos Curty, and Kiyoshi Tamaki. "Secure quantum key distribution". In: *Nature Photonics* 8.8 (July 2014), pp. 595–604. doi: 10.1038/nphoton.2014.149. url: https://doi.org/10.1038/nphoton.2014.149.

[Li+18] Ming-Han Li et al. “Test of Local Realism into the Past without Detection and Locality Loopholes”. In: *Physical Review Letters* 121.8 (Aug. 2018). doi: 10.1103/physrevlett.121.080404. url: https://doi.org/10.1103/physrevlett.121.080404.

[Lia+17] Sheng-Kai Liao et al. “Satellite-to-ground quantum key distribution”. In: *Nature* 549.7670 (Aug. 2017), pp. 43–47. doi: 10.1038/nature23655. url: https://doi.org/10.1038/nature23655.

[Liu+18] Yang Liu et al. “Device-independent quantum random-number generation”. In: *Nature* 562.7728 (Sept. 2018), pp. 548–551. doi: 10.1038/s41586-018-0559-3. url: https://doi.org/10.1038/s41586-018-0559-3.

[Liu+21] Wen-Zhao Liu et al. “Device-independent randomness expansion against quantum side information”. In: *Nature Physics* 17.4 (Feb. 2021), pp. 448–451. doi: 10.1038/s41567-020-01147-2. url: https://doi.org/10.1038/s41567-020-01147-2.

[Liu+22] Wen-Zhao Liu et al. “Toward a Photonic Demonstration of Device-Independent Quantum Key Distribution”. In: *Physical Review Letters* 129.5 (July 2022). doi: 10.1103/physrevlett.129.050502. url: https://doi.org/10.1103/physrevlett.129.050502.

[Łuk+22] Karol Łukanowski et al. “Upper Bounds on Key Rates in Device-Independent Quantum Key Distribution Based on Convex-Combination Attacks”. In: *Quantum 2.0 Conference and Exhibition*. Optica Publishing Group, 2022, QTu4C.1. doi: 10.1364/QUANTUM.2022.QTu4C.1. url: https://opg.optica.org/abstract.cfm?URI=QUANTUM-2022-QTu4C.1.

[Lyd+10] Lars Lydersen et al. “Hacking commercial quantum cryptography systems by tailored bright illumination”. In: *Nature Photonics* 4.10 (Aug. 2010), pp. 686–689. doi: 10.1038/nphoton.2010.214. url: https://doi.org/10.1038/nphoton.2010.214.

[Mag+06] Frédéric Magniez et al. “Self-testing of Quantum Circuits”. In: *Automata, Languages and Programming*. Springer Berlin Heidelberg, 2006, pp. 72–83. doi: 10.1007/11786986_8. url: https://doi.org/10.1007/11786986_8.

[May01] Dominic Mayers. “Unconditional security in quantum cryptography”. In: *Journal of the ACM* 48.3 (May 2001), pp. 351–406. doi: 10.1145/382780.382781. url: https://doi.org/10.1145/382780.382781.

[McK16] Matthew McKague. “Interactive Proofs for BQP via Self-Tested Graph States”. In: *Theory of Computing* 12.1 (2016), pp. 1–42. doi: 10.4086/toc.2016.v012a003. url: https://doi.org/10.4086/toc.2016.v012a003.

[Mel+18] Alexey A. Melnikov et al. “Active learning machine learns to create new quantum experiments”. In: *Proceedings of the National Academy of Sciences* 115.6 (Jan. 2018), pp. 1221–1226. doi: 10.1073/pnas.1714936115. url: https://doi.org/10.1073/pnas.1714936115.

[Mil20] Greg Miller. “The intelligence coup of the century”. In: *The Washington Post* (Feb. 11, 2020). url: https://www.washingtonpost.com/graphics/2020/world/national-security/cia-crypto-encryption-machines-espionage/ (visited on 02/11/2020).

