Quantum cryptographic primitives in realistic conditions

Anna Pappa

ParisTech
INSTITUT DES SCIENCES ET TECHNOLOGIES
PARIS INSTITUTE OF TECHNOLOGY

TELECOM ParisTech

2014-ENST-0045

EDITE - ED 130

Doctorat ParisTech

T H È S E

pour obtenir le grade de docteur délivré par

TELECOM ParisTech

Spécialité « Informatique et Réseaux »

présentée et soutenue publiquement par

Anna PAPPA

le 10 juillet 2014

Primitives Cryptographiques Quantiques dans des Conditions Réalistes

Directeurs de thèse : **Eleni DIAMANTI**
Iordanis KERENIDIS

Jury

M. Antonio ACIN, Professeur, ICREA, The Institut of Photonic Studies, Barcelona	Rapporteur
M. Serge MASSAR, Chargé de cours, Directeur LIQ, Université Libre de Bruxelles	Rapporteur
M. Norbert LUTKENHAUS, Professeur, IQC, University of Waterloo	Examinateur
M. Simone SEVERINI, Royal Society Research Fellow, University of London	Examinateur
M. Jean-Pierre TILLICH, Directeur de recherche, INRIA Paris, Rocquencourt	Examinateur
Mme Eleni DIAMANTI, Chargée de recherche, CNRS LTCI, Télécom ParisTech	Directrice de thése
M. Iordanis KERENIDIS, Directeur de recherche, CNRS LIAFA, Paris Diderot	Directeur de thése

TELECOM ParisTech
école de l'Institut Télécom - membre de ParisTech

T H È S E

Abstract

Quantum Computing has attracted great attention in the last decades, due to its tremendous potential for faster and more secure communications. This thesis focuses on quantum communication protocols between two or more parties, and their implementability in a realistic environment. The aim is to provide a level of security for cryptographic and game-theoretic tasks that classical computation cannot achieve. The first task that this thesis is concerned with, is coin flipping, a cryptographic primitive where two players that are separated by distance, want to agree on a common bit. We propose a new quantum coin flipping protocol, analyse its security in the presence of standard imperfections and implement it using a commercial plug&play system. We report a quantum advantage for 15 km, a distance which is larger by three orders of magnitude with respect to previous implementations of quantum coin flipping.

The second task that this thesis addresses, is entanglement verification in a distrustful setting. We propose and analyse a verification protocol for a source that is supposed to create multiparty entangled states and share them with honest and dishonest parties. By increasing the number of measurement setting of the parties, the protocol is able to tolerate high amounts of losses and errors. An experimental verification procedure is also described, and preliminary results of an optical implementation of the protocol are reported.

Furthermore, the thesis investigates the connection between game theory and quantum non-locality, in the context of conflicting-interest Bayesian games. We examine how shared entanglement can provide an advantage to the players of this type of games, by helping them win a game with higher probability than any classical resources could achieve. The different strategies of the players are also examined in the context of Nash Equilibria, in order to find the strategies for which the players do not have an incentive to diverge from. Finally, we implement a two-player conflicting-interest Bayesian game using an entangled source, and experimentally verify the quantum advantage of our game.

Resumé

L'Informatique Quantique a attiré une grande attention ces dernières années, en raison de son énorme potentiel pour des communications plus rapides et plus sûres. Cette thèse porte sur les protocoles de communication quantiques entre plusieurs parties, ainsi que leur application dans un cadre réaliste. L'objectif est de fournir un niveau de sécurité pour les tâches de chiffrement et certains jeux bipartites, qui ne peut pas être atteint avec des primitives classiques. La première tâche que cette thèse étudie est le tirage à pile ou face, une primitive cryptographique pour laquelle deux joueurs qui sont séparés par une grande distance, veulent se mettre d'accord sur un bit commun. Nous proposons un nouveau protocole de tirage à pile ou face quantique, nous analysons sa sécurité en présence de toutes les imperfections connues et nous le mettons en œuvre à l'aide d'un système commercial appelé "plug&play". Nous démontrons un avantage quantique pour 15 km, une distance qui est plus grande par trois ordres de grandeur des précédentes implémentations de tirage pile ou face quantique.

La deuxième tâche étudiée dans cette thèse, est la vérification d'intrication dans un cadre malhonnête. Nous proposons et analysons un protocole de vérification pour une source qui est censée créer des états intriqués multipartites et les partager avec des parties honnêtes et malhonnêtes. En augmentant le nombre de mesures différentes des parties, le protocole est capable de tolérer des pertes et des taux d'erreurs importants. Une procédure de vérification expérimentale est également décrite, et les résultats préliminaires d'une mise en œuvre optique sont présentés et analysés.

Finalement, cette thèse étudie le lien entre la théorie des jeux et la non-localité quantique, dans le contexte des jeux Bayésiens avec conflit d'intérêt. Nous examinons comment l'intrication partagée peut fournir un avantage pour les joueurs de ce genre de jeux, en les aidant à gagner un match avec une probabilité plus élevée que la probabilité maximale accessible avec des ressources classiques. Les différentes stratégies des acteurs sont également examinées dans le cadre des Equilibres de Nash, afin de trouver des stratégies pour que les joueurs n'aient pas une incitation à s'écarter. Enfin, nous mettons en place un jeu Bayésien pour deux joueurs avec conflits d'intérêts, en utilisant une source intriquée, et nous vérifions expérimentalement l'avantage quantique de notre jeu.

Acknowledgements

First and foremost, I want to thank my two supervisors, Eleni Diamanti and Iordanis Kerenidis for their continuous support and patience during this thesis. I cannot imagine a friendlier environment and a better supervision for my doctoral studies than the one that they provided. Their scientific excellence and commitment to their work will always be an inspiration to me.

One of the many positive things about doing a joint PhD between Télécom ParisTech and Paris Diderot, is that I met a lot of amazing people and I want to thank them all for their company and friendship during numerous lunches, conferences, karaoke nights and Sunday barbeques. Sophie Laplante deserves a special thank you for securing the scholarship that funded my doctoral studies.

I was also very lucky to have worked with a lot of inspiring researchers during these years, and more especially with Bryn Bell, Paul Jouguet, Tom Lawson, Damian Markham, Anne Marin, Will McCutcheon, Marc Tame, Marc Kaplan and Stephanie Wehner. Special thanks goes to Zizhu Whang for having a solution to every problem and André Chailloux for always being available to chat or work and for always surprising me with his knowledge and skills.

A big part of this thesis would not have been possible without the collaboration with IdQuantique, and especially with Patrick Trinkler and Matthieu Legré, whose support and hospitality during my visits to Geneva are greatly appreciated.

I want to thank Louis Salvail for hosting me for two amazing months at the University of Montreal and for sharing his research ideas with me, as well as Benno, Dave and the rest of the group for making me feel at home. I also want to thank Serge Massar and Antonio Acín for taking the time to review this thesis as well as Norbert Lütkenhaus, Simone Severini and Jean-Pierre Tillich for being in my jury.

Cheerful chats with my sister Elpi and my friends, especially Asli, Nikoleta, Efi and Vaggelis during this whole time, kept me sane and I am forever grateful to them. Last, I want to thank my parents for believing in me and supporting me all these years and for all their hard work that provided me with the happiest childhood and the best education that I could have.

Contents

List of Figures

List of Tables

Résumé en français

Pendant les dernières années, il est devenu évident que les outils fournis par la mécanique quantique peuvent être utilisés dans de nombreux domaines, tels que la cryptographie, les algorithmes et la théorie de la complexité, la théorie des jeux et même la biologie. Dès le début du 20e siècle, Einstein, Podolski et Rosen [1] ont compris la puissance de la mécanique quantique, et ils ont presenté les principes sur lesquels devait reposer la cryptographie quantique. Ce qui semblait très paradoxal et difficile à accepter est le fait que la nature est intrinsèquement probabiliste, même lorsqu' on prend en compte tous les paramètres locales cachés. En 1964, John Bell [2] a prouvé que cet effet paradoxal est une caractéristique intrinsèque de la nature qu'on nomme "non-localité".

Presque vingt ans après le théorème de Bell, les premières implémentations expérimentales de "l'action fantôme à distance" de Einstein-Podolski-Rosen (EPR) ont eu lieu, le plus célèbre étant celui de Aspect et al en 1982 [3]. Cependant, malgré le grand progrès scientifique en ce qui concerne les implémentations quantiques, une vérification expérimentale du théorème de Bell qui ferme toutes les "loopholes" (c'est à dire les problèmes qui risquent de rendre les conclusions expérimentales invalides) n'a pas encore été atteinte.

En même temps, les théoriciens essayaient d'utiliser ce caractère aléatoire inhérent de la mécanique quantique dans plusieurs sous-champs de l'informatique et de la théorie de communication. En 1984, Charles Bennet et Gilles Brassard, inspirés par le travail de Stephen Wiesner [4], ont proposé le premier schéma de distribution quantique de clés [5]. Dix ans plus tard, Peter Shor va inventer un des résultats les plus célèbres de l'informatique quantique [6], un algorithme qui résout le problème de factorisation[1], en temps polynomial, beaucoup plus rapide que le meilleur algorithme classique qui fonctionne en temps sous-exponentiel. Puisque les schémas cryptographiques à clé publique les plus utilisés, comme RSA, sont basées sur la difficulté de factorisation des grands nombres avec un ordinateur classique, l'utilisation d'un ordinateur quantique pourrait conduire à des failles de sécurité importantes.

Malgré le progrès considérable des dernières années, à la fois théorique et expérimentale, il semble que nous sommes encore loin de la construction d'un ordinateur quantique universel qui pourrait remplacer les ordinateurs classiques dans la quotidienne. Un scénario plus plausible est d'un réseau hybride des parties quantiques et classiques, où les agents individuels peuvent communiquer des façons differents avec les parties fiables et non fiables, et déléguer des tâches de calcul aux serveurs puissants quantiques non fiables. Dans tous les réseaux de télécommunication, la securité des calculs et de la communication entre des agents est une condition prérequise, ce qui rend certains primitives cryptographiques essentielles.

[1] écrire un entier naturel N non nul sous forme d'un produit de nombres premiers.

Une autre propriété autant important d'un tel réseau hybride est la possibilité de vérifier que les agents et les serveurs non fiables du réseau exécutent les processus quantiques comme ils doivent, ce qui est intimement liée à la possibilité d'observer des effets non locaux et de tester la mécanique quantique. Dans ce contexte, beaucoup de recherche a été concentrée sur les notions liées de "self-testing", "device-independence" et vérification de calcul.

Finalement, lors de la conception d'un protocole quantique, il est également important de ne pas oublier que sa mise en œuvre expérimentale peut se avérer difficile à cause de particularités de la mécanique quantique. Il y a des protocoles nombreux qui sont en théorie sécures, mais qui ne peuvent pas être implementés, parce qu'ils ne peuvent pas tolerer des pertes ou de bruit. Il est donc nécessaire de considérer des attaquants qui peuvent manipuler les pertes et les erreurs du systeme à leur avantage, et adapter l'analyse de la sécurité des protocoles.

L'objectif de cette thèse est de concevoir et d'analyser de nouveaux protocoles de plusieurs parties, qui peuvent former la base pour d'autres protocoles plus compliqués, et en plus d'étudier leur applicabilité. Dans les paragraphes suivants, nous discutons le progrès théorique et expérimentale qui a été atteint au cours de cette thèse.

Tirage à pile ou face

Les protocoles des deux parties sont à la base de tout système de calcul distribué, classique et quantique. Il existe deux modèles de calcul des deux parties, le *coopérative* et le *non coopératif*. Dans le modèle coopératif, les parties se font mutuellement confiance, et ils travaillent ensemble vers un but commun. En même temps, ils essaient d'atteindre un niveau de sécurité satisfaisant contre un attaquant externe qui peut écouter leur communication. Un exemple d'un protocole quantique de deux partis est la distribution des clés, où les parties veulent partager une clé commune, qui doit rester secret. Depuis les premiers resultats sur la distribution de clé quantique (QKD) [5], de nombreux protocoles ont été proposés et mises en œuvre, qui permettent d'atteindre un ordre de génération de clé assez élevé pour des distances allant jusqu'à quelques centaines de kilomètres [7, 8].

En revanche, le modèle non coopératif a été moins étudié, en théorie et en pratique. Dans ce modèle, l'une des deux parties est malhonnête et essaie de tricher. Des exemples importants de protocoles de deux parties sont l'engagement de bits ("bit commitment"), le tirage à pile ou face ("coin flipping") et le transfert inconscient ("oblivious transfer"). Dans cette thèse, nous nous concentrerons sur *tirage à pile ou face*, où deux parties veulent obtenir un bit aléatoire commune, alors qu'ils sont loin l' un de l' autre. Ici, le but de la partie malhonnête est de choisir et tirer un bit spécifique plutôt qu'au hasard, ou comme on dit, il/elle veut *biaiser* la valeur du tirage à pile ou face.

Le tirage à pile ou face est largement utilisé dans les réseaux de communication. Par exemple, il est utilisé pour les jeux en ligne et pour les protocoles de consensus randomisés [9]. Malheureusement, le tirage à pile ou face parfait contre des adversaires non bornés est impossible à la fois classiquement et quantiquement [10, 11]. Cela signifie que lorsque l'une des parties est malhonnête, il/elle peut biaiser le résultat de la coin flip de sorte que ce n'est plus parfaitement aléatoire. Néanmoins, contrairement au cas classique, l'utilisation d'états quantiques permet d'atteindre un certain niveau de sécurité, ce qui signifie qu'il est possible de limiter la probabilité de biais de la partie malhonnête. Ils existent plusieurs protocoles théoriques quantiques qui fournissent une limite sur la probabilité de biais, mais il n'y a pas beaucoup entre eux qui ont été mis en œuvre; quelques exceptions atteignent une distance de communication limitée à quelques mètres.

L'objectif est de fournir un cadre théorique et expérimentale complète pour la mise en œuvre de tirage à pile ou face quantique dans les scénarios de communication pratiques. Le protocole que nous considérons prend en compte des imperfections expérimentales standards (émission multi-photon, perte de transmission, inefficacité des détecteurs). Nous montrons que notre protocole peut être combiné avec des protocoles qui permettent d'atteindre une sécurité presque parfaite, c'est à dire, un biais asymptotiquement proche de zéro, contre des adversaires avec des ressources limitées. Plus explicitement, si l'adversaire est bornée, le protocole garantit une sécurité presque parfaite, tandis que dans le cas d'un adversaire tout-puissant, le protocole garantit toujours un niveau de sécurité plus élevé que possible avec des moyens strictement classiques. Assurer la sécurité contre des adversaires de complexité variable est de grande importance dans le contexte des réseaux de communication actuels, où les capacités technologiques et informatiques évoluent très rapidement. En outre, nous mettons en œuvre le protocole en utilisant un système pratique "plug & play", qu'on a amélioré de manière significative [12, 13]. L'élément le plus important de notre mise en œuvre, c' est que nous prenons une approche réaliste: pour tenir compte des erreurs inévitables dans le système, on permet une probabilité d'abandon non nulle mais petite, dans le cas où les deux parties sont honnêtes, et on accepte la dépendance de la probabilité de fraude par le montant de perte de communication, se écartant alors de la notion de tolérance de perte absolue. Ceci constitue un changement important par rapport aux protocoles précédents [14, 15] et nous donne un gain de trois ordres de grandeur sur la distance de communication. En effet, en utilisant une analyse de sécurité relative à notre mise en œuvre aussi qu' une référence appropriée pour les protocoles de tirage á pile ou face classiques [16], on peut rigoureusement quantifier l'avantage offert par la communication quantique en fonction de la distance. De cette façon, on démontre un avantage évident pour le tirage à pile ou face quantique contre des attaquers non-bornés, sur des distances de communication appropriés pour les réseaux métropolitaines, avec un système facile à déployer.

Le protocole est un raffinement de celle proposée par Berlin et al [14]; la différence principale est que Alice envoie un nombre fixe d'impulsions K, et utilise une source de laser atténué. En limitant le nombre d'impulsions et en considerant une probabilité d'abandon honnête, le protocole peut atteindre une probabilité de fraude très proche de celle constatée par Berlin et al, et dans le même temps être plus approprié pour une utilisation pratique.

Le nombre des photons dans chaque impulsion produit par la source suit la distribution de Poisson; pour un nombre moyen de photons μ, la probabilité que le nombre de photons est i, est $p_i = \frac{e^{-\mu}\mu^i}{i!}$.

Protocole de tirage à pile ou face

1. Pour $i = 1, ..., K$:
   (a) Alice choisit uniformément au hasard une base $\alpha_i \in \{0,1\}$ et un bit $c_i \in \{0,1\}$.
   (b) Elle prépare l'état $|\Phi_{\alpha_i,c_i}\rangle$, tel que:

$$\begin{aligned} |\Phi_{\alpha_i,0}\rangle &= \sqrt{y}|0\rangle + (-1)^{\alpha_i}\sqrt{1-y}|1\rangle \\ |\Phi_{\alpha_i,1}\rangle &= \sqrt{1-y}|0\rangle - (-1)^{\alpha_i}\sqrt{y}|1\rangle \end{aligned}$$

   et elle l'envoie à Bob.
2. Bob choisit uniformément au hasard β_i et il mesure l'état dans la base $\{|\Phi_{\beta_i,0}\rangle, |\Phi_{\beta_i,1}\rangle\}$. Si ses détecteurs ne cliquent pas du tout, il avorte. Sinon, j est la première impulsion qu'il détecte.
3. Alice révèle α_j, c_j.
4. Si $\alpha_j = \beta_j$, Bob vérifie que le résultat de sa mesure est en effet c_j, sinon il avorte.
5. Si Bob n'avorte pas, le résultat du protocole est $x = c_j \oplus b$.