[ML12] Xiongfeng Ma and Norbert Lütkenhaus. “Improved data post-processing in quantum key distribution and application to loss thresholds in device independent QKD”. In: *Quantum Inf. Comput.* 12.3-4 (2012), pp. 203–214. doi: 10.26421/QIC12.3-4-2. url: https://doi.org/10.26421/QIC12.3-4-2.

[Mni+15] Volodymyr Mnih et al. “Human-level control through deep reinforcement learning”. In: *Nature* 518.7540 (Feb. 2015), pp. 529–533. doi: 10.1038/nature14236. url: https://doi.org/10.1038/nature14236.

[MSS20] Alexey A. Melnikov, Pavel Sekatski, and Nicolas Sangouard. “Setting Up Experimental Bell Tests with Reinforcement Learning”. In: *Physical Review Letters* 125.16 (Oct. 2020). doi: 10.1103/physrevlett.125.160401. url: https://doi.org/10.1103/physrevlett.125.160401.

[MVW13] Abel Molina, Thomas Vidick, and John Watrous. “Optimal Counterfeiting Attacks and Generalizations for Wiesner’s Quantum Money”. In: *Theory of Quantum Computation, Communication, and Cryptography*. Springer Berlin Heidelberg, 2013, pp. 45–64. doi: 10.1007/978-3-642-35656-8_4. url: https://doi.org/10.1007/978-3-642-35656-8_4.

[MY04] Dominic Mayers and Andrew Yao. “Self Testing Quantum Apparatus”. In: *Quantum Info. Comput.* 4.4 (July 2004), pp. 273–286. issn: 1533-7146.

[MYS12] M McKague, T H Yang, and V Scarani. “Robust self-testing of the singlet”. In: *Journal of Physics A: Mathematical and Theoretical* 45.45 (Oct. 2012), p. 455304. doi: 10.1088/1751-8113/45/45/455304. url: https://doi.org/10.1088/1751-8113/45/45/455304.

[Nad+22] D. P. Nadlinger et al. “Experimental quantum key distribution certified by Bell’s theorem”. In: *Nature* 607.7920 (July 2022), pp. 682–686. doi: 10.1038/s41586-022-04941-5. url: https://doi.org/10.1038/s41586-022-04941-5.

[Nau+19] Hendrik Poulsen Nautrup et al. “Optimizing Quantum Error Correction Codes with Reinforcement Learning”. In: *Quantum* 3 (Dec. 2019), p. 215. doi: 10.22331/q-2019-12-16-215. url: https://doi.org/10.22331/q-2019-12-16-215.

[NC12] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, June 2012. doi: 10.1017/cbo9780511976667. url: https://doi.org/10.1017/cbo9780511976667.

[NCS20] NCSC. “Quantum security technologies”. In: (Mar. 24, 2020). url: https://www.ncsc.gov.uk/pdfs/whitepaper/quantum-security-technologies.pdf.

[Niu+19] Murphy Yuezhen Niu et al. “Universal quantum control through deep reinforcement learning”. In: *npj Quantum Information* 5.1 (Apr. 2019). doi: 10.1038/s41534-019-0141-3. url: https://doi.org/10.1038/s41534-019-0141-3.

[NPA07] Miguel Navascués, Stefano Pironio, and Antonio Acín. “Bounding the Set of Quantum Correlations”. In: *Physical Review Letters* 98.1 (Jan. 2007). doi: 10.1103/physrevlett.98.010401. url: https://doi.org/10.1103/physrevlett.98.010401.

[NSA21] National Security Agency (NSA). “Quantum Key Distribution (QKD) and Quantum Cryptography QC”. In: (2021). url: https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/.

[Pau+22] Hari P. Paudel et al. “Quantum Computing and Simulations for Energy Applications: Review and Perspective”. In: *ACS Engineering Au* 2.3 (Jan. 2022), pp. 151–196. doi: 10.1021/acsengineeringau.1c00033. url: https://doi.org/10.1021/acsengineeringau.1c00033.