On démontre l'implementation de notre protocole de tirage à pile ou face quantique en utilisant un système plug & play, qui est une version améliorée du système de distribution de clé quantique Clavis2 de idQuantique [12]. Un système plug & play est un type de interféromètre de Mach-Zehnder, qui ne nécessite pas de stabilisation continue

et d'ajustement de polarisation, et fournit donc une solution de communication plus stable. Le dispositif expérimental (voir Figure 1) contient une approche à deux voies. La source laser à la configuration de Bob émet des impulsions de photons à 1550 nm, qui sont séparées à une 50/50 séparateur de faisceau (beamsplitter), puis recombinées à un diviseur de faisceau de polarisation (polarised beamsplitter), après avoir parcouru un bras court et un bras long. Ce dernier contient un modulateur de phase (non actif à ce stade) et un élément optique qui transforme les états horizontalement polarisés aux états de polarisation verticale et vice versa. En raison de ces deux chemins différents, nous avons maintenant deux impulsions qui voyagent aux temps différents, d'abord une impulsion de " référence" venant du chemin court et de polarisation verticale, puis une impulsion de " signal" , venant du chemin long et de polarisation horizontale.

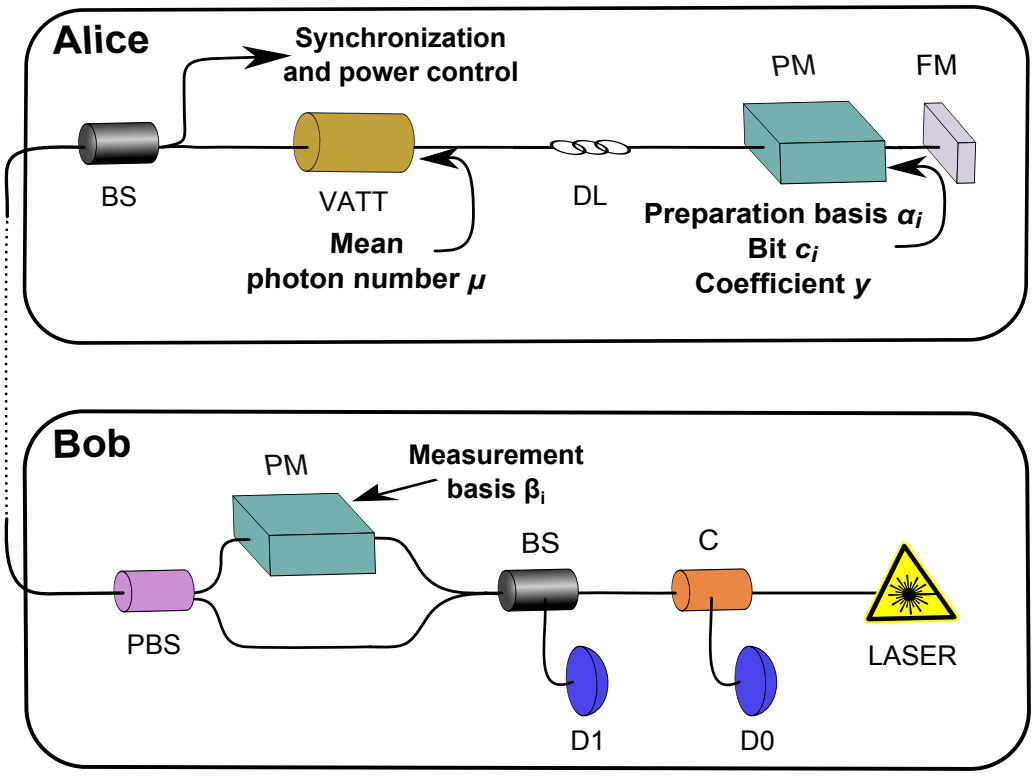


Figure 1: Dispositif experimental du système plug & play

Les impulsions se propagent vers Alice à travers le canal de communication et se reflètent sur un miroir de Faraday, en changeant leurs polarisations. Ensuite, Alice choisit les valeurs de sa base et de son bit, en appliquant un décalage de phase appropriée

avec son modulateur de phase sur la deuxième impulsion (l' impulsion de “signal” qui a maintenant une polarisation vertical). En même temps, elle choisit le coefficient de l'état y. Alice utilise aussi son atténuateur variable (voir Figure 1) pour appliquer l'atténuation nécessaire pour obtenir un nombre spécifique de photons par impulsion moyenne μ.

Ensuite, les deux impulsions se propagent vers Bob, en passant à travers le PBS, par conséquent, l'impulsion de “référence” avec une polarisation horizontale (H) se reflète vers le bras long et l'impulsion de “signal” avec une polarisation verticale (V) se transmet vers la bras court. L'impulsion de “référence” traverse l'élément optique qui lui donne une polarisation V et le modulateur de phase permet Bob à choisir une base de mesure en appliquant la phase appropriée. Grâce à la construction du système plug&play, les impulsions arrivent simultanément au diviseur de faisceau, où ils interfèrent et sont détectées par les détecteurs. A la fin du protocole, nous dérivons un ensemble de données contenant les bases de préparation et des bits d' Alice et les bases de mesure et les résultats de Bob.

Nous avons effectué des expériences de tirage à pile ou face quantique en utilisant des fibres de 15 et 25 km, avec plusieurs valeurs de nombre moyen de photons μ pour chaque longueur de canal. On a calculé le nombre de cycles de protocole K qui sont nécessaires pour atteindre une probabilité d'abandon honnête H specifique. Le nombre des détections utilisé pour calculer les cycles nécessaires K est suffisamment grande (typiquement 10^6) afin d'assurer des effets de taille finie négligeables dans nos expériences. Pour les paramètres spécifiques du système, les valeurs de μ, K et y qui minimisent la probabilité de fraude et qui rendent le protocole juste, peuvent ensuite être calculés.

La Figure 2 montre la probabilité de fraude calculée à partir de nos données expérimentales pour les 15 et 25 km, en fonction de la probabilité d'abandon honnête. Pour chaque valeur de la probabilité d'abandon honnête, le nombre de cycles K et le nombre moyen de photons par impulsion μ ont été optimisés. Les valeurs correspondent à un protocole juste, et l'incertitude dans l'estimation de μ est illustrée par les zones ombragées dans la figure. Pour quantifier l'avantage offert par la communication quantique, nous utilisons la borne de la probabilité de fraude classique P_c, défini dans [16] et représentée par une ligne continue dans la Figure 2. On peut voir que la probabilité de fraude est strictement inférieur à celle qui peut être obtenu classiquement pour 15 km, pour plusieurs valeurs pratiques de la probabilité d'abandon honnête (de 0.4% à 1.45%). La zone correspondant aux données obtenues à 25 km est juste au-dessus de la borne de fraude classique pour toutes les valeurs de probabilité d'abandon honnête, ce qui signifie que un avantage quantique ne peut être affirmé dans ce cas.

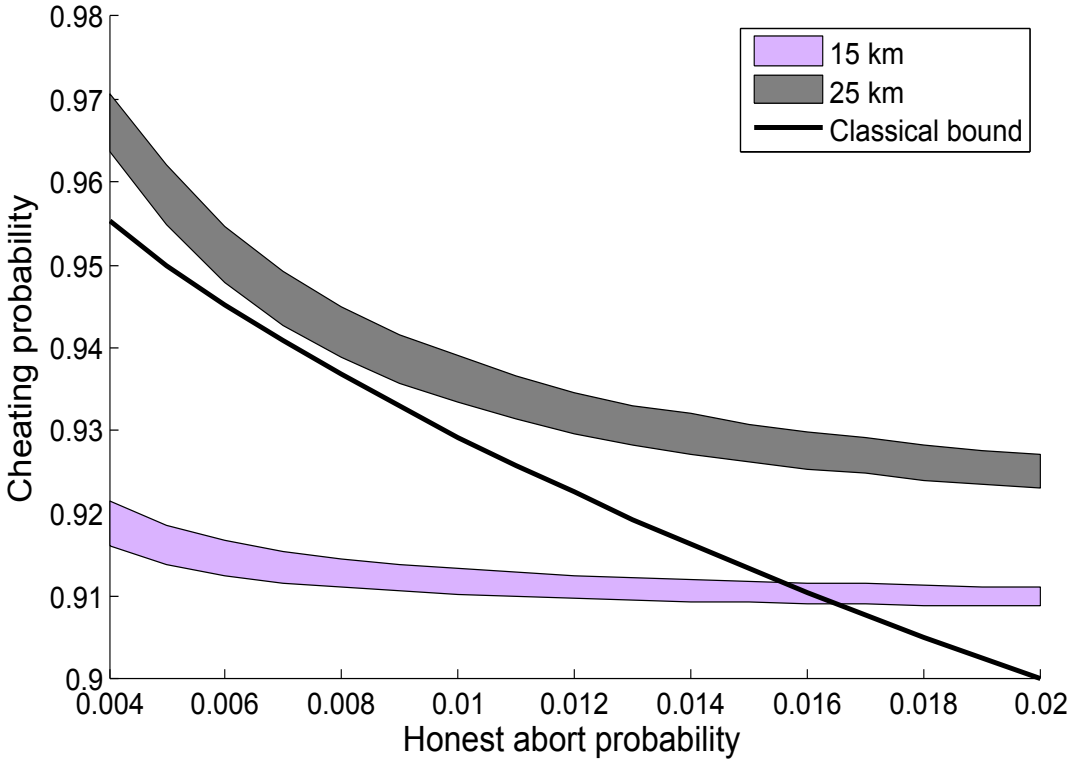


Figure 2: Probabilité de fraude vs probabilité d'abandon honnête pour 15 et 25 km

Verification d'intrication

Un des phénomènes les plus importants de la mécanique quantique est l'*intrication*. Les systèmes intriqués sont composés de deux ou plusieurs particules qui interagissent en telle manière que même s'ils sont séparés par une grande distance, ils présentent des corrélations qui sont impossibles à simuler avec un formalisme classique.

L'intrication joue un rôle important dans l'étude et le développement de la théorie de l'information quantique. Elle a été largement utilisé dans tous les aspects de l'information quantique et aussi pour montrer les avantages obtenus par rapport aux systèmes classiques. Initialement défini pour les états bipartites, la notion d'intrication a été généralisée aux systèmes multipartites et malgré la complexité de cette notion dans ce cas-là, de nombreuses propriétés intéressantes des états intriqués multipartites sont connus. Par exemple, les corrélations quantiques des états Greenberger-Horne-Zeilinger [17] aident à gagner un jeu spécifique avec une probabilité 1 dans le cadre quantique, alors que toute théorie locale classique donne une probabilité maximale de 3/4 [18].

En général, les états intriqués multipartites sont une ressource fondamentale pour les réseaux de communication quantiques. En effet, ils permettent aux agents des réseaux de créer de corrélations fortes afin d'effectuer des tâches réparties, de déléguer le calcul à des serveurs non-fiables [19], ou de calculer, par exemple dans le modèle de "Measurement-based Quantum Computation" [20]. Une question naturelle et fondamentale qui se pose alors est si les agents du réseau doivent faire confiance à la source qui leur fournit ces états intriqués multipartites, ou s'ils sont capables de vérifier l'intrication eux-mêmes.

Cette thèse rapporte la première étude de vérification d'intrication multipartite en présence des partis malhonnêtes, à la fois dans des conditions parfaites et en présence d'erreurs expérimentales réalistes. Compte tenu d'une source non fiable qui crée un état quantique multipartite et le partage avec les parties non fiables (qui peuvent éventuellement collaborer entre eux et avec la source), nous fournissons un test pour les parties honnêtes pour vérifier si l'état quantique partagé est un état specifique d'intrication maximale. Tout d'abord, on assume des conditions idéales (pas de pertes, pas d'erreurs) et on étudie un protocole qui est lié aux protocols de pseudo-télépathie [21]. On analyse sa sécurité dans deux cas: lorsque toutes les parties sont honnêtes, et quand certains d'entre eux sont malhonnêtes, et on présente un test pour que les partis honnêtes vérifient si l'état quantique qu'ils utilisent dans le calcul, est intriqué au maximum. La probabilité qu'un état quantique passe notre test est une fonction de sa distance de l'état correcte.

Nous commençons notre analyse en décrivant d'abord en détail notre modèle:

Source: La source n'est pas fiable. Elle doit créer l'état n-partite GHZ: $|G_0^n\rangle = \frac{1}{\sqrt{2}}\big(|0^n\rangle + |1^n\rangle\big)$ et la distribuer aux n parties. En réalité, elle est permis de partager n'importe quel état.

Parties: Les parties honnêtes ne savent pas quelles parties sont honnêtes et quelles sont malhonnêtes. Les parties malhonnêtes peuvent agir comme une seule unité, contrôlée par la source, et ils sont également considérés comme ayant de l'équipement parfait. Leur but est de convaincre les parties honnêtes qu'ils partagent un état GHZ, alors qu'en réalité ils partagent effectivement un état "ϵ-away" de GHZ.

Resources locales: Toutes les parties ont un dispositif de mesure des qubits fiable avec deux paramètres de mesure.

Ressources du réseau: Chaque paire de parties partage un canal classique privé, ce qui maintient la communication classique entre deux parties honnêtes secrets.

Le protocole de vérification Ici, nous présentons un protocole de vérification d'intrication, où une source partage un état $|\Psi\rangle$ avec n parties et veut convaincre le Vérificateur que l'état est en fait un état GHZ n-partite (jusqu'aux opérations locales sur les parties malhonnêtes).

Le protocole de vérification

1. Le Vérificateur choisit $\theta_j \in [0, \pi)$ pour chaque partie A_j, $j = 1, \ldots, n$, tels que:
$$\sum_j \theta_j = 0 \pmod{\pi} \tag{1}$$
et les envoie séquentiellement à toutes les parties.

2. Chaque partie A_j mesure dans la base:
$$\{|\theta_j^+\rangle, |\theta_j^-\rangle\} = \{\frac{|0\rangle + e^{i\theta_j}|1\rangle}{\sqrt{2}}, \frac{|0\rangle - e^{i\theta_j}|1\rangle}{\sqrt{2}}\}$$
et envoie le bit y_j au Vérificateur. $y_j = 0$ lorsque le résultat de mesure est le vecteur de base $|\theta_j^+\rangle$ et $y_j = 1$ lorsque le résultat de mesure est le vecteur de base $|\theta_j^-\rangle$.

3. Si toutes les parties ont envoyé leurs résultats de mesure et n'ont pas déclaré des pertes, le Vérifieur accepte l'état $|\Psi\rangle$ si le test T réussit:
$$T(|\Psi\rangle): \qquad \bigoplus_j y_j = \frac{1}{\pi}\sum_j \theta_j \pmod{2} \tag{2}$$

On désigne par $T(|\Psi\rangle)$ le résultat du test ci-dessus sur l'état $|\Psi\rangle$ (c'est égal à 1 si l'état passe le test et 0 s'il échoue). Ce n'est pas difficile de voir que le test passe toujours sur l'état $|G_0^n\rangle$ ($T(|G_0^n\rangle) = 1$).

Maintenant on va supposer que toutes les parties sont honnêtes et on va voir quelle est la probabilité que le test T accepte un état $|\Psi\rangle$ en fonction de la distance entre cet état et $|G_0^n\rangle$. En désignant par $D(|\psi\rangle, |\phi\rangle)$ la distance de trace entre deux états $|\psi\rangle$ et $|\phi\rangle$, on peut prouver le théorème suivant:

Theorem 1 (Cas Honnête)**.** *Si $|\Psi\rangle$ est l'état partagé entre n parties, et $D(|\Psi\rangle, |G_0^n\rangle) = \epsilon$, alors* $\Pr[T(|\Psi\rangle) = 1] \leq 1 - \frac{\epsilon^2}{2}$.

Proof. On a besoin de définir un test de vérification pour un état GHZ pivoté:

Etat: $|G_\Theta^n\rangle = \frac{1}{\sqrt{2}}\big(|0^n\rangle + e^{i\Theta}|1^n\rangle\big)$, où $\Theta \in [0, 2\pi)$

Promesse sur les entrées: $\sum_{j=1}^n \theta_j \equiv \Theta \pmod{\pi}$

Test: $\bigoplus_{j=1}^n y_j = \frac{\sum_{j=1}^n \theta_j - \Theta}{\pi} \pmod 2$

Par la promesse sur les entrées, on peut distinguer deux cas: soit $\sum_{j=1}^n \theta_j - \Theta \equiv 0 \pmod{2\pi}$ ou $\sum_{j=1}^n \theta_j - \Theta \equiv \pi \pmod{2\pi}$. Après toute activité des parties et avant la mesure dans la base "de calcul" ($|0\rangle, |1\rangle$), dans le premier cas l'état est dans une superposition égale de tous les bistrings avec un nombre pair des 1, et dans le deuxieme cas, il est dans une superposition égale de tous les bistrings avec un nombre impair des 1. Par conséquent, le test réussit toujours à $|G_\theta^n\rangle$, pour les entrées qui sont compatibles avec la promesse.

On peut maintenant considerer la mesure la plus générale d'un état $|\Psi\rangle$. C'est un POVM $\{P_\Theta^n, \mathbb{I}_n - P_\Theta^n\}$, où le premier élément désigne succès du test et le deuxième échec. Nous allons prouver par induction que:

$$P_\Theta^n = |G_\Theta^n\rangle\langle G_\Theta^n| + \frac{1}{2} I_\Theta^n$$

où I_Θ^n est la projection sur l'espace orthogonal à $|G_\Theta^n\rangle$ et $|G_{\Theta+\pi}^n\rangle$.

Induction. Pour $n = 1$, on a $P_\Theta^1 = |G_{\theta_1}^1\rangle\langle G_{\theta_1}^1|$, alors la déclaration est correcte. On suppose que c'est vrai pour n parties et on va montrer la déclaration pour $n + 1$.

Si $\{P_\Theta^{n+1}(\theta_1), \mathbb{I}_{n+1} - P_\Theta^{n+1}(\theta_1)\}$ est le POVM qui correspond au test pour une angle θ_1 de la partie A_1, alors on peut distinguer deux cas selon la sortie de A_1:

1. Partie A_1 sorties $y_1 = 0$. Les autres n parties doivent passer le test:

$$\bigoplus_{j=2}^{n+1} y_j = \frac{\sum_{j=2}^{n+1} \theta_j - (\Theta - \theta_1)}{\pi} \pmod 2$$

2. Partie A_1 sorties $y_1 = 1$. Les autres n parties doivent passer le test:

$$\bigoplus_{j=2}^{n+1} y_j = \frac{\sum_{j=2}^{n+1} \theta_j - (\Theta - \theta_1 + \pi)}{\pi} \pmod 2$$

Si $\Theta_{\neg 1} \equiv \Theta - \theta_1 \pmod{2\pi}$, c'est evident que le premier test est equivalent à l'élément positif du POVM $P^n_{\Theta_{\neg_1}}$ à l'état $|G^n_{\Theta_{\neg_1}}\rangle$ et le deuxieme à l'élément positif du POVM $P^n_{\Theta_{\neg_1}+\pi}$ à l'état $|G^n_{\Theta_{\neg_1}+\pi}\rangle$. De l'induction, on sait que:

$$\begin{aligned} P^n_{\Theta_{\neg_1}+\pi} &= |G^n_{\Theta_{\neg_1}+\pi}\rangle\langle G^n_{\Theta_{\neg_1}+\pi}| + \frac{1}{2} I^n_\Theta \\ &= |G^n_{\Theta_{\neg_1}+\pi}\rangle\langle G^n_{\Theta_{\neg_1}+\pi}| + |G^n_{\Theta_{\neg_1}}\rangle\langle G^n_{\Theta_{\neg_1}}| + I^n_\Theta - |G^n_{\Theta_{\neg_1}}\rangle\langle G^n_{\Theta_{\neg_1}}| - \frac{1}{2} I^n_\Theta \\ &= \mathbb{I}_n - P^n_{\Theta_{\neg_1}} \end{aligned} \tag{3}$$

Pour que le test aux $n+1$ parties réussisse avec une angle θ_1:

$$\begin{aligned} P^{n+1}_\Theta(\theta_1) &= |G^1_{\theta_1}\rangle\langle G^1_{\theta_1}| \otimes P^n_{\Theta_{\neg_1}} + |G^1_{\theta_1+\pi}\rangle\langle G^1_{\theta_1+\pi}| \otimes (\mathbb{I}_n - P^n_{\Theta_{\neg_1}}) \\ &= |G^1_{\theta_1}\rangle\langle G^1_{\theta_1}| \otimes |G^n_{\Theta_{\neg_1}}\rangle\langle G^n_{\Theta_{\neg_1}}| + |G^1_{\theta_1+\pi}\rangle\langle G^1_{\theta_1+\pi}| \otimes |G^n_{\Theta_{\neg_1}+\pi}\rangle\langle G^n_{\Theta_{\neg_1}+\pi}| \\ &+ \frac{1}{2}\Big(|G^1_{\theta_1}\rangle\langle G^1_{\theta_1}| + |G^1_{\theta_1+\pi}\rangle\langle G^1_{\theta_1+\pi}|\Big) \otimes I^n_\Theta \\ &= |G^{n+1}_\Theta\rangle\langle G^{n+1}_\Theta| + |\Phi^{n+1}_{\theta_1,\Theta}\rangle\langle \Phi^{n+1}_{\theta_1,\Theta}| + \frac{1}{2}\mathbb{I}_1 \otimes I^n_\Theta \end{aligned} \tag{4}$$

où pour un $\Theta \in [0, 2\pi)$ donné, et pour $\theta_1 \in [0, \pi)$ one définit:

$$|\Phi^{n+1}_{\theta_1,\Theta}\rangle = \frac{1}{\sqrt{2}}\Big(|G^1_{\theta_1}\rangle|G^n_{\Theta_{\neg_1}}\rangle - |G^1_{\theta_1+\pi}\rangle|G^n_{\Theta_{\neg_1}+\pi}\rangle\Big)$$

L'angle θ_1 est choisi uniformément au hasard dans $[0, \pi)$, alors on a:

$$\begin{aligned} P^{n+1}_\Theta &= \frac{1}{\pi}\int_0^\pi P^{n+1}_\Theta(\theta_1) d\theta_1 = \frac{1}{\pi}\int_0^{\pi/2} \Big[P^{n+1}_\Theta(\theta_1) + P^{n+1}_\Theta(\theta_1 + \frac{\pi}{2})\Big] d\theta_1 \\ &= \frac{1}{\pi}\int_0^{\pi/2} \Big[2 \times |G^{n+1}_\Theta\rangle\langle G^{n+1}_\Theta| + |\Phi^{n+1}_{\theta_1,\Theta}\rangle\langle \Phi^{n+1}_{\theta_1,\Theta}| + |\Phi^{n+1}_{\theta_1+\frac{\pi}{2},\Theta}\rangle\langle \Phi^{n+1}_{\theta_1+\frac{\pi}{2},\Theta}| + \mathbb{I}_1 \otimes I^n_\Theta\Big] d\theta_1 \\ &= |G^{n+1}_\Theta\rangle\langle G^{n+1}_\Theta| + \frac{1}{2} I^{n+1}_\Theta \end{aligned} \tag{5}$$

parce que:

$$I_{\Theta}^{n+1} = |\Phi_{\theta_1,\Theta}^{n+1}\rangle\langle\Phi_{\theta_1,\Theta}^{n+1}| + |\Phi_{\theta_1+\frac{\pi}{2},\Theta}^{n+1}\rangle\langle\Phi_{\theta_1+\frac{\pi}{2},\Theta}^{n+1}| + \mathbb{I}_1 \otimes I_{\Theta}^{n}$$

Eq. 5 est correcte pour toutes les angles $\Theta \in [0, 2\pi)$, et plus particulierement pour $\Theta = 0 \pmod{2\pi}$, alors notre argument selon lequel le test de vérification T pour l'état GHZ $ket G_0^n$ est équivalent à l'exécution du POVM $\{P_0^n, \mathbb{I}_n - P_0^n\}$ est correct.

Notre objectif est de tester un état $|\Psi\rangle$ inconnu, partagée par la source entre n parties. Si l'état a une distance de trace avec GHZ égal á $\epsilon = D(|\Psi\rangle, |G_0^n\rangle)$, on peut écrire:

$$|\Psi\rangle = \sqrt{1-\epsilon^2}|G_0^n\rangle + \epsilon_1|G_\pi^n\rangle + \sqrt{\epsilon^2 - \epsilon_1^2}|\mathcal{X}\rangle,$$

où $|\mathcal{X}\rangle$ est un vecteur orthogonale à $|G_0^n\rangle$ et $|G_\pi^n\rangle$. Enfin:

$$\Pr[T(|\Psi\rangle) = 1] = \mathrm{tr}(P_0^n|\Psi\rangle\langle\Psi|) \leq 1 - \frac{\epsilon^2}{2}$$

□

Maintenant, on va étudier le cas des parties malhonnêtes, où un Vérificateur honnête veut exécuter le test afin de vérifier l'état $|\Psi\rangle$. Le Vérificateur ne sait pas si les parties malhonnêtes agissent comme $n-k$ parties indépendantes, chacun tenant un qubit, ou s' ils s'agissent ensemble. Alors, toute preuve de sécurité doit considerer que les parties malhonnêtes peuvent appliquer n' importe quel opérateur sur leur espace.

Theorem 2 (Cas malhonnête)**.** *Si $|\Psi\rangle$ est l' état partagé entre n parties, et $\min_U D\big((\mathbb{I} \otimes U)|\Psi\rangle, |G_0^n\rangle\big) = \epsilon$, où U est un operateur sur l'espace des parties malhonnêtes, alors $\Pr[T(|\Psi\rangle) = 1] \leq 1 - \frac{\epsilon^2}{4}$.*

Proof. on peut exprimer l'état qui est partagée par la source comme suit:

$$|\Psi\rangle = |G_h^k\rangle|\Psi_h\rangle + |G_{h+\pi}^k\rangle|\Psi_{h+\pi}\rangle + |\mathcal{X}\rangle \tag{6}$$

où $|G_a^k\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle^k + e^{ia}|1\rangle^k\big)$, $\mathcal{H}$: l'ensemble des parties honnêtes, $k = |\mathcal{H}|$: le nombre de parties honnêtes et $h = \sum_{j\in\mathcal{H}} \theta_j \pmod{\pi}$: l'entrée de toutes les parties dans $\mathcal{H}$, connu par l'ensemble malhonnête. Les états $|\Psi_h\rangle$ et $|\Psi_{h+\pi}\rangle$ ne sont pas normalisés et $|\mathcal{X}\rangle$ est un état arbitraire dont la part "honnête" est orthogonale à $|G_h^k\rangle$ et $|G_{h+\pi}^k\rangle$.

Les parties malhonnêtes veulent savoir dans lequel des deux états $|G_h^k\rangle$ et $|G_{h+\pi}^k\rangle$ la part honnête va se effondrer après la mesure, et par conséquent ce que sera la sortie honnête $Y_{\mathcal{H}} = \sum_{j\in\mathcal{H}} y_j \pmod 2$. Ils vont effectuer une mesure Helstrom sur leur part afin de distinguer entre $|\Psi_h\rangle$ et $|\Psi_{h+\pi}\rangle$. Cette mesure est optimale et donne la borne

suivante:

$$\Pr[\text{guess } Y_{\mathcal{H}}|h] = \frac{1}{2} + \frac{1}{2}\left\| |\Psi_h\rangle\langle\Psi_h| - |\Psi_{h+\pi}\rangle\langle\Psi_{h+\pi}| \right\|_1$$

Pour calculer la norme ci-dessus, on fait usage d'une propriété bien connu, que la norme de trace d'une matrice Hermitienne est égale à la somme des valeurs absolues de ses valeurs propres. Après quelques calculs simples, on peut vérifier que la probabilité ci-dessus est égale à:

$$\Pr[\text{guess } Y_{\mathcal{H}}|h] \leq 1 - \frac{1}{4}\Big(1 - \big(|||\Psi_h\rangle||^2 + |||\Psi_{h+\pi}\rangle||^2 \big)^2 + 4|\langle\Psi_h|\Psi_{h+\pi}\rangle|^2\Big) \tag{7}$$

Ensuite, on fait une décomposition de Schmidt à $|G_h^k\rangle|\Psi_h\rangle + |G_{h+\pi}^k\rangle|\Psi_{h+\pi}\rangle$, et on peut exprimer le produit scalaire $|\langle\Psi_h|\Psi_{h+\pi}\rangle|$ comme une fonction des normes des états de la décomposition p_h and q_h[2], où $p_h + q_h = |||\Psi_h\rangle||^2 + |||\Psi_{h+\pi}\rangle||^2$ et un paramètre α, qui peut être considéré comme une caractéristique de l'état $|\Psi\rangle$. Nous pouvons donc réécrire l'Equation 7:

$$\Pr[\text{guess } Y_{\mathcal{H}}|h] \leq 1 - \frac{1}{4}\Big(1 - (p+q)^2 + (p-q)^2 sin^2(h+\alpha)\Big) \tag{8}$$

En général, nous considérons que les parties malhonnêtes peuvent effectuer toute opération locale U sur leur état, afin de maximiser leur probabilité de tricherie. Ainsi, il est préférable d'exprimer la distance entre $|\Psi\rangle$ et le GHZ comme:

$$\epsilon = min_U D(((\mathbb{I}\otimes U)|\Psi\rangle, |G_0^n\rangle) = min_U \sqrt{1 - F^2(((\mathbb{I}\otimes U)|\Psi\rangle, |G_0^n\rangle)}$$

où $F(|\psi\rangle, |\phi\rangle)$ est la fidelité entre deux états $|\psi\rangle$ et $|\phi\rangle$. Comme précédemment, si on décrit les matrices de densité réduites des parties honnêtes de l'état parfait et l'état réel avec $\sigma_{\mathcal{H}}$ et $\rho_{\mathcal{H}}$ respectivement, il existe une opération local R sur l'état malhonnête telle que:

$$F(((\mathbb{I}\otimes R)|\Psi\rangle, |G_0^n\rangle) = F(\sigma_{\mathcal{H}}, \rho_{\mathcal{H}})$$

En appliquant cette opération R, nous obtenons:

$$\epsilon^2 \quad = \quad 1 - \frac{p+q}{2} - \sqrt{pq} \leq 1 - (p+q)^2 + \frac{(p-q)^2}{2}$$

et puisque h est choisi uniformément au hasard et $p+q$ est constante pour chaque h, on

[2]Ici, p_h et q_h dependent de h, mais pour faciliter l'utilisation, dans ce qui suit, on n'utilise pas un indice pour un h fixe.

a:

$$\begin{aligned}\Pr[\text{guess } Y_{\mathcal{H}}] &= \frac{1}{\pi}\int_0^{\pi} \Pr[\text{guess } Y_{\mathcal{H}}|h]dh \\ &\leq 1-\frac{1}{4}\Big(1-(p+q)^2+\epsilon^2-1+(p+q)^2\Big) \\ &\leq 1-\frac{\epsilon^2}{4}\end{aligned}$$

□

Jeux Quantiques

Un domaine de recherche qui a récemment attiré beaucoup d'intérêt est la theorie des jeux quantiques [22, 23], en raison du potentiel de la communication quantique à fournir des gains plus élevés pour les joueurs. En général, on peut exprimer toute interaction entre les parties comme un jeu où les joueurs interagissent et reçoivent des informations, prennent des décisions et à la fin ils reçoivent un gain conformément à une fonction qui dépend de leurs actions. En général, on suppose que les joueurs d'un jeu choisissent leurs actions d'une manière qui maximise leur gain à la fin du jeu.

Dans cette thèse, nous allons étudier un type spécifique de jeux à information incomplète qui a été introduit par Harsanyi en 1967 [24]. Ces jeux sont aussi appelés jeux bayésiens. En général, tous les jeux qui sont d'intérêt pour la théorie de la communication quantique, appartiennent à cette catégorie de jeux à information incomplète. Par exemple, le célèbre jeu de CHSH [25], où les deux joueurs, Alice et Bob, reçoivent leurs entrées au hasard et partagent un état intriqué, est un jeu bayésien, car chaque joueur doit décider la valeur de son bit de sortie sans connaître l'entrée de l'autre joueur. Le lien entre la non-localité et les jeux bayésiens a donc été étudié pendant une longue période, avec une étude plus récent apparaissant dans [26].

Toutes les études précédentes de jeux bayésiens quantiques considéraient des jeux d'*intérêt commun*. Dans l'exemple du jeu CHSH, la fonction de gain pour les deux joueurs est le même, alors la stratégie optimale pour un joueur est également la stratégie optimale pour l'autre joueur. Cependant, les jeux de *conflit d'intérêts* sont également très important, car il est fréquent que l'intérêt d'une personne est en opposition avec l'intérêt de l'autre. Un exemple typique de ce type de jeux est la *Bataille des Sexes*, où Alice et Bob veulent rencontrer le samedi soir, mais Alice préfère aller au ballet, tandis que Bob veut aller au théâtre.

Ici, on s'intéresse à examiner si la mécanique quantique fournit un avantage pour les jeux bayésiens de conflit d'intérêts. Nous allons présenter un jeu quantique bayésien à deux joueurs, où les joueurs ont des intérêts contradictoires. Nous allons considérer que les deux joueurs partagent un état quantique avant que le jeu commence et au début du jeu, chacun d'entre eux reçoit un bit aléatoire qui détermine leur type. Les actions des joueurs sont des mesures de l'état quantique, et dépendent du type de chaque joueur et leur conviction sur l'action de l'autre joueur. Après la mesure de l'état, ils donnent leurs résultats qui, avec leur entrée, déterminent leurs gains suivant une fonction. Par conséquent, la fonction de gain, qui peut être différent pour chaque joueur, dépend à la fois les types/entrées et actions/sorties des joueurs et est généralement représentée par une table.

Nous allons examiner l'avantage offert par la mécanique quantique, en observant qu'il existe des stratégies quantiques qui donnent une somme plus élevée des gains

des deux joueurs, par rapport à toute stratégie classique. Nous allons étudier s' il est avantageux pour les joueurs de respecter les stratégies quantiques proposées ou s'ils préférent plutôt agir différemment pour augmenter leurs gains. Une stratégie jointe qui n'encourage pas un joueur de changer son action, étant donné que l'autre joueur la suit également, définit un équilibre de Nash. On va voir que presque aucune des stratégies qui maximisent la somme des gains des deux joueurs n'est pas un point d'équilibre, à l'exception de la stratégie juste (c'est à dire celle qui, si suivie par les deux joueurs, retourne des gains égaux aux deux joueurs). Par conséquent, nous allons montrer qu'il existe des jeux bayésiens de conflit d'intérêts, où l'équilibre quantique peut fournit de meilleures gains pour les joueurs que l'équilibre classique. Enfin, nous allons utiliser une source commerciale de photons intriqués afin de jouer le jeu quantique proposé. Nous allons montrer qu'en partageant un état presque au maximum intriqué et en suivant des stratégies spécifiques (mesures sur l'état quantique), les deux joueurs gagnent plus que classiquement possible.