[Pel+21] Emanuele Pelucchi et al. “The potential and global outlook of integrated photonics for quantum technologies”. In: *Nature Reviews Physics* 4.3 (Dec. 2021), pp. 194–208. doi: 10.1038/s42254-021-00398-z. url: https://doi.org/10.1038/s42254-021-00398-z.

[Pir+09] Stefano Pironio et al. “Device-independent quantum key distribution secure against collective attacks”. In: *New Journal of Physics* 11.4 (Apr. 2009), p. 045021. doi: 10.1088/1367-2630/11/4/045021. url: https://doi.org/10.1088/1367-2630/11/4/045021.

[PNA10] S. Pironio, M. Navascués, and A. Acín. “Convergent Relaxations of Polynomial Optimization Problems with Noncommuting Variables”. In: *SIAM Journal on Optimization* 20.5 (2010), pp. 2157–2180. doi: 10.1137/090760155. eprint: https://doi.org/10.1137/090760155. url: https://doi.org/10.1137/090760155.

[PR92] Sandu Popescu and Daniel Rohrlich. “Which states violate Bell’s inequality maximally?” In: *Physics Letters A* 169.6 (1992), pp. 411–414. issn: 0375-9601. doi: https://doi.org/10.1016/0375-9601(92)90819-8. url: https://www.sciencedirect.com/science/article/pii/0375960192908198.

[Pre18] John Preskill. “Quantum Computing in the NISQ era and beyond”. In: *Quantum* 2 (Aug. 2018), p. 79. doi: 10.22331/q-2018-08-06-79. url: https://doi.org/10.22331/q-2018-08-06-79.

[Pri+23] Ignatius W. Primaatmaja et al. “Security of device-independent quantum key distribution protocols: a review”. In: *Quantum* 7 (Mar. 2023), p. 932. doi: 10.22331/q-2023-03-02-932. url: https://doi.org/10.22331/q-2023-03-02-932.

[PS18] Anton Pljonkin and Pradeep Kumar Singh. “The Review of the Commercial Quantum Key Distribution System”. In: *2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC)*. IEEE, Dec. 2018. doi: 10.1109/pdgc.2018.8745822. url: https://doi.org/10.1109/pdgc.2018.8745822.

[RGK05] Renato Renner, Nicolas Gisin, and Barbara Kraus. “Information-theoretic security proof for quantum-key-distribution protocols”. In: *Physical Review A* 72.1 (July 2005). doi: 10.1103/physreva.72.012332. url: https://doi.org/10.1103/physreva.72.012332.

[Rie+22] Roman Rietsche et al. “Quantum computing”. In: *Electronic Markets* 32.4 (Aug. 2022), pp. 2525–2536. doi: 10.1007/s12525-022-00570-y. url: https://doi.org/10.1007/s12525-022-00570-y.

[RKB18] Marc Olivier Renou, J ędrzej Kaniewski, and Nicolas Brunner. “Self-Testing Entangled Measurements in Quantum Networks”. In: *Phys. Rev. Lett.* 121 (25 Dec. 2018), p. 250507. doi: 10.1103/PhysRevLett.121.250507. url: https://link.aps.org/doi/10.1103/PhysRevLett.121.250507.

[RMB21] Denis Rosset, Felipe Montealegre-Mora, and Jean-Daniel Bancal. “RepLAB: A Computational/Numerical Approach to Representation Theory”. In: *Quantum Theory and Symmetries*. Springer International Publishing, 2021, pp. 643–653. doi: 10.1007/978-3-030-55777-5_60. url: https://doi.org/10.1007/978-3-030-55777-5_60.