Jeux Bayésiens Nous allons commencer par définir un jeu bayésien dans le cadre des deux partis (voir [27] pour une définition plus générale de jeux bayésiens). C'est composé de:

- Deux joueurs, Alice (A) et Bob (B).
- Un ensemble $\mathcal{X} = \mathcal{X}_A \otimes \mathcal{X}_B$ des types/mesures $x = \{x_A, x_B\}$, où $x_A \in \mathcal{X}_A$, $x_B \in \mathcal{X}_B$.
- Un ensemble $\mathcal{Y} = \mathcal{Y}_A \otimes \mathcal{Y}_B$ des actions/sorties $y = \{y_A, y_B\}$, où $y_A \in \mathcal{Y}_A$, $y_B \in \mathcal{Y}_B$.
- Une fonction d'utilité $u_i : \mathcal{X}_A \times \mathcal{X}_B \times \mathcal{Y}_A \times \mathcal{Y}_B \to \mathbb{R}$ pour chaque joueur $i \in \{A, B\}$ et pour toutes les combinaisons de types et des actions des deux joueurs.
- Une distribution de probabilité sur les types des joueurs, $P : \mathcal{X} \to [0, 1]$.

Les fonctions d'utilité u_A et u_B pour chaque combinaison des types et actions des joueurs peuvent être visualisés sous la forme d'une table: les lignes correspondent aux valeurs possibles de la variable y_A et les colonnes correspondent aux valeurs possibles de la variable y_B. Les chiffres dans chaque cellule sont les utilités des joueurs (u_A, u_B) en fonction de leurs types et les actions. Au cas où les utilités sont différents pour différents types des deux joueurs, alors nous avons besoin d'introduire plus de tables. En général, chaque joueur $i \in \{A, B\}$ est intéressé à maximiser son gain moyen F_i défini comme suit:

$$F_i = \sum_{\substack{x \in \mathcal{X} \\ y \in \mathcal{Y}}} P(x) \Pr(y|x) u_i(x, y) \tag{9}$$

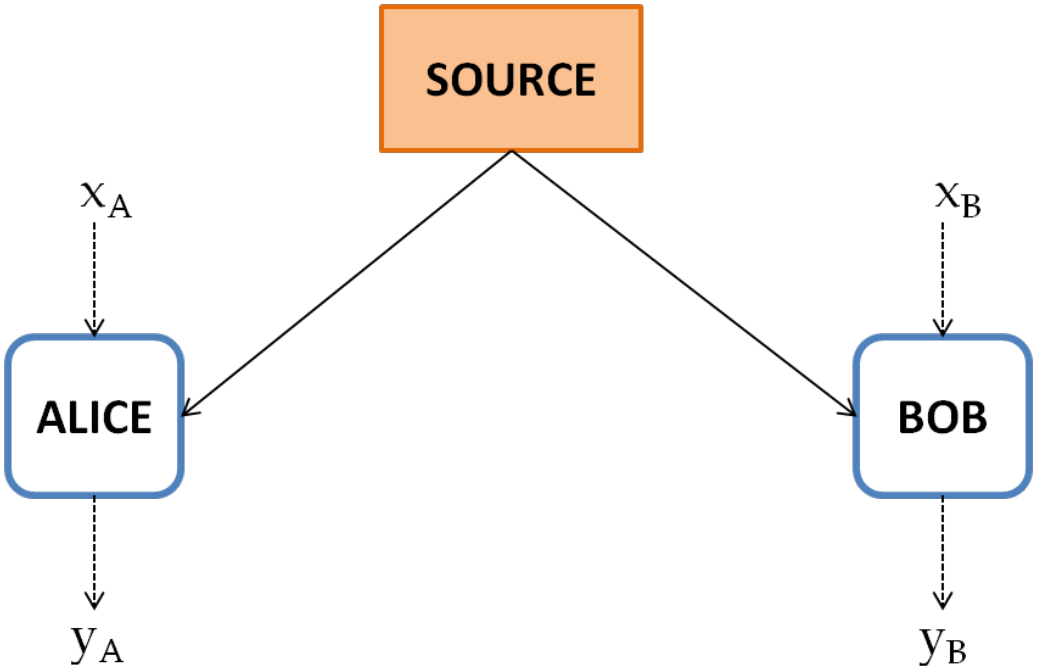


Figure 3: Le jeu bayésien entre deux parties

Le jeu se déroule comme dans la Figure 3. Les entrées des joueurs sont choisis après une distribution de probabilité en produit $P = P_A \times P_B$, donc chaque joueur $i \in \{A, B\}$ acquiert un type x_i selon la distribution de probabilité P_i . Ils reçoivent également un conseil d'une source qui est indépendante des entrées choisies x_i. Enfin, ils décident de leur action/sortie y_i, selon une stratégie choisie.

On va examiner l'effet des corrélations classiques et quantiques dans les jeux bayésiens avec conflit d'intérêt en examinant un jeu bayésien qui combine la " Bataille des Sexes " et le jeu de CHSH. Le jeu est défini par les gains des deux joueurs tels que décrits dans les tables d' utilité de la Figure 4. Nous avons deux tables d'utilité, en fonction de AND logique entre les types des joueurs.

y_A \ y_B	0	1
0	(1,1/2)	(0,0)
1	(0,0)	(1/2,1)

(a) $x_A \wedge x_B = 0$

y_A \ y_B	0	1
0	(0,0)	(3/4,3/4)
1	(3/4,3/4)	(0,0)

(b) $x_A \wedge x_B = 1$

Figure 4: Jeu avec conflit d'intérêts

Considérons maintenant le cas où la source envoie des conseils quantiques aux deux joueurs, sous la forme d'un état quantique des deux qubits, partagé entre les deux joueurs.

Nous examinerons d'abord un ensemble de mesures quantiques dans le cas d'un état EPR, puis nous allons examiner ce qui arrive quand l'état partagé n'est pas maximalement intriqué.

Supposons d'abord que l'état partagé est une paire EPR $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. Une stratégie quantique consiste de l'état $|\Phi\rangle$ et les observables que Alice et Bob appliquent à l'état. Le gain moyenne pour chaque joueur est donné par Eq. 9. Comme pour l'analyse du jeu CHSH par Cleve et al [28], si les joueurs utilisent les mesures projectives qui suivent, en fonction de leurs entrées:

$$\begin{aligned}
\mathcal{A}_0^a &= |\phi_a(0)\rangle\langle\phi_a(0)| \\
\mathcal{A}_1^a &= |\phi_a(\frac{\pi}{4})\rangle\langle\phi_a(\frac{\pi}{4})| \\
\mathcal{B}_0^b &= |\phi_b(\frac{\pi}{8})\rangle\langle\phi_b(\frac{\pi}{8})| \\
\mathcal{B}_1^b &= |\phi_b(-\frac{\pi}{8})\rangle\langle\phi_b(-\frac{\pi}{8})|
\end{aligned}$$

pour $a, b \in \{0,1\}$, où $\phi_0(\theta) = \cos\theta|0\rangle + \sin\theta|1\rangle$ et $\phi_1(\theta) = -\sin\theta|0\rangle + \cos\theta|1\rangle$, on a:

$$\Pr(y_A, y_B|x_A, x_B) = \frac{1}{2}\mathrm{tr}(\mathcal{A}_{x_A}^{y_A}, \mathcal{B}_{x_B}^{y_B}) = \frac{1}{2}\cos^2\frac{\pi}{8}$$

Pour $i \in \{A, B\}$, Eq. 9 devient:

$$F_i = \frac{1}{8}\cos^2\frac{\pi}{8}\sum_{\substack{x\in\mathcal{X}\\ y\in\mathcal{Y}}} u_i(x,y) = \frac{3}{4}\cdot 0.85$$

Une stratégie quantique $\mathcal{M} = (\mathcal{A}, \mathcal{B}, |\Phi\rangle)$, où $\mathcal{A} = \{\mathcal{A}_0, \mathcal{A}_1\}$, $\mathcal{B} = \{\mathcal{B}_0, \mathcal{B}_1\}$, se compose de Alice et Bob appliquant respectivement les observables $\mathcal{A}_{x_A} = \{A_{x_A}^0, A_{x_A}^1\}$ et $\mathcal{B}_{x_B} = \{B_{x_B}^0, B_{x_B}^1\}$ sur l'état quantique $|\Phi\rangle$. La probabilité que les deux joueurs produisent comme sortie y quand l'entrée est x, est $\Pr(y|x) = \mathrm{tr}(M_x^y\rho)$, où $M_x^y = A_{x_A}^{y_A} \otimes B_{x_B}^{y_B}$. On peut utiliser des programmes positifs semi-définis (SDP) avec des contraintes appropriées, afin de montrer que la stratégie quantique $\mathcal{M}$ est un point d'équilibre de Nash quantique, car si l'un des deux joueurs change son strategie, cela ne lui donne pas un gain plus élevé.

On constate également que cette stratégie spécifique est juste pour les deux joueurs, car elle donne des gains moyens égaux. Cependant, on peut voir qu'il existe des stratégies pas justes classiques qui donnent des gains moyens plus élevés pour un seul joueur que cette stratégie quantique. Mais si on regarde à la somme des gains des deux joueurs, on a $F_A^{juste} + F_B^{juste} = \frac{3}{2}\cdot 0.85$, toujours plus grand que $\frac{9}{8}$, la borne supérieure pour la somme

des gains de toute stratégie classique, avec ou sans le conseil d'un tiers. On peut donc observer l'avantage apporté par le partage d'un état intriqué, si on regarde le gain moyen des deux joueurs en même temps.

Le jeu qu'on a précédemment défini, permet de tester l'avantage quantique expérimentale d'une manière simple, à l'aide d'un Générateur d'intrication commerciale (EGD) de QuTools [29]. La source crée des paires intriquées, que nous allons utiliser pour jouer notre jeu. On mesure chaque état en utilisant les mêmes bases que celles définies auparavant, selon l'entrée de chaque joueur.

Plus précisément, Alice mesure dans $\{\mathcal{A}^0_{x_A}, \mathcal{A}^1_{x_A}\}$ et Bob mesure dans $\{\mathcal{B}^0_{x_B}, \mathcal{B}^1_{x_B}\}$. Pour chaque entrée (x_A, x_B), on veut savoir:

$$\Pr(y_A, y_B | x_A, x_B) = \frac{\text{nombre des détections } (\mathcal{A}^{y_A}_{x_A}, \mathcal{B}^{y_B}_{x_B})}{\text{nombre total des détections pour } (x_A, x_B)}$$

Le EGD a deux canaux de sortie qui ont été connectés à un converteur Time-to-Digital (TDC), pour compter les coïncidences produites entre les détecteurs de Alice et Bob. Le TDC nous donne accès à la fois aux comptes individuels de chaque détecteur et les coïncidences entre eux. On peut aussi soustraire le montant des comtes noirs (dark counts) et trouver le nombre des coïncidences qui résultent uniquement de l'état intriqué créé par le EGD. On peut alors calculer les gains moyens quantiques des deux joueurs avant et après le retrait des comtes noirs:

$$F_A = \frac{1}{4}\sum_{x_A,x_B} F_A(x_A,x_B) = 0.612416, \quad F_B = \frac{1}{4}\sum_{x_A,x_B} F_B(x_A,x_B) = 0.620532$$

$$F'_A = \frac{1}{4}\sum_{x_A,x_B} F'_A(x_A,x_B) = 0.621367, \quad F'_B = \frac{1}{4}\sum_{x_A,x_B} F'_B(x_A,x_B) = 0.624569$$

et vérifier que la somme des gains est bien au-dessus de la valeur classique 1.125 ($F_A + F_B = 1.232948$ et $F'_A + F'_B = 1.245936$). Ces deux sommes sont légèrement en dessous de la valeur maximale imposée par la mécanique quantique, comme prévu en raison de la distance entre l'état généré et la paire EPR.

Dans la Figure 5 on peut comparer les stratégies classiques optimales avec les stratégies quantiques qui maximisent la somme des gains, et on peut également voir que la stratégie quantique juste est un équilibre de Nash. En outre, on présente les données expérimentales obtenues après l'élimination des comtes noirs, et on vérifie que les résultats se situent au-dessus de la limite classique, mais en dessous de la limite optimale quantique, puisque la fidélité entre l'état partagé et la paire EPR est inférieur à un.

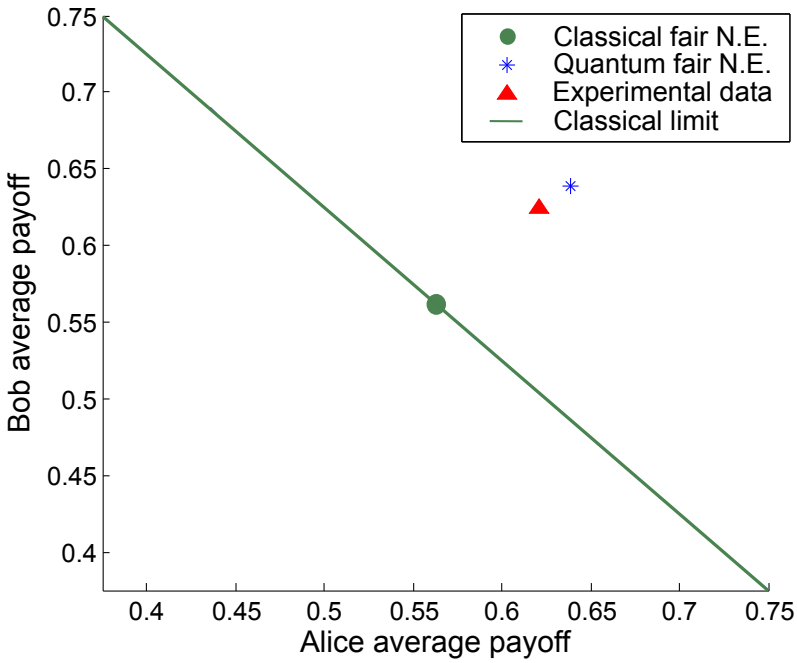


Figure 5: Comparison of classical and quantum strategies

Chapter 1

Introduction

During the last decades, it has become apparent that the tools provided by quantum mechanics can be used in many fields, such as cryptography, algorithms and complexity theory, game theory and even biology. From the early 20th century, Einstein, Podolski and Rosen [1] had realized the power of quantum mechanics, presenting the basic principles on which quantum cryptography was to be based. What seemed very counterintuitive and hard to accept was the fact that nature is inherently probabilistic, even when one takes into account any local hidden parameters. Several years later, in 1964, it was theoretically proven by John Bell [2], that the paradox that seemed so hard to accept, is an intrinsic characteristic of nature called "non-locality".

Almost two decades after Bell's ground-breaking theorem, the first experimental implementations of the Einstein-Podolski-Rosen (EPR) "spooky action at a distance" took place, with the most famous one being that of Aspect et al. in 1982 [3]. However, even though there has been tremendous scientific progress in quantum implementations over the years, an experimental verification of Bell's theorem that closes all so-called "loopholes" (i.e. problems that may render the experimental conclusions invalid) has yet to be achieved.

At the same time, theorists have been trying to find ways to use this inherent randomness of quantum mechanics in several subfields of computation and communication theory. Things started to quickly progress after Charles Bennet and Gilles Brassard, based on previous work by Stephen Wiesner [4], proposed the first quantum key distribution and coin flipping scheme in 1984 [5]. A decade later, Peter Shor invented one of the most famous results in quantum computing [6], an algorithm that solves the factoring problem[1] in polynomial time, much faster than the best classical algorithm that runs in sub-exponential time. Since widely used public-key cryptographic schemes, such as the RSA, are based on the difficulty of factoring large numbers on a classical computer, the

[1] Given a large integer N, find its prime factors.

use of a quantum computer could potentially lead to important security breaches over the Internet.

Despite the tremendous progress of the last years, both theoretical and experimental, it seems that we are still far from constructing a universal quantum computer that could replace classical computers in everyday use. A more plausible scenario is that of a hybrid network of quantum and classical devices, where individual agents have the ability to communicate in a variety of ways with trusted and untrusted parties, and securely delegate computational tasks to a number of untrusted largescale quantum computing servers. As in all telecommunication networks, secure computation and communication between agents is a prerequisite, rendering specific cryptographic primitives essential. These include authentication, identification, leader election, bit commitment and coin flipping and are the basis of more complex computations.

Another equally important property of such a hybrid network is the ability to verify that the untrusted agents and servers in the network perform the expected quantum processes, a task which is intimately related to the possibility of observing nonlocal effects and testing quantum mechanics. In this context, a lot of research has been concentrated on the closely related notions of self-testing, device-independence and verification of computation (blind computing, entanglement verification, etc).

Finally, when designing a quantum protocol, it is also important to keep in mind that its experimental implementation may prove difficult because of the particularities of quantum mechanics. Many protocols that are in theory secure, cannot be experimentally implemented, because they do not tolerate any amount of losses or noise. It is therefore necessary to always consider adversaries that might be able to manipulate losses and errors to their advantage, and of course adapt the security analysis of the protocols accordingly.

1.1 Thesis Contribution

This thesis aims at bringing closer the theoretical and experimental approaches on quantum computing. The goal is to design and analyse new multiparty protocols that can be used as building blocks for other more complicated protocols, and also study their implementability. In the following paragraphs, we discuss the theoretical and experimental progress that was achieved during this thesis, on quantum coin flipping, multipartite entanglement verification and quantum games.

1.1.1 Quantum Coin Flipping

Two-party protocols are the basis of any distributed computation scheme, classical or quantum. There are two models of two-party computation, the *cooperative* and the *non-*

cooperative model. In the cooperative model, the parties trust each other, and they are working together towards a common goal. At the same time, they try to achieve some kind of security against an external adversary that may be eavesdropping their communication. An example of a well studied two-party quantum protocol is key distribution, where the parties want to share a common key, that is kept secret from any third party. Since the first work on quantum key distribution (QKD) appeared [5], many protocols have been proposed and implemented, that achieve high key generation rates for distances that go up to a couple hundreds of kilometers [7, 8].

On the other hand, the non-cooperative model has been much less studied, both in theory and in practice. In this model, one of the two parties is dishonest and tries to cheat. Important examples of two-party protocols are bit commitment, coin flipping and oblivious transfer. In this thesis, we will concentrate on *coin flipping*, the primitive where two parties want to flip a coin (i.e. obtain a random bit), while they are separated by long distance. Here, the goal of the dishonest party is to output a specific bit rather than a random one, or as we will usually say, he/she wants to *bias* the outcome of the coin flip.

Coin flipping is widely used in communication networks. For instance, it is used for online gaming, for randomized consensus protocols (due to its equivalence to the leader election functionality, a fundamental primitive in distributed computing), and it is also an integral component for secure function evaluation [9]. Unfortunately, perfect coin flipping against unbounded adversaries is known to be impossible both classically and quantumly [10, 11]. This means that when one of the parties is dishonest, he/she can bias the outcome of the coin flip so that it is no longer perfectly random. Nevertheless, contrary to the classical case, when using quantum states it is still possible to achieve some kind of security, meaning that it is possible to upperbound the probability of the dishonest party to bias the coin. There have been several theoretical quantum protocols that provide an upperbound on the bias probability, but not many of them have been implemented, with the few exceptions achieving limited communication distance up to a few meters.

One of the main contributions of this thesis is the proposal of a simple quantum coin flipping protocol that takes into account all standard experimental imperfections, including loss of signal and errors in transmission and detection. We provide extensive proofs of security that can be adapted to experimental implementations, but also particularly to the so-called *plug& play* system, and show how to evaluate and post-process experimental data, given the specific amounts of errors and losses in the experiment. We then use an enhanced version of a commercial plug&play system (IdQuantique's Clavis2) in order to demonstrate our theoretical results. We manage to significantly improve previous experimental implementations by achieving several coin flips per second over 15km of optical fibre. We also note that the proposed protocol is also a bit commitment

protocol, and we can thus provide for this primitive the same security as for coin flipping.

Finally, we explore ways to combine our protocol with other protocols that are secure against adversaries with bounded resources. The restrictions on the adversaries can be either computational (inability to solve hard problems), or physical (memories that have bounded storage, or that get noisy over time). The purpose is to secure future communication networks against adversaries of varying complexity, where technological and computational capabilities may evolve very rapidly. Our results offer a complete theoretical and experimental framework for the implementation of quantum coin flipping in real communication scenarios.

1.1.2 Entanglement Verification

One of the most important phenomena in quantum mechanics is *entanglement*. Entangled systems are composed of two or more particles interacting in such a specific way that even when separated by great distance, they exhibit correlations that are not possible to simulate with any classical formalism.

Entangled systems are widely used in quantum computation and cryptography, for example in key distribution schemes, in secret sharing and in blind computing. It is therefore of great importance to be able to verify the entanglement in a multipartite system, especially in the case of distributed computation between untrusted parties.

This thesis reports the first study of multipartite entanglement verification in the presence of dishonest parties, both under perfect conditions and in the presence of realistic experimental errors. Given an untrusted source that creates a multiparty quantum state and shares it with untrusted (and possibly collaborating between them and with the source) parties, we provide a test for the honest parties to verify if the shared quantum state is a specific maximally entangled state. We start from ideal conditions (i.e. no losses, no errors) and study a protocol for pseudo-telepathy [21] that extends a well-known game to the multiparty case. We analyse its security in two cases: when all parties are honest, and when some of them are dishonest, and provide a test for the honest parties to check if the quantum state that they use in the computation, is properly (maximally) entangled. The probability of a quantum state to pass our test is a function of its distance from the correct (maximally) entangled one. This means that the further "away" the shared state is from the correct one, the lower the probability of passing the test is.

We then start introducing some losses in the test and observe that the security of our original protocol is completely "broken", when the amount of losses exceeds 50%. We show that the cause for this loss-intolerance, is the low number of different settings of the parties (in this case it is 2), and examine what happens when we try to increase it. We observe that by increasing the set of possible settings, we can recover the loss tolerance of our test for any amount of losses. We also examine the noise tolerance of

our new enhanced protocol, and provide a tradeoff between the amount of losses and noise that our protocol can tolerate in order to remain secure.

We finally provide a simple experimental procedure for verification of multiparty entangled states, that can be used in order to demonstrate the advantage of the new enhanced protocol in comparison with the original one. We are currently in the process of implementing the experimental procedure using the experimental setup that was presented in [30].

1.1.3 Quantum Game Theory

A research area that has lately attracted a lot of interest is Quantum Game Theory [22, 23], due to the potential of quantum communication to provide higher payoffs for the players. In general, we can express any interaction between players as a game, where the interacting players receive information, take actions and at the end receive a payoff according to a function that depends on the transcript of the game. We assume that the players of a game will try to choose their actions in a way that maximises their payoff at the end of the game. Since the payoff function of each player could depend on the actions of the other players, it is also interesting to search for points of equilibria, i.e. strategies such that if all players follow them, none of them would have an incentive to change his action. These strategies are called *Nash Equilibria*.

In this thesis, we will study a specific type of games with incomplete information first introduced by Harsanyi in 1967 [24], which are also called Bayesian games. In general, all games that are of interest in quantum communication theory, belong to this category of games of incomplete information. For example, the well-known CHSH game [25], where the two players, Alice and Bob, receive their inputs at random and share an entangled state, is a Bayesian game, since each player needs to decide on his output without knowing the input of the other player. The link between non-locality and Bayesian games has therefore been studied for a long time, with a more recent review appearing in [26].

All previous studies of quantum Bayesian games considered *common interest* games. In the previous example of the CHSH game, the payoff function for the two players is the same, so the optimal strategy for one player is also the optimal strategy for the other player. However, *conflicting interest* games are also very important, since it is common that the interest of one person is in clear contrast with the interest of the other. A typical example of this type of games is the *Battle of the Sexes*, where Alice and Bob want to meet on Saturday night, but Alice prefers going to the ballet, while Bob wants to go to the theater.

In this thesis, we are interested in examining whether quantum mechanics provides an advantage for conflicting interest Bayesian games. We will present a two-player quantum

Bayesian game where the players have conflicting interests. We will consider that the two players share a quantum state before the game starts and at the beginning of the game, each of them receives a random bit that determines their type. The players' actions are measurements of the quantum state, and depend on each player's type and their belief on the other player's action. After the measurement, they output their outcome which, together with their input, determines their payoffs according to a function. Therefore, the payoff function, which can be different for each player, depends on both the types/inputs and actions/outputs of the players and is usually depicted as a table.

We will examine the advantage offered by quantum mechanics, by observing that there exist quantum strategies that give a higher sum of the two players' payoffs, compared to any classical strategy. We will investigate whether it is to the benefit of the players to respect the proposed quantum strategies or if they would instead choose to act differently to increase their payoffs. A strategy that provides no incentive to any player to change their strategy, given that the other player also respects it, defines a Nash Equilibrium. We will see that almost none of the strategies that maximise the sum of the payoffs of the two players is an equilibrium point, with the exception of the fair strategy (i.e. the one that if followed by the two players, returns equal payoffs to both players). Hence, we will show that there exist Bayesian games with conflicting interests, where the quantum fair equilibrium has provides better payoffs for the players than the classical one. Finally, we will use a commercial entangled photon source in order to play the proposed quantum game in the lab. We will show that by sharing an almost maximally entangled state and by following specific strategies (i.e. measurements on the quantum state), the two players gain higher payoffs than classically possible.

1.2 Thesis Outline and Scientific Production

The thesis is organised as follows:

In Chapter 2 we introduce the basic notions of quantum computing and cryptography. We present the postulates of Quantum Mechanics and we look at the necessary building block for manifestation of non-locality, entanglement. We also briefly describe some basic cryptographic primitives and conclude with a presentation of the fundamental experimental tools that we will need in order to comprehend the implementations that follow.

Chapter 3 presents a theoretical and experimental approach to Coin Flipping. We show how to implement a theoretical protocol by using a plug&play system and how to evaluate and post-process the data, given the specific amounts of errors and losses in the experiment. We provide a full security analysis in the case of imperfections, and present a way to combine protocols against adversaries of unknown computational power.

In Chapter 4 we address the topic of entanglement verification in a non-trusted

environment. We particularly focus on GHZ states, a set of multiparty entangled states that are widely used in many schemes. In order to render our protocol implementable in practice, we introduce a novel way of dealing with losses and noise at the same time. Finally, we describe a simple experimental procedure in order to verify the validity of our protocol, which is also currently implemented using a 3-party and a 4-party noisy GHZ state.

Chapter 5 examines the effect of non-locality in Bayesian Game Theory. We present a conflicting interest game with incomplete information, where the players share an entangled state. We show that the quantum correlations that result from measurements on the entangled state, provide higher gains in states of equilibrium, than possible with the use of any classical correlations. We finally use an entangled photon source to experimentally demonstrate this gain.

Finally, in Chapter 6 we summarize our results and present some perspectives on future research.

The results in Chapter 3 and in the first half of Chapter 4, have appeared in the following publications:

[31] A. Pappa, A. Chailloux, E. Diamanti, and I. Kerenidis, *Practical Quantum Coin Flipping*, Phys. Rev. A **84**, 052305 (2011).

[32] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti and I. Kerenidis, *Multipartite Entanglement Verification Resistant against Dishonest Parties*, Phys. Rev. Lett. **108**, 260502 (2012).

[33] A. Pappa, P. Jouguet, T. Lawson, A. Chailloux, M. Legré, P. Trinkler, I. Kerenidis and E. Diamanti, *Experimental plug and play quantum coin flipping*, Nature Communications. **5**, 3717 (2014).

Two more manuscripts corresponding to the loss-tolerant entanglement verification protocol and its experimental implementation (Chapter 4), as well as the results of Chapter 5 on quantum games, are currently in preparation:

A. Pappa, W. McCutcheon, B. Bell, A. Chailloux, T. Lawson, M. Tame, D. Markham, E. Diamanti, I. Kerenidis and J. Rarity, *Experimental Demonstration of Entanglement Verification in a Cryptographic Setting*.

A. Pappa, N.Kumar, T. Lawson, E. Diamanti and I. Kerenidis, *Quantum Bayesian Game with Conflicting Interest*.

The results of this thesis have also been presented at the following conferences, workshops and seminars:

- Quantum Information Group, University of Bristol, 13 February 2014 (Seminar).
- Theoretical Computer Science and Quantum Computing Group (LITQ), University of Montreal, 20 November 2013 (Seminar).
- ACAC'13 - 8th Athens Colloquium on Algorithms and Complexity, 22-23 August 2013, Athens.
- Device-Independent Quantum Information Processing (DIQIP), Quantum Computer Scince (QCS) & Quantum Algorithms (QAlgo) Workshop, 14-17 May 2013, Paris, France.
- Fundamental Research on Quantum Networks and Cryptography (Frequency), Final Meeting, 18-19 February 2013, Paris, France.
- QIP'13 - 16th Workshop on Quantum Information Processing, 21-25 January 2013, Tsinghua University, Beijing, China (poster).
- Topical Research Meetings on Physics: Quantum Technologies, taking concepts through to implementations, 17-18 December 2012, Institute of Physics, London, UK.
- 2nd Workshop of GDR - IQFA, 28-30 November 2012, Neel Institute, Grenoble (poster).
- ACAC'12 - 7th Athens Colloquium on Algorithms and Complexity, 27-28 August 2012, Athens.
- TQC'12 - 7th Conference on Theory of Quantum Computation, Communication and Cryptography, 17-19 May 2012, Tokyo, Japan.
- Workshop of 'Fédération de Recherche en Mathématiques de Paris Centre / GT-Information Quantique', 9-10 May 2012, Université Denis Diderot, Paris, France.
- 1st Workshop of GDR - IQFA, 23-25 November 2011, Institut Henri Poincare, Paris France.
- Quantum Information in Paris Seminar, 29 September 2011, Institut Henri Poincare, Paris France.
- QCRYPT 2011: First Annual Conference on Quantum Cryptography, 12-16 September 2011, Zurich, Switzerland (poster).
- Workshop of GDR - IQFA, 23-25 March 2011, Parc Valrose, Université de Nice - Sophia Antipolis (poster).

1.3 Scientific Collaborations

This doctoral project has involved various scientific collaborations. In particular, the experimental demonstration of the Coin Flipping protocol has been conducted with the support of colleagues working at IdQuantique, Geneva. Furthermore, the thesis has been financially supported by Region Ile-de-France through a Digiteo Doctoral Scholarship, by Google through an Anita Borg Memorial Scholarship and by ANR through the project FREQUENCY (ANR-09-BLAN-0410).

Chapter 2

Preliminaries

2.1 Mathematical Preliminaries

In this Section we will present some basic notions of linear algebra that we will be using during the rest of the thesis. Two readings that provide a more detailed introduction to the mathematical foundations of quantum mechanics are the book of Nielsen and Chuang [34] and the lecture notes of John Watrous [35].

The first definition we need to give is that of a *complex vector space* $\mathcal{V}$. A complex vector space is formed by a set of vectors that can be added together or multiplied by complex numbers (called scalars). For $\mathcal{V}$ to be a complex vector space, $\forall\ \mathbf{u},\mathbf{v},\mathbf{w} \in \mathcal{V}$ and $\forall\ a, b \in \mathbb{C}$, the following properties are necessary for the two operations, $+ : \mathcal{V} \times \mathcal{V} \to \mathcal{V}$ and $\cdot : \mathbb{C} \times \mathcal{V} \to \mathcal{V}$

Closure of $+$	$\mathbf{u}+\mathbf{v} \in \mathcal{V}$
Closure of $\cdot$	$a \cdot \mathbf{u} \in \mathcal{V}$
Associativity of $+$	$\mathbf{u}+(\mathbf{v}+\mathbf{w}) = (\mathbf{u}+\mathbf{v})+\mathbf{w}$
Commutativity of $+$	$\mathbf{u}+\mathbf{v} = \mathbf{v}+\mathbf{u}$
Identity element of $+$	$\exists\ \mathbf{0} \in \mathcal{V}$ such that $\mathbf{0}+\mathbf{u} = \mathbf{u}$
Identity element of $\cdot$	$\exists\ 1 \in \mathbb{C}$ such that $1 \cdot \mathbf{u} = \mathbf{u}$
Inverse element for $+$	$\exists\ -\mathbf{u} \in \mathcal{V}$ such that $-\mathbf{u}+\mathbf{u} = \mathbf{0}$
Distributivity of $\cdot$	$a \cdot (\mathbf{u}+\mathbf{v}) = a\mathbf{u}+a\mathbf{v}$
	$(a+b) \cdot \mathbf{u} = a \cdot \mathbf{u} + b \cdot \mathbf{u}$
Compatibility of scalar and field multiplication	$(ab) \cdot \mathbf{u} = a \cdot (b \cdot \mathbf{u})$

A very important operation on pairs of vectors from a vector space, is the *inner product* $\langle \cdot, \cdot \rangle : \mathcal{V} \times \mathcal{V} \to \mathbb{C}$. An inner product function must satisfy the following requirements,

$\forall \mathbf{u}, \mathbf{v}, \mathbf{w} \in \mathcal{V}$ and $\forall a, b \in \mathbb{C}$

Linearity in the second argument	$\langle \mathbf{u}, a\mathbf{v} + b\mathbf{w} \rangle = a\langle \mathbf{u}, \mathbf{v} \rangle + b\langle \mathbf{u}, \mathbf{w} \rangle$
Conjugate symmetry	$\langle \mathbf{u}, \mathbf{v} \rangle = \langle \mathbf{v}, \mathbf{u} \rangle^*$
Positive-definiteness	$\langle \mathbf{u}, \mathbf{u} \rangle \geq 0$, with equality if and only if $\mathbf{u} = 0$

A vector space that has an inner product functionality is called an *inner product space*. The vector space that we will be using in this thesis is the space $\mathbb{C}^n$, where each vector $\mathbf{u} \in \mathbb{C}^n$ is an n-tuple of complex numbers, $\mathbf{u} = (u_1, \ldots, u_n)$. For a pair of vectors $\mathbf{u}, \mathbf{v} \in \mathbb{C}^n$, we will consider the inner product defined as:

$$\langle \mathbf{u}, \mathbf{v} \rangle = \langle (u_1, \ldots, u_n), (v_1, \ldots, v_n) \rangle = \sum_{i=1}^{n} u_i^* v_i$$

We also define the *norm* of a vector $||\cdot|| : \mathcal{V} \to \mathcal{R}$, as a function that satisfies the following requirements, $\forall\ \mathbf{u}, \mathbf{v} \in \mathcal{V}$ and $a \in \mathbb{C}$

Positive definiteness	$||\mathbf{u}|| \geq 0$, with $||\mathbf{u}|| = 0$ if and only if $\mathbf{u} = \mathbf{0}$
Absolute scalability	$||a\mathbf{u}|| = |a|\,||\mathbf{u}||$
Triangle inequality	$||\mathbf{u} + \mathbf{v}|| \leq ||\mathbf{u}|| + ||\mathbf{v}||$

There exist several types of norms in a vector space, but there is one that is naturally defined from the inner product functionality, called the *Euclidean norm*:

$$||\mathbf{u}|| = \sqrt{\langle \mathbf{u}, \mathbf{u} \rangle}$$

A vector $\mathbf{u}$ that has $||\mathbf{u}|| = 1$ is called *normalised* or *unit vector*. Two vectors $\mathbf{u}, \mathbf{v}$ are called *orthogonal* if their inner product is zero. More generally, a set of vectors $\{\mathbf{u}_i : i \in \Sigma\} \subset \mathcal{V}$ is called an *orthogonal set*, if every pair of vectors in the set indexed by Σ is mutually orthogonal, i.e. $\langle \mathbf{u}_i, \mathbf{u}_j \rangle = 0$, for every $i, j \in \Sigma$ with $i \neq j$. What is more, if the orthogonal set consists of unit vectors, it is called an *orthonormal set*. Now if this orthonormal set spans the vector space $\mathcal{V}$, meaning that every vector in $\mathcal{V}$ can be written as a combination of scalar multiplications and additions of the vectors in the orthonormal set, the set is called a *basis* of $\mathcal{V}$.