[Ros+17] Wenjamin Rosenfeld et al. “Event-Ready Bell Test Using Entangled Atoms Simultaneously Closing Detection and Locality Loopholes”. In: *Physical Review Letters* 119.1 (July 2017). doi: 10.1103/physrevlett.119.010402. url: https://doi.org/10.1103/physrevlett.119.010402.

[RS07] Joseph M. Renes and Graeme Smith. “Noisy Processing and Distillation of Private Quantum States”. In: *Physical Review Letters* 98.2 (Jan. 2007). doi: 10.1103/physrevlett.98.020502. url: https://doi.org/10.1103/physrevlett.98.020502.

[RUV13] Ben W. Reichardt, Falk Unger, and Umesh Vazirani. “Classical command of quantum systems”. In: *Nature* 496.7446 (Apr. 2013), pp. 456–460. doi: 10.1038/nature12035. url: https://doi.org/10.1038/nature12035.

[SB18] Richard S Sutton and Andrew G Barto. *Reinforcement Learning*. 2nd ed. Adaptive Computation and Machine Learning series. Cambridge, MA: Bradford Books, Nov. 2018.

[ŠB20] Ivan Šupić and Joseph Bowles. "Self-testing of quantum systems: a review". In: *Quantum* 4 (Sept. 2020), p. 337. doi: 10.22331/q-2020-09-30-337. url: https://doi.org/10.22331/q-2020-09-30-337.

[SC23] Paul Skrzypczyk and Daniel Cavalcanti. *Semidefinite Programming in Quantum Information Science*. IOP ebooks. London, England: Institute of Physics Publishing, Mar. 2023.

[Sca+09] Valerio Scarani et al. "The security of practical quantum key distribution". In: *Reviews of Modern Physics* 81.3 (Sept. 2009), pp. 1301–1350. doi: 10.1103/revmodphys.81.1301. url: https://doi.org/10.1103/revmodphys.81.1301.

[Sca19] Valerio Scarani. *Bell Nonlocality*. Oxford University Press, Aug. 2019. doi: 10.1093/oso/9780198788416.001.0001. url: https://doi.org/10.1093/oso/9780198788416.001.0001.

[Sch+17] John Schulman et al. "Proximal Policy Optimization Algorithms". In: *CoRR* abs/1707.06347 (2017). arXiv: 1707.06347. url: http://arxiv.org/abs/1707.06347.

[Sch+21] René Schwonnek et al. "Device-independent quantum key distribution with random key basis". In: *Nature Communications* 12.1 (May 2021). doi: 10.1038/s41467-021-23147-3. url: https://doi.org/10.1038/s41467-021-23147-3.

[Sch35] E. Schrödinger. "Discussion of Probability Relations between Separated Systems". In: *Mathematical Proceedings of the Cambridge Philosophical Society* 31.4 (1935), pp. 555–563. doi: 10.1017/S0305004100013554.

[Sek+18] Pavel Sekatski et al. "Certifying the Building Blocks of Quantum Computers from Bell's Theorem". In: *Physical Review Letters* 121.18 (Nov. 2018). doi: 10.1103/PhysRevLett.121.180505. url: https://doi.org/10.1103/PhysRevLett.121.180505.

[Sek+21] Pavel Sekatski et al. "Device-independent quantum key distribution from generalized CHSH inequalities". In: *Quantum* 5 (Apr. 2021), p. 444. doi: 10.22331/q-2021-04-26-444. url: https://doi.org/10.22331/q-2021-04-26-444.

[Sha+15] Lynden K. Shalm et al. "Strong Loophole-Free Test of Local Realism". In: *Physical Review Letters* 115.25 (Dec. 2015). doi: 10.1103/physrevlett.115.250402. url: https://doi.org/10.1103/physrevlett.115.250402.

[Sho94] P.W. Shor. “Algorithms for quantum computation: discrete logarithms and factoring”. In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. IEEE Comput. Soc. Press, 1994. doi: 10.1109/sfcs.1994.365700. url: https://doi.org/10.1109/sfcs.1994.365700.

[Sil+17] David Silver et al. “Mastering the game of Go without human knowledge”. In: *Nature* 550.7676 (Oct. 2017), pp. 354–359. doi: 10.1038/nature24270. url: https://doi.org/10.1038/nature24270.

[SP00] Peter W. Shor and John Preskill. “Simple Proof of Security of the BB84 Quantum Key Distribution Protocol”. In: *Physical Review Letters* 85.2 (July 2000), pp. 441–444. doi: 10.1103/physrevlett.85.441. url: https://doi.org/10.1103/physrevlett.85.441.

[SW87] Stephen J. Summers and Reinhard Werner. “Maximal violation of Bell’s inequalities is generic in quantum field theory”. In: *Communications in Mathematical Physics* 110.2 (June 1987), pp. 247–259. doi: 10.1007/bf01207366. url: https://doi.org/10.1007/bf01207366.

[Swe+20] Ryan Sweke et al. “Reinforcement learning decoders for fault-tolerant quantum computation”. In: *Machine Learning: Science and Technology* 2.2 (Dec. 2020), p. 025005. doi: 10.1088/2632-2153/abc609. url: https://doi.org/10.1088/2632-2153/abc609.

[Tan+17] T. R. Tan et al. “Chained Bell Inequality Experiment with High-Efficiency Measurements”. In: *Physical Review Letters* 118.13 (Mar. 2017). doi: 10.1103/physrevlett.118.130403. url: https://doi.org/10.1103/physrevlett.118.130403.

[Tan+22] Ernest Y.-Z. Tan et al. “Improved DIQKD protocols with finite-size analysis”. In: *Quantum* 6 (Dec. 2022), p. 880. doi: 10.22331/q-2022-12-22-880. url: https://doi.org/10.22331/q-2022-12-22-880.

[Tan21] Ernest Y. -Z. Tan. *Prospects for device-independent quantum key distribution*. 2021. doi: 10.48550/ARXIV.2111.11769. url: https://arxiv.org/abs/2111.11769.

[The+18] Oliver Thearle et al. “Violation of Bell’s Inequality Using Continuous Variable Measurements”. In: *Physical Review Letters* 120.4 (Jan. 2018). doi: 10.1103/physrevlett.120.040406. url: https://doi.org/10.1103/physrevlett.120.040406.

[Tsi80] Boris S. Tsirelson. “Quantum generalizations of Bell’s inequality”. In: *Letters in Mathematical Physics* 4.2 (Mar. 1980), pp. 93–100. doi: 10.1007/bf00417500. url: https://doi.org/10.1007/bf00417500.

[Tsi93] Boris S Tsirelson. “Some results and problems on quantum Bell-type inequalities”. In: *Hadronic Journal Supplement* 8.4 (1993), pp. 329–345.

[Val+20] Xavier Valcarce et al. “What is the minimum CHSH score certifying that a state resembles the singlet?” In: *Quantum* 4 (Mar. 2020), p. 246. doi: 10.22331/q-2020-03-23-246. url: https://doi.org/10.22331/q-2020-03-23-246.

[Val+22] Xavier Valcarce et al. “Self-testing two-qubit maximally entangled states from generalized Clauser-Horne-Shimony-Holt tests”. In: *Physical Review Research* 4.1 (Jan. 2022). doi: 10.1103/physrevresearch.4.013049. url: https://doi.org/10.1103/physrevresearch.4.013049.

[Val+23] Xavier Valcarce et al. “Automated design of quantum-optical experiments for device-independent quantum key distribution”. In: *Phys. Rev. A* 107 (June 2023), p. 062607. doi: 10.1103/PhysRevA.107.062607. url: https://link.aps.org/doi/10.1103/PhysRevA.107.062607.

[Val21] Xavier Valcarce. *QuantumOpticalCircuits.jl*. https://github.com/xvalcarce/QuantumOpticalCircuits.jl. 2021.