For example, a naturally defined orthonormal basis for the vector space $\mathbb{C}^n$, is given by the vector set:

$$\{\mathbf{e}(i) : i = 1, \ldots, n\}, \qquad \text{where} \quad \mathbf{e}_j(i) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$$

Suppose we have a vector $\mathbf{u} \in \mathcal{U}$ and a vector $\mathbf{v} \in \mathcal{V}$. The *tensor product* of the two vectors $\mathbf{u} \otimes \mathbf{v}$ belongs to a bigger vector space $\mathcal{U} \otimes \mathcal{V}$ that has dimension $|U| \times |V|$. The new vector space is characterised by the following properties, $\forall\ \mathbf{u}_1, \mathbf{u}_2 \in \mathcal{U}, \forall\ \mathbf{v}_1, \mathbf{v}_2 \in \mathcal{V}, \forall\ c \in \mathbb{C}$

Bilinearity	$(\mathbf{u}_1 + \mathbf{u}_2) \otimes \mathbf{v}_1 = \mathbf{u}_1 \otimes \mathbf{v}_1 + \mathbf{u}_2 \otimes \mathbf{v}_1$
	$\mathbf{u}_1 \otimes (\mathbf{v}_1 + \mathbf{v}_2) = \mathbf{u}_1 \otimes \mathbf{v}_1 + \mathbf{u}_1 \otimes \mathbf{v}_2$
Scalar multiplication	$c \cdot (\mathbf{u}_1 \otimes \mathbf{v}_1) = c \cdot \mathbf{u}_1 \otimes \mathbf{v}_1 = \mathbf{u}_1 \otimes c \cdot \mathbf{v}_1$

In order to examine operations on more than one vector spaces, we will need to introduce the notion of the *tensor product*. We can have a tensor product of several structures, like matrices, vectors or spaces. It is out of the scope of this thesis to give a rigorous mathematical definition of the tensor product, but it will be useful to examine it in the recurring example of the complex vector spaces $\mathbb{C}^{n_1}, \mathbb{C}^{n_2}$. The tensor (or *outer*) product of two vectors $\mathbf{u} \in \mathbb{C}^{n_1}, \mathbf{v} \in \mathbb{C}^{n_2}$, is equivalent to the matrix multiplication $\mathbf{u}\mathbf{v}^*$, where $\mathbf{v}^*$ is the conjugate transpose of $\mathbf{v}$:

$$\mathbf{u} \otimes \mathbf{v} = \mathbf{u}\mathbf{v}^* = \begin{bmatrix} u_1 \\ \vdots \\ u_{n_1} \end{bmatrix} [v_1^* \cdots v_{n_2}^*] = \begin{bmatrix} u_1 v_1^* & \cdots & u_1 v_{n_2}^* \\ \vdots & \ddots & \vdots \\ u_{n_1} v_1^* & \cdots & u_{n_1} v_{n_2}^* \end{bmatrix}$$

Another way to look at the outer product $\mathbf{u} \otimes \mathbf{v}$ is as a linear operator from $\mathcal{V}$ to $\mathcal{U}$. In general, linear operators can also be viewed in terms of their matrix representation. In the rest of this thesis, we will use the following notation:

A^*: the complex conjugate of matrix A,

A^T: the transpose of matrix$A$,

$A^\dagger$: the adjoint of matrix A.

An operator A is called *Hermitian* when $A = A^\dagger$. The set of Hermitian operators forms a real inner product space, with real eigenvalues for all matrices in the space. An important subset of Hermitian operators are the *positive semidefinite* operators. An $n \times n$ operator P is called positive semidefinite ($P \succeq 0$), if for any n-length vector $\mathbf{u}$, $\mathbf{u}^\dagger P \mathbf{u} \geq 0$. Positive semidefinite operators have two other important properties that will become handy:

1. $P = B^\dagger$ B, where B is an $m \times n$ matrix.

2. All eigenvalues of P are non-negative.

An operator U is called *unitary* when $UU^\dagger = U^\dagger U = \mathbb{I}$. Unitary operators preserve the inner product of vectors: $\langle U\mathbf{u}, U\mathbf{v}\rangle = \langle \mathbf{u}, \mathbf{v}\rangle$, and consequently, they preserve the Euclidean norm: $||U\mathbf{u}|| = ||\mathbf{u}||$. An important matrix norm that is widely used in quantum information, is the *trace norm* $||\cdot||_1$, given by:

$$||A||_1 = tr\left(\sqrt{A^\dagger A}\right)$$

Finally, three operators that will be used in this thesis are the *Pauli* matrices:

$$X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

so whenever in the next chapters, we say that we do an X measurement, what we will mean is that we apply the X operator on our system (vector, matrix, etc). Two equally important operators are the Hadamard transform and the identity, whose matrix representations are shown:

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad \mathbb{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

2.2 The Postulates of Quantum Mechanics

Following [34], we will examine some fundamental concepts of quantum mechanics, explaining what is a quantum system, how can we measure it to obtain information and how does it evolve in time. All this is given in the form of four postulates.

Postulate 1. *Associated to any isolated physical system is a complex vector space with inner product, known as the state space of the system. The system is completely described by its state vector, which is a unit vector in the system's state space.*

What this postulate tells us is that a quantum state is a unit vector in a specific Hilbert space[1]. In quantum mechanics, we use the *ket* notation, $|\cdot\rangle$, to indicate that a specific object is a vector in a 2-dimensional Hilbert space. Then the quantum state that describes the state of the 2-dimensional system is called a *qubit* and can be expressed as a linear combination of the spanning set of the vector space, what we usually refer to as a *superposition*.

[1]For finite dimension spaces, which will be the only ones we will study in this thesis, a Hilbert space is the same as a complex vector space with inner product.

If we consider a specific orthonormal basis for the vector space composed of vectors $|0\rangle$ and $|1\rangle$, called the *computational basis*, we can write a qubit $|\Psi\rangle$ in the form:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

with $\alpha, \beta \in \mathbb{C}$. Since we consider $|\Psi\rangle$ to be a unit vector in Hilbert space $\mathcal{H}$, it holds that $|\alpha|^2 + |\beta|^2 = 1$. It also holds that $\langle\Psi|\Psi\rangle = 1$, where $\langle\Psi|$ is the dual vector of $|\Psi\rangle$ known as *bra*.

In the same way as in the 2-dimensional Hilbert space, we can describe any finite k-dimensional Hilbert space using basis vectors $\{|0\rangle, ..., |d-1\rangle\}$. Any linear combination of the basis vectors $\sum_j \alpha_j|j\rangle$ is called a *superposition* of the vectors $|j\rangle$, $j = \{0, ..., d-1\}$, with *amplitude* α_j for state $|j\rangle$.

Postulate 2. *The evolution of a closed quantum system is described by a unitary transformation. That is, the state $|\Psi\rangle$ of the system at time t is related to the state $|\Psi'\rangle$ of the system at time t' by a unitary operator U which depends only on the times t and t',*

$$|\Psi'\rangle = U|\Psi\rangle.$$

The time evolution of the state $|\Psi\rangle$ can also be described for continuous time by the *Schrödinger equation*.

Postulate 3. *Quantum measurements are described by a collection $\{M_m\}$ of* measurement operators. *These are operators acting on the state space of the system being measured. The index m refers to the measurement outcomes that may occur in the experiment. If the state of the quantum system is $|\Psi\rangle$ immediately before the measurement then the probability that result m occurs is given by*

$$p(m) = \langle\Psi|M_m^\dagger M_m|\Psi\rangle$$

and the state of the system after the measurement is $\frac{M_m|\Psi\rangle}{\sqrt{p(m)}}$. The measurement

operators satisfy the completeness equation

$$\sum_m M_m^\dagger M_m = \mathbb{I}.$$

The above postulate can be reformulated in order to only contain the positive operators $E_m = M_m^\dagger M_m$. The complete set of the operators $\{E_m\}$ is known as a *POVM measurement*, where POVM stands for 'Positive Operator-Valued Measure'.

Finally, an important special case of general measurements is the *projective measurement*, described by a set of projectors P_m, each corresponding to a possible measurement outcome m. Projectors follow the orthogonality condition $P_m P_{m'} = \delta_{m,m'} P_m$, where $\delta_{i,j} = 1$ when $i = j$ and 0 otherwise, and they also satisfy the completeness equation $\sum_m P_m = I$. We can associate the complete set of projectors $\{P_m\}$ to a Hermitian (i.e. self-adjoint) operator M on the space of the observed system, called *observable*,

$$M = \sum_m m P_m$$

For every possible measurement outcome, we can use orthogonal vectors $|\mu_m\rangle$ such that $P_m = |\mu_m\rangle\langle\mu_m|$ and $M|\mu_m\rangle = m|\mu_m\rangle$. We say that m is an *eigenvalue* of M associated with projector P_m. Then, by postulate 3, given a state $|\Psi\rangle$, the probability that result m occurs in given by

$$\Pr[m] = \langle\Psi|P_m|\Psi\rangle$$

and the state of the system after the measurement is $\frac{P_m|\Psi\rangle}{\sqrt{\Pr[m]}}$.

Postulate 4. *The state space of a composite physical system is the tensor product of the state spaces of the component physical systems. Moreover, if we have systems numbered 1 through n, and system number i is prepared in the state $|\Psi_i\rangle$, the joint state of the total system is $|\Psi_1\rangle \otimes \cdots \otimes |\Psi_n\rangle$.*

The above postulates hold not only for pure states, i.e. states of the form $|\Psi\rangle$. They also hold for *mixed states*, that is, quantum systems that are in a pure state $|\Psi_i\rangle$ with probability p_i. We can describe this ensemble of states $\{p_i, |\Psi_i\rangle\}$ using the *density operator* formalism:

$$\rho = \sum_i p_i |\Psi_i\rangle\langle\Psi_i|$$

A system described by a density matrix ρ evolves according to the unitary operator U as follows:

$$\rho' = U\rho U^\dagger = \sum_i p_i U|\Psi_i\rangle\langle\Psi_i|U^\dagger$$

What is more, if that system is measured using measurement operators $\{M_m\}$, then the probability to get outcome m is:

$$\Pr[m] = \sum_i p_i \mathrm{tr}(M_m^\dagger M_m |\Psi_i\rangle\langle\Psi_i|) = \mathrm{tr}(M_m^\dagger M_m \rho)$$

and the state after the outcome m, is

$$\rho_m = \frac{M_m \rho M_m^\dagger}{\mathrm{tr}(M_m^\dagger M_m \rho)}$$

2.3 Entanglement

We call a pure state of two or more quantum systems *entangled*, when it cannot be expressed as a tensor product of the states of the different systems. In the bipartite case for example, where the Hilbert space of the whole system is the tensor product of the two Hilbert spaces, a state $|\Psi\rangle$ is entangled if it cannot be written in the form $|\Psi_1\rangle \otimes |\Psi_2\rangle$. More generally, a bipartite entangled state with density matrix ρ_{AB}, cannot be written in the form:

$$\rho = \sum_i p_i \rho_A^i \otimes \rho_B^i \tag{2.1}$$

where p_i are positive numbers in $[0, 1]$ representing probabilities, and ρ_A^i, ρ_B^i are physical states in the systems A and B respectively. A state of the form 2.1 is called *biseparable*.

Entangled physical systems were first discussed in the famous paper by Einstein, Podolsky and Rosen [1], even though the term entanglement was used by Schrödinger one year later. Described as "spooky action at a distance", the EPR paradox states the following: Consider two parties, Alice and Bob, that are separated by great distance. Before they got separated, each of the two parties got a share (one qubit) of the entangled bipartite state $|\Phi^+\rangle = (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)/\sqrt{2}$. When Alice measures her qubit in the *computational basis*, defined by vectors $\{|0\rangle, |1\rangle\}$, and observes one of the two outcomes, Bob's qubit will also collapse into the same state as Alice's qubit, even though they are very far away from each other.

This counterintuitive logical problem troubled scientists for decades, since it seemed that, in order to incorporate this paradoxical behavior in a complete description of physical reality, one needs to abandon specific features of classical physics, like *local realism*, that were intuitively widely accepted as true. Local realism consists of two principles:

Realism – Objects in a system have predetermined values for all measurements, before those measurements happen.

Locality – An event on one site cannot instantaneously affect the value of another object that is at a distant location.

In 1964, John Bell [2] provided a more rigorous mathematical description, showing that the predictions of quantum mechanical theory cannot be reproduced by any local-realistic theory. The correlations between any local hidden variables can be shown to satisfy specific contraints (known as *Bell Inequalities*), that can nevertheless be violated by correlations between quantum systems. The most well-known inequality of this type is the CHSH Inequality (named after Clauser, Horne, Shimony and Holt, the authors of [25]), which bounds the classical correlations between two parties, Alice and Bob, as follows:

$$|\mathbb{E}(a,b)+\mathbb{E}(a',b)+\mathbb{E}(a,b')-\mathbb{E}(a',b')| \leq 2 \tag{2.2}$$

Here, Alice measures one of two observables a and a', and Bob measures b or b' respectively. All observables take values in $\{-1,+1\}$. $\mathbb{E}(i,j)$ is the expectation value of the measurement of observable i for Alice and j for Bob respectively:

$$\mathbb{E}(i,j) = \Pr[i=j]-\Pr[i\neq j]$$

Entanglement is used to achieve tasks that are otherwise impossible with purely classical means. Such examples are quantum teleportation and superdense coding. It is also used in order to violate Bell Inequalities like the one in Eq. 2.2. However, the quantum advantage provided by entanglement is also bounded. For example, the quantum bound for equation 2.2 (discovered by Boris Tsirelson [36]) is equal to $2\sqrt{2}$.

Recent research has been focused on models of computation [20] that use entanglement as a resource, in order to do several computational tasks such as Blind-Computing [19] and Secret Sharing [37]. In the following paragraphs we will examine how entanglement helps to win games with higher probability than is classically possible. We will then use these results in subsequent Chapters, in order to provide an entanglement verification test for cryptographic scenarios (Chapter 4) and to examine Bayesian Games between entangled players (Chapter 5).

2.3.1 The CHSH Game

The first example of a game where quantum mechanics provides a higher winning probability than classically achievable, is the CHSH game. We have two non-communicating parties, Alice and Bob and a Referee who communicates with both parties. The Referee chooses randomly a pair of bits (s,t) from $\{0,1\}$ and sends s to Alice and t to Bob. The parties then reply to the referee with one bit each, Alice sending a and Bob b. The predicate of the game is:

$$V(a,b|s,t) = \begin{cases} 1 & \text{if } a \oplus b = s \wedge t, \\ 0 & \text{otherwise.} \end{cases}$$

After many repetitions, the Referee computes the value of the game according to the inputs and outputs of the two parties:

$$\omega^{CHSH} = \frac{1}{4} \sum_{a,b,s,t} \Pr[a,b|s,t] \times V(a,b|s,t)$$

The *classical value* of the CHSH game can always be obtained using some deterministic functions of getting a and b from s and t respectively[2]. We will denote this maximum value that results from any purely classical strategy, as ω_c. It is not difficult to verify that:

$$\omega_c^{CHSH} = 3/4$$

Now if we consider that Alice and Bob share the entangled state $|\Phi^+\rangle = (|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B)/\sqrt{2}$, a quantum strategy for the two parties consists of a pair of measurement operators that depend on the pair of inputs (s,t). More specifically, we can think of Alice and Bob's measurements as a collection of positive semidefinite 2×2 matrices $\{X_s^a\}$ and $\{Y_t^b\}$, such that for every input pair (s,t):

$$\sum_{a \in \{0,1\}} X_s^a = \mathbb{I} \quad \text{and} \quad \sum_{b \in \{0,1\}} Y_t^b = \mathbb{I}$$

Then, the probability to output a and b, given s and t, is given by the postulates of quantum mechanics:

$$\Pr[a,b|s,t] = \langle \Phi^+ | X_s^a \otimes Y_t^b | \Phi^+ \rangle \tag{2.3}$$

In [28], a collection of optimal measurements for Alice and Bob is presented, that

[2] since any probabilistic strategy is a convex combination of deterministic strategies, and therefore there exists one deterministic strategy that maximizes the value of the game.

provides the optimal value for the CHSH game, derived from Tsirelson's Inequality [36]:

$$\omega_q^{CHSH} = \cos^2(\frac{\pi}{8}) \geq 3/4$$

We therefore see how sharing an entangled state like $|\Phi^+\rangle$, helps two parties apply a quantum strategy that outperforms any classical one for the CHSH game. In [28], we can find more examples of games, where sharing e-bits helps the parties win with higher probabilities than classically possible. However, all these games cannot be won with probability one. In the next paragraph, we will examine how, by increasing the number of parties, we can win a quantum game with certainty.