[Vin+19] Oriol Vinyals et al. “Grandmaster level in StarCraft II using multi-agent reinforcement learning”. In: *Nature* 575.7782 (Oct. 2019), pp. 350–354. doi: 10.1038/s41586-019-1724-z. url: https://doi.org/10.1038/s41586-019-1724-z.

[Viv+15] V. Caprara Vivoli et al. “Challenging preconceptions about Bell tests with photon pairs”. In: *Physical Review A* 91.1 (Jan. 2015). doi: 10.1103/physreva.91.012107. url: https://doi.org/10.1103/physreva.91.012107.

[VV14] Umesh Vazirani and Thomas Vidick. “Fully Device-Independent Quantum Key Distribution”. In: *Physical Review Letters* 113.14 (Sept. 2014). doi: 10.1103/physrevlett.113.140501. url: https://doi.org/10.1103/physrevlett.113.140501.

[WAP21] Erik Woodhead, Antonio Acín, and Stefano Pironio. “Device-independent quantum key distribution with asymmetric CHSH inequalities”. In: *Quantum* 5 (Apr. 2021), p. 443. doi: 10.22331/q-2021-04-26-443. url: https://doi.org/10.22331/q-2021-04-26-443.

[Wei+11] Henning Weier et al. “Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors”. In: *New Journal of Physics* 13.7 (July 2011), p. 073024. doi: 10.1088/1367-2630/13/7/073024. url: https://doi.org/10.1088/1367-2630/13/7/073024.

[Wei+98] Gregor Weihs et al. “Violation of Bell’s Inequality under Strict Einstein Locality Conditions”. In: *Physical Review Letters* 81.23 (Dec. 1998), pp. 5039–5043. doi: 10.1103/physrevlett.81.5039. url: https://doi.org/10.1103/physrevlett.81.5039.

[Wie83] Stephen Wiesner. “Conjugate coding”. In: *ACM SIGACT News* 15.1 (Jan. 1983), pp. 78–88. doi: 10.1145/1008908.1008920. url: https://doi.org/10.1145/1008908.1008920.

[Xu+20] Feihu Xu et al. “Secure quantum key distribution with realistic devices”. In: *Reviews of Modern Physics* 92.2 (May 2020). doi: 10.1103/revmodphys.92.025002. url: https://doi.org/10.1103/revmodphys.92.025002.

[Xu+22] Feihu Xu et al. “Device-Independent Quantum Key Distribution with Random Postselection”. In: *Physical Review Letters* 128.11 (Mar. 2022). doi: 10.1103/physrevlett.128.110506. url: https://doi.org/10.1103/physrevlett.128.110506.

[Yan+14] Tzyh Haur Yang et al. “Robust and Versatile Black-Box Certification of Quantum Devices”. In: *Phys. Rev. Lett.* 113 (4 July 2014), p. 040401. doi: 10.1103/PhysRevLett.113.040401. url: https://link.aps.org/doi/10.1103/PhysRevLett.113.040401.

[YN13] Tzyh Haur Yang and Miguel Navascués. “Robust self-testing of unknown quantum systems into any entangled two-qubit states”. In: *Phys. Rev. A* 87 (5 May 2013), p. 050102. doi: 10.1103/PhysRevA.87.050102. url: https://link.aps.org/doi/10.1103/PhysRevA.87.050102.

[Zap+23] Víctor Zapatero et al. “Advances in device-independent quantum key distribution”. In: *npj Quantum Information* 9.1 (Feb. 2023). doi: 10.1038/s41534-023-00684-x. url: https://doi.org/10.1038/s41534-023-00684-x.

[Zha+22] Wei Zhang et al. “A device-independent quantum key distribution system for distant users”. In: *Nature* 607.7920 (July 2022), pp. 687–691. doi: 10.1038/s41586-022-04891-y. url: https://doi.org/10.1038/s41586-022-04891-y.