2.3.2 The Mermin-GHZ Game

Let us consider three non-communicating parties, Alice, Bob and Charlie. A Referee sends to each one of them an input bit, s,t and u for Alice, Bob and Charlie respectively. We have the following promise on the inputs:

$$s + t + u = 0 \pmod 2 \tag{2.4}$$

The parties then need to reply to the Referre with one bit each, a, b and c for Alice, Bob and Charlie respectively. The predicate of the game is:

$$V(a,b,c|s,t,u) = \begin{cases} 1 & \text{if } a \oplus b \oplus c = \frac{s+t+u}{2} \pmod 2, \\ 0 & \text{otherwise.} \end{cases}$$

The different combinations of inputs and outputs that win the game are summarized in the following table:

s	t	u	$a \oplus b \oplus c$
0	0	0	0
0	1	1	1
1	0	1	1
1	1	0	1

$$\Longrightarrow \qquad V(a,b,c|s,t,u) = 1$$

Note that the predicate does not directly depend on all three inputs, since the promise determines one of the inputs, given the other two. The Referee, after repeating the game many times and gathering all output bits, computes the value of the game:

$$\omega^{GHZ} = \frac{1}{4}\sum \Pr[a,b,c|s,t,u] \times V(a,b,c|s,t,u)$$

where the sum is over all inputs and outputs and we also suppose that the four eligible combinations of inputs are selected with equal probability 1/4. Mermin demonstrated a simple *gedanken* experiment [38] to prove that only three out of the four different combinations of inputs and outputs can be true given only classical information, therefore the classical value of the game is:

$$\omega_c^{GHZ} = 3/4$$

Let us now consider the case where the players are allowed to share an entangled state before the beginning of the protocol. Suppose that each party has a qubit of the 3-party GHZ state [17]:

$$|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$$

Whenever a player gets as input 0, he/she measures in the X basis:

$$\{x_+, x_-\} = \{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$$

and when a player gets as input 1, he/she measures in the Y basis:

$$\{y_+, y_-\} = \{\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}$$

We can express the GHZ state in four different ways, according to each eligible combination of inputs:

$$000 \longrightarrow |GHZ\rangle = \tfrac{1}{2}\big(|x_+x_+x_+\rangle + |x_+x_-x_-\rangle + |x_-x_+x_-\rangle + |x_-x_-x_+\rangle\big)$$

$$011 \longrightarrow |GHZ\rangle = \tfrac{1}{2}\big(|x_+y_+y_-\rangle + |x_+y_+y_-\rangle + |x_-y_+y_+\rangle + |x_-y_-y_-\rangle\big)$$

$$101 \longrightarrow |GHZ\rangle = \tfrac{1}{2}\big(|y_+x_+y_-\rangle + |y_+x_+y_-\rangle + |y_-x_+y_+\rangle + |y_-x_-y_-\rangle\big)$$

$$110 \longrightarrow |GHZ\rangle = \tfrac{1}{2}\big(|y_+y_+x_-\rangle + |y_+y_+x_-\rangle + |y_-y_+x_+\rangle + |y_-y_-x_-\rangle\big)$$

It is not difficult to observe that for all sets of possible inputs (s,t,u), such that $s \oplus t \oplus u = 0$, the players can always output combinations of bits (a,b,c) that always pass the test, i.e. the predicate of the game $V(a,b,c|s,t,u)$ will always be equal to 1. We therefore have:

$$\omega_q^{GHZ} = 1$$

which not only is better than any classical strategy could achieve, but is no longer probabilistic (i.e. the players will win the game everytime).

2.4 Cryptography

Cryptography is the art of securing *communication* or *computation* between two or more parties who may or may not trust one another [34]. Throughout the centuries, people have used many different cryptographic schemes, from the ancient-greek scytale, to the Caesar cipher and the modern-age Enigma machines. However, building cryptographic schemes that are secure against all types of malicious activity is not easily achievable. Since in general, we cannot assume that the adversaries will adopt specific strategies, the only assumption that we need to base our schemes upon, is their *computational power*. While many classical cryptographic schemes are based on the computational hardness of solving specific problems, quantum mechanics holds the promise of providing *information theoretic* security, meaning that the security only relies on the quantum mechanical laws and not on an assumption on the computational power of the adversary.

One of the earliest results in Quantum Cryptography was proposed by Bennett and Brassard [5]. Known as BB84, it comprised of a quantum key distribution protocol, whose security lies in the creation and sharing of non-orthogonal quantum states. Due to the *no cloning* theorem, any malicious activity from an eavesdropper can be detected and the security of the key is guaranteed. The pioneering work in BB84 marked the beginning of a new era in cryptography and information theory. Even though at first there was a lot of optimism about providing security for all cryptographic primitives, soon this would prove to be incorrect, due to the no-go theorems for bit commitment by Lo and Chau [11] and Mayers [10]. However, as we will see in more detail in the next Chapter, quantum mechanics can still provide security for many cryptographic functionalities, that is better than what can be classically achieved.

2.4.1 One-way Functions

Classical cryptographic schemes are based on the difficulty of solving specific problems. This difficulty is captured by the notion of *one-way functions*, which are functions that are easy to compute, but hard to invert[3]. The existence of one-way functions is conjectured but not proven, and it would imply that $\mathcal{P} \neq \mathcal{NP}$. The most well known candidate for one-way functions is integer factorization, but there exist many others, such as the subset-sum and the discrete exponential functions. The difficulty of inverting one-way

[3]When we say that a function f is *hard to invert*, we mean that any probabilistic polynomial-time algorithm, trying to find $f^{-1}(y)$ from some randomly chosen input y, succeeds with negligible probability on the length of the input y.

functions is the basis for some of the most widely-used schemes in cryptography, such as pseudorandom generators, bit commitment and digital signatures.

However, given a random y, it might still be possible to extract some partial information about $f^{-1}(y)$, where f is a one-way function. Fortunately, according to [9], we can construct one-way functions that hide specific partial information about their pre-images. This partial information can be viewed as the "hard-core" of the difficulty of inverting f. More specifically, a polynomial-time computable function $b : \{0,1\}^* \rightarrow \{0,1\}$ is called a *hardcore predicate* of a function f, if no efficient algorithm, when given $f(x)$, can guess $b(x)$ with success probability that is (more than negligibly) better than one-half.

In the quantum world, Shor's algorithm can be used to factor any large integer in polynomial time, thus breaking any cryptosystem that is based on integer factoring (e.g. RSA). We therefore need to be very careful when we consider computationally bounded quantum devices, in order to use one-way functions that are secure against quantum adversaries. Candidates for *quantum one-way* functions could come from conjectured hard problems such as Graph Non-Isomorphism and Approximate Closest Lattice Vector. More generally, in [39] it is shown that any hard instance of Circuit Quantum Sampling could be transformed in a quantum one-way function.

2.4.2 Bit Commitment and No-go Theorems

A bit commitment scheme is a two-party protocol that is used in order for one party (the Sender) to commit himself towards another party (the Receiver) to a specific bit value. It comprises of two phases, the *Commit* and the *Reveal* phase, and has to be:

1. Concealing – At the end of the *Commit* phase, the Receiver does not obtain any knowledge of the Sender's bit value.

2. Binding – At the end of the *Reveal* phase, and given all communication transactions between the two parties, there exists at most one value that the Receiver accepts as a valid "opening" of the commitment.

Bit Commitment schemes play an important role in multiparty computation, since they allow to construct *Zero-Knowledge* and *Coin Flipping* protocols and are therefore essential for any type of *Secure Function Evaluation* (see [9] for an extensive study of multiparty computation). Bit commitment schemes are constructed from one-way functions, and consequently their security also relies on the existence of such functions.

It is well known that a classical Bit Commitment scheme cannot be perfectly concealing and perfectly binding at the same time. One of the two parties needs to be computationally bounded, in order for a perfect classical Bit Commitment scheme to be possible. At the dawn of the Quantum Cryptography era, researchers were confident that quantum mechanical effects could be used to strengthen Bit Commitment, and provide a protocol

with information-theoretic security. Unfortunately, this was proven to be impossible, due to the *no-go theorems* (as they are now known) by Lo and Chau [11] and Mayers [10]. Loosely speaking, the reason why Quantum Bit Commitment is impossible, is because any protocol that is perfectly concealing, needs to associate each of two indistinguishable quantum states, i.e. that have the same density matrix, with one of the two values of the bit. Using the Gram-Schmidt decomposition, the Sender can then perform some local operation on his share of an entangled state, in order to transform the state associated to the bit value 0, to the state associated to the bit value 1 (and vice versa), and therefore break the binding condition.

However, it is possible to have an information-theoretically secure Quantum Bit Commitment protocol that is partially binding and partially concealing, i.e. the Receiver learns the committed bit before the Reveal phase with bounded probability P_R, and the Sender can reveal any value at the Reveal phase and the Receiver will accept it with bounded probability P_S [40]. We already mentioned that Bit Commitment is a fundamental cryptographic primitive that can be used to construct other protocols like Coin Flipping. In Chapter 3, we will analyse a specific type of *generalised BB84* Bit Commitment protocols [41] and examine how to enhance them in order to propose a Quantum Coin Flipping Protocol that is partially binding and partially concealing against a computationally unbounded player.

2.5 Experimental Tools

When we want to experimentally demonstrate a quantum communication protocol, we are mostly interested in photon implementations, because they are ideal for carrying information for long distances. Such implementations are very robust, demonstrating low error and loss rates. Information can be encoded in different ways, using photons as the carrier; here we will briefly describe two of them, polarisation and phase encoding.

2.5.1 Polarisation Encoding

When Charles Bennett and Gilles Brassard introduced the idea of using quantum states to distribute cryptographic keys in 1984, they proposed to use non-orthogonal states of *polarised* photons. In their setup, the photons are polarised either rectilinearly or diagonally in one of four states $|\updownarrow\rangle, |\leftrightarrow\rangle, |\nearrow\rangle, |\nwarrow\rangle$. These states can be obtained by combining *half-wave* or *quarter-wave* plates to "rotate" the polarisation direction of the beam of particles. The receiver of the photons then needs to use a *Polarisation Beamsplitter* (PBS) to split the beam in two orthogonal components according to their polarisation and to detect each of them by one detector.

Beamsplitters (BS) are another important ingredient of most basic experiments in

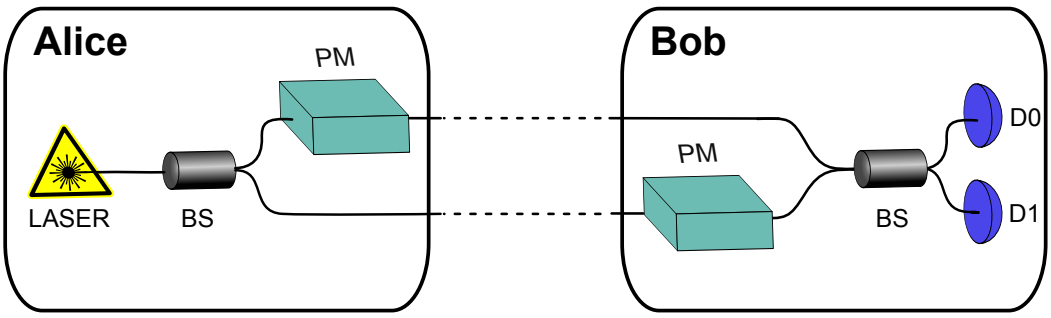


Figure 2.1: The extended Mach Zehnder Interferometer

quantum information. A 50/50 beamsplitter "splits" a beam of particles in two, where with 50% probability a particle will get transmitted and with 50% probability it will get reflected. The action of a 50/50 beamsplitter is described by the Hadamard transform, taking a qubit in superposition:

$$|q\rangle = \alpha|0\rangle + \beta|1\rangle$$

to the state:

$$|q'\rangle = H|q\rangle = \frac{1}{\sqrt{2}}(\alpha+\beta)|0\rangle + \frac{1}{\sqrt{2}}(\alpha-\beta)|1\rangle$$

A particularly interesting quantum phenomenon, *single-particle interference*, can be observed when we use two beamsplitters sequentially on the state $|0\rangle$ [42]. This is equivalent to doing a Hadamard transformation twice; since the Hadamard matrix is unitary and Hermitian, the operation has no effect on the state: $HH|0\rangle = |0\rangle$.

2.5.2 Phase Encoding

Even though polarisation encoding can be used in free-space implementations, it is less suitable for other types of experiments, like fibre implementations, due to birefringence, which causes random polarisation fluctuations. We can instead use another way of encoding information, through phase. *Phase encoding* can be better understood by examining an extended Mach-Zehnder (MZ) interferometer. As shown in Fig. 2.1, an extended MZ interferometer contains a Laser source, two detectors, two *Phase Modulators* (PM) and two Beamsplitters (BM). A PM is used by Alice to encode information on a particle by applying a phase to it. 0 and π phases correspond to the computational basis, with 0 phase corresponding to bit 0 and π to bit 1, while $\pi/2$ and $3\pi/2$ phases correspond to the Hadamard basis, with $\pi/2$ corresponding to bit 0 and $3\pi/2$ to bit 1.

Bob then uses the second PM to choose his measurement basis; 0 phase for computational basis and $\pi/2$ phase for Hadamard. If the bases agree, then we can observe

either constructive or destructive interference on the BM, depending on the encoded bit. When both Alice and Bob apply a 0 phase or a $\pi/2$ phase then we have constructive interference, and the particle arrives at Detector 0 (D0). When Alice applies a π phase and Bob a 0 phase (or Alice applies a $3\pi/2$ phase and Bob a $\pi/2$ phase), then we have destructive interference and the particle arrives at Detector 1 (D1). When the bases disagree, the detection events of the detectors are random.

One of the most frequent implementation errors when using polarisation encoding, is a misalignment in Bob's beamsplitter. In order to have low error rates in standard one-way communication implementations, like Fig 2.1, we need to have continuous polarisation control and alignment in the system. This can be avoided if we use a "plug&play" system [43] like the one we will introduce in Chapter 3. The difference with this system is that the laser source is not situated at Alice's side, but at Bob's, and the light gets reflected by Alice using a Faraday mirror. This causes any changes done on the way to the mirror, to be reversed on the way back to Bob.

Chapter 3

Coin Flipping

3.1 Introduction

Quantum communication holds the promise of achieving a security level that is impossible to reach by purely classical means. Indeed, information-theoretic security has been demonstrated for the cryptographic task of distributing a secret key between two trusted and collaborating communicating parties using systems exploiting quantum effects [44]. However, many advanced cryptographic schemes belong to a model where the two parties do not trust each other and hence cannot collaborate. In the previous Chapter, we have introduced a fundamental primitive of the non-collaborative model, bit commitment. In this Chapter, we will focus on coin flipping, a primitive where two distrustful parties, Alice and Bob, are separated by distance and wish to agree on a random bit.

In general, there exist two types of coin flipping: *strong* coin flipping, where the players wish to share a random bit without caring for a specific outcome, and *weak* coin flipping, where each player has a preference for one of the two values of the bit. An honest party would like the outcome of a coin flipping protocol to be a random bit. On the other hand, a cheating party will try to bias the coin to take a specific value. We define the cheating probabilities p^A and p^B for Alice and Bob respectively, as the maximum probability of biasing the coin c towards one of the two values:

$$\begin{aligned} p^A &= \max_A\{\Pr[c=0], \Pr[c=1]\} \leq \frac{1}{2} + \epsilon \\ p^B &= \max_B\{\Pr[c=0], \Pr[c=1]\} \leq \frac{1}{2} + \epsilon \end{aligned}$$

We also define $p = \max\{p^A, p^B\}$ to be the overall cheating probability of a coin flipping protocol and ϵ to be the *bias*. When $p^A = p^B$, the coin flipping protocol is called *fair*.

Blum [45] introduced the first coin flipping protocol in 1981. This protocol was

asynchronous, in the sense that the two players do not simultaneously exchange messages but rather communicate with each other in rounds. In the asynchronous classical model, it is impossible to have a coin-flipping protocol with cheating probability less than 1, unless computational assumptions are considered (for example the existence of one-way functions). In other words, a computationally unbounded dishonest player can always force the outcome of the coin flip with probability 1. On the other hand, in the *synchronous* (or *relativistic*) classical model [46], unconditionally secure coin flipping is possible, but the model itself is hard to implement because the security lies solely on the simultaneity of the communication and thus the verification of the distance between the two players.

In the quantum model, where the two parties share a quantum channel, the initial results for unconditionally secure coin flipping were discouraging. Due to the no-go theorems for bit commitment [10, 11], it is impossible to achieve unconditional perfect security for quantum coin flipping protocols that are based on bit-commitment. On the other hand, several quantum protocols have been proposed that achieve a cheating probability lower than 1. Aharonov et al. proposed the first such protocol [41], and other protocols followed [47–50] that nevertheless could not go below the cheating probability bound of 3/4. At the same time, Kitaev [51], using semi-definite programming, proved that the cheating probability of any fair quantum coin flipping protocol is at least $1/\sqrt{2}$. Finally Chailloux and Kerenidis [52], using Mochon's result [53, 54] for *weak* coin flipping with arbitrarily small bias, bridged the gap by presenting a protocol that has cheating probability arbitrarily close to $1/\sqrt{2}$.

These results are important from a theoretical point of view, however they assume perfect implementation of the protocols. The situation is more subtle when we consider the imperfections that naturally appear in practical devices, since if taken into account they may render some of the above-mentioned protocols completely unsecure in practice. For photonic systems, which constitute the chosen architecture for quantum communications, imperfections typically appear in the form of losses in the channel and measurement apparatus, and errors in the different implementation stages. Furthermore, systems suitable for long-distance communications over fiber-optic channels usually employ coherent light sources, thus becoming vulnerable to attacks exploiting the non-deterministic photon emission inherent in such sources [55].

Some of the aforementioned practical issues have been addressed in recent theoretical and experimental studies. An analysis of the problem of *loss tolerance*, i.e., the tolerance to photon losses at any communication distance, provided an elegant solution [14], which however did not account for the presence of multi-photon pulses in coherent light source implementations. The relatively high cheating probability of 0.9 achieved by this protocol was slightly reduced in subsequent work [56, 57]. As a way to account for errors and thus retain a zero abort probability when both players are honest, researchers

proposed the related primitive of bit string generation [58–60].

The first coin flipping implementation concerned a protocol that becomes insecure for any loss [61], while a consequent promising solution [62] gave results that unfortunately cannot be used in realistic conditions. More recently, an implementation of the loss-tolerant protocol of [14], used an entangled-photon source to eliminate the problem of multi-photon pulses [15]. This was the first experiment that demonstrated an advantage of quantum over classical communication for coin flipping in the presence of losses and errors. However, although in principle the cheating probability bound in the implemented protocol is independent of losses, because of errors in the implementation, a gain was only shown for a distance of a few meters.

It is worthwhile noting that the closely related primitives of quantum bit commitment and oblivious transfer were experimentally demonstrated in a bounded model called the *noisy storage* model, where adversaries have access to an imperfect quantum memory [63, 64]. However, these protocols do not offer security against all-powerful adversaries. Finally, quantum bit commitment with relativistic constraints was also recently implemented [65].

The rest of the Chapter will be organised as follows: In Section 3.2, we will present previous research on coin flipping and study the advantages and vulnerabilities of the proposed protocols. In Section 3.3, we will explain the novelty of our work, and present an easily implementable coin flipping protocol that takes into account imperfections such as losses and noise, that are common in fiber optics experiments. In Section 3.4, we lay out the experimental details of the plug&play system and the modifications necessary to be able to implement our coin flipping protocol. Section 3.5 contains a basic security analysis of the coin flipping protocol, when one of the two players is dishonest, while Section 3.6 shows how to enhance the previous security proofs in order to take into account the specific particularities and imperfections of our plug&play system. In Section 3.7 we present the experimental results from the implementation of our protocol using a commercial plug&play system. Finally in Section 3.8 we propose ways to enhance the security of quantum coin flipping protocols, when the capabilities of the adversary are potentially bounded by physical or computational assumptions, and in Section 3.9 we sum up our contribution to the field, and discuss the limitations of the specific setting as well as ways to deal with potential security loopholes.

3.2 Previous Work

In the seminal paper of Charles Bennett and Gilles Brassard [5], the first Quantum Coin Flipping protocol was presented, using quantum states $|\Psi_{\alpha,c}\rangle$ that have since been refered

to as the BB84 states:

$$|\Psi_{0,0}\rangle = |0\rangle, \quad |\Psi_{0,1}\rangle = |1\rangle$$
$$|\Psi_{1,0}\rangle = |+\rangle, \quad |\Psi_{1,1}\rangle = |-\rangle$$

BB84 Protocol (Simplified)

1. Alice picks at random one of the four BB84 states $|\Psi_{\alpha,c}\rangle$ and sends it to Bob.
2. Bob chooses randomly a basis $\beta \in \{0,1\}$ and measures in $\{|\Psi_{\beta,0}\rangle, |\Psi_{\beta,1}\rangle\}$.
3. Bob chooses a random bit $b \in \{0,1\}$and sends it to Alice.
4. Alice replies with the basis α and the bit c that she used to form the state.
5. If the bases agree ($\alpha = \beta$), Bob checks that his measurement outcome is equal to c. If they are equal or if $\alpha \neq \beta$, the value of the coin is $\alpha \oplus b$.

There is an obvious problem with this protocol that was already mentioned in the original paper: the two density matrices used by Alice to commit to the two values of α are equal. We have seen in Section 2.4 that the no-go theorems for bit commitment dictate that whenever a protocol is perfectly concealing (i.e. the density matrices for the two bits are equal), it is not binding for the sender. Thus, Alice can always cheat by sending half of an EPR pair to Bob, and then waiting for his bit b to appropriately transform her state in order to convince Bob for the correctness of the protocol.

It is therefore clear that whenever the density matrices corresponding to the two different values of the bit, are equal, we can not have any security for a coin flipping protocol, since the cheating probability of one of the players will always be 1.

The first quantum coin flipping protocol with a cheating probability smaller than 1 for unbounded malicious parties was proposed in [41]. The protocol is based on a *generalised BB84* bit commitment scheme, meaning that the states $|\Psi_{\alpha,c}\rangle$ used are similar to the states of the BB84 protocol, but rotated by an angle θ:

$$|\Psi_{0,0}\rangle = \cos\theta|0\rangle - \sin\theta|1\rangle, \quad |\Psi_{0,1}\rangle = \sin\theta|0\rangle + \cos\theta|1\rangle$$
$$|\Psi_{1,0}\rangle = \cos\theta|0\rangle + \sin\theta|1\rangle, \quad |\Psi_{1,1}\rangle = \sin\theta|0\rangle - \cos\theta|1\rangle$$

Aharonov *et al.* Protocol

1. Alice picks at random one of the four rotated BB84 states $|\Psi_{\alpha,c}\rangle$ and sends it to Bob.
2. Bob stores the state in a quantum memory and sends a random bit $b \in \{0,1\}$ to Alice.
3. Alice replies with the basis α and the bit c that she used to form the state.
4. Bob measures in the basis α and checks if his measurement outcome is equal to c. If they are not equal, he aborts, else, the value of the coin is $c \oplus b$.

The novelty of this protocol is that even though it is similar to the BB84 protocol, it differs in two very important aspects. First, the value of the final coin is not $\alpha \oplus b$, but instead $c \oplus b$. This difference in the last step of the protocol (using bit c instead of the basis a to construct the coin), makes the density matrices for the two values of the committed bit, unequal:

$$\rho_0 = \tfrac{1}{2}|\Psi_{0,0}\rangle\langle\Psi_{0,0}| + \tfrac{1}{2}|\Psi_{1,0}\rangle\langle\Psi_{1,0}| = \begin{bmatrix} \cos^2\theta & 0 \\ 0 & \sin^2\theta \end{bmatrix}$$

$$\rho_1 = \tfrac{1}{2}|\Psi_{0,1}\rangle\langle\Psi_{0,1}| + \tfrac{1}{2}|\Psi_{1,1}\rangle\langle\Psi_{1,1}| = \begin{bmatrix} \sin^2\theta & 0 \\ 0 & \cos^2\theta \end{bmatrix}$$

Second, the authors tried to minimize Alice's cheating probability, by not allowing measurements in different bases (since Bob waits to measure till after he has received the basis α). The bounds of the cheating probabilities computed in the paper are not tight, giving a total protocol bias $\epsilon = 0.42$.

In subsequent work, Robert Spekkens and Terry Rudolph [66] observed that these specific sets of states associated with the two different values of bit c correspond to two parallel chords on the Bloch sphere. They proved that Alice does not gain anything by submitting an entangled state, and can therefore attain her optimal cheating probability by sending either of the states $|+\rangle$ or $|-\rangle$. Furthermore, they improved the cheating probability bounds for Aharonov et al. protocol, by proving that with the right choice of angle $\theta = \pi/8$, the protocol is fair, with cheating probability[1]:

$$p_q = \frac{1}{2} + \frac{1}{2\sqrt{2}}$$

[1]When the protocol is quantum, we will denore the cheating probability by p_q, while when the protocol is classical, we will denote it by p_c.

which gives bias around 0.3536, smaller than 0.42. The problem with this protocol is that it is not tolerant to losses, because Bob has to wait till Alice reveals her basis and bit, in order to perform his measurement. Whenever he is not happy with the bit c , he can declare that he lost his state and ask for a repetition, until he is happy with Alice's choice. Unless there is a way for Bob to perform quantum non-demolition measurements in order to anounce that he received a state, without in any way disturbing it, in its current form this protocol is not appropriate for use in any implementation, since there will always be losses that will need to be taken into account.

Berlin et al [14] proposed an ingenious protocol that combines the BB84 protocol's sequence of events with the states used by Aharonov et al. Their protocol is completely loss-tolerant, to the expense of a higher cheating probability equal to 90%. Since our protocol is a modification of [14], we will not present it individually, but incorporate their security analysis in our proofs in the next Sections. The main problem with the Berlin et al. protocol, which was the motivation of part of the work in this thesis, is that it requires a single-photon source, which is not easy to build. If we were to use an attenuated laser source, as is common to most optical experiments, Bob would be able to perfectly cheat, using a pulse with two or more photons. The reason is that there exists a conclusive measurement that he can do, to distringuish between two-photon pulses formed with bit 0 and bit 1. Due to the loss-tolerance property, he could ask for repetitions of the protocol till he gets a 2-photon pulse that leads him to a correct conclusive measurement of Alice's bit. To overcome this problem, in a follow-up implementation of this scheme [15], an entangled source is used to perform coin flips, beating the classical bounds for 10m, but not being able to demonstrate a quantum advantage for 12km.

3.3 Our work

The goal is to provide a complete theoretical and experimental framework for the implementation of quantum coin flipping in practical communication scenarios. The protocol that we consider takes standard experimental imperfections (multi-photon emission, transmission loss, detector inefficiency and dark counts) into account. We show that our protocol can be combined with protocols that achieve almost perfect security, i.e., a bias asymptotically close to zero, against adversaries with bounded resources. More explicitly, if the adversary is bounded, then the protocol guarantees almost perfect security, while in the case of an all-powerful adversary, the protocol still guarantees a security level strictly higher than classically possible. Providing security against adversaries of varying complexity is of great importance in the context of current communication networks, where technological and computational capabilities can evolve very rapidly. Furthermore, we experimentally implement the protocol using a practical plug&play system, developed by significantly enhancing a commercial quantum key distribution (QKD) device

[12, 13]. The key element of our implementation is that we take a realistic approach: to account for the unavoidable errors in the system and for coherent light source emission statistics, we allow for a non-zero but small probability of abort when both parties are honest, and accept the dependence of the cheating probability on communication loss thus departing from absolute loss tolerance. This constitutes an important change with respect to previous protocols [14, 15] and leads to a gain of three orders of magnitude in communication distance. Indeed, using a security analysis pertaining to our implementation and an appropriate benchmark for classical coin flipping protocols [16], we can rigorously quantify the advantage offered by quantum communication as a function of distance, much in the way that the secret key fraction is calculated in practical QKD implementations [44]. In this way, we demonstrate a clear advantage for quantum coin flipping with information-theoretic security, at a communication distance suitable for metropolitan area network communications, with a system that can readily be deployed in such networks.

We emphasize that dealing with distrustful parties is more complicated than the quantum key distribution scenario, both in theory and in practice. For example, although randomized procedures like error correction and privacy amplification that are widely employed in QKD have been used in the security analysis of protocols dealing with bounded adversaries [67], it is an open question whether such procedures can be used in the information-theoretic security setting; in principle, any such step can be used by the malicious party to his or her advantage. Therefore, new techniques are necessary to deal with the imperfections of the implementation and the inherent limitations to the attainable communication distance. Our results bring quantum cryptography in the distrustful model at a comparable level of practicality as quantum key distribution and provide means to benchmark this type of primitives in a way similar to QKD protocols.

3.3.1 The Protocol

Our protocol is a refinement of the one proposed by Berlin et al [14]; the main difference is that Alice sends a fixed number of pulses K, and uses an attenuated laser source to produce her states instead of a perfect single-photon or an entangled-photon source. By restraining the number of pulses and by allowing an honest abort probability, the protocol can achieve a cheating probability very close to the one proven by Berlin et al, and at the same time be more suitable for practical use.

The number of photons in each pulse produced by the source suit la distribution de Poisson; pour un nombre moyen de photons μ, la probabilité que le nombre de photons est i, est $p_i = \frac{e^{-\mu}\mu^i}{i!}$.

Basic Coin Flipping Protocol

1. For $i = 1, ..., K$:
   (a) Alice picks uniformly at random a basis $\alpha_i \in \{0, 1\}$ and a bit $c_i \in \{0, 1\}$.
   (b) She prepares the state $|\Phi_{\alpha_i, c_i}\rangle$ (see Figure 3.1), such that:

$$\begin{aligned} |\Phi_{\alpha_i,0}\rangle &= \sqrt{y}|0\rangle + (-1)^{\alpha_i}\sqrt{1-y}|1\rangle \\ |\Phi_{\alpha_i,1}\rangle &= \sqrt{1-y}|0\rangle - (-1)^{\alpha_i}\sqrt{y}|1\rangle \end{aligned}$$

   and sends it to Bob.

2. Bob chooses uniformly at random β_i and measures in basis $\{|\Phi_{\beta_i,0}\rangle, |\Phi_{\beta_i,1}\rangle\}$. If his detectors do not click for any pulse, then he aborts. Else, let j the first pulse he detects.

3. Bob picks uniformly at random $b \in \{0, 1\}$ and sends it to Alice, together with the index j.

4. Alice reveals α_j, c_j.

5. If $\alpha_j = \beta_j$, Bob checks that the outcome of his measurement is indeed c_j, otherwise he aborts.

6. If Bob has not aborted, then the outcome of the protocol is $x = c_j \oplus b$.

The parameters K and y are known from the beginning of the protocol; we will later see how to choose them in order to optimise the performance. We note that when the BB84 QKD protocol [5] is implemented using the plug&play system, the states prepared by Alice and measured by Bob correspond to the states $|\Phi_{\alpha_i, c_i}\rangle$ of our quantum coin flipping protocol, with $y = 1/2$. Hence, the quantum transmission stage of the QKD protocol is identical to that of the coin flipping protocol with the exception that, in the latter, y is appropriately modified to guarantee the fairness of the implemented protocol.

3.3.2 Honest Player Abort

Any amount of noise in an experimental implementation results in a non-zero honest abort probability. Here, we analyse exactly how noise and the other experimental parameters affect the honest abort probability in order to ensure that the protocol achieves a task which remains impossible classically. The cases in which an honest abort might occur

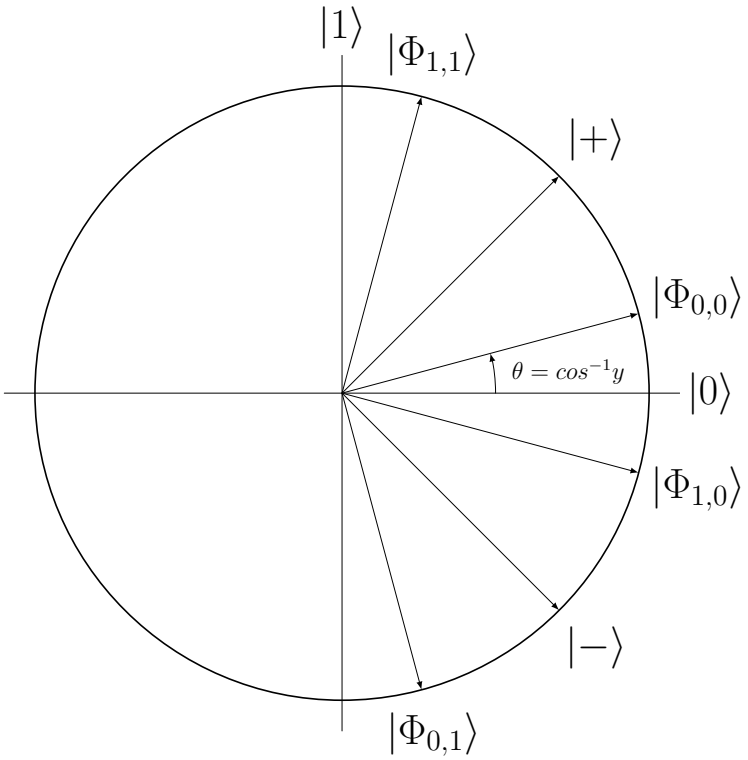


Figure 3.1: The quantum states of the protocol

with some probability are the following:

1. Bob's detectors do not click in any of the K rounds of the coin flip. In this case, the abort probability is 1.

2. Bob's first detection is due to a dark count[2]. The abort probability is $1/4$, since if $\alpha_j = \beta_j$ (step 5), he will abort with probability $1/2$ (dark count is totally random), else if $\alpha_j \neq \beta_j$ he will not abort.

3. The noise in the channel alters the state of the photon. In this case, the abort probability is $1/2$, since he will only abort if $\alpha_j = \beta_j$ (step 5).

[2]Random detection on one of the detectors, not due to real communication between the parties

The total honest abort probability is:

$$
\begin{aligned}
H &= \sum_{i=1}^{3} \Pr[\text{case } i] \cdot \Pr[\text{abort}|\text{case } i] \\
&= \underbrace{Z^K(1-d_B)^K}_{\Pr(\text{case 1})} + \underbrace{\frac{1}{4}\sum_{i=1}^{K}(1-d_B)^{i-1}d_B Z^i}_{\Pr(\text{case 2})} + \underbrace{\frac{e}{2}\Big[1-Z^K(1-d_B)^K - \sum_{i=1}^{K}(1-d_B)^{i-1}d_B Z^i\Big]}_{\Pr(\text{case 3})}
\end{aligned}
$$

where, given that the photon source with mean photon number μ emits pulses that contain i photons with probability $p_i = \frac{e^{-\mu}\mu^i}{i!}$, we define:

$Z = p_0 + \big(1-p_0\big)\big(1-F\eta\big)$: probability that no signal arrives at Bob's detectors;

F: system transmission efficiency;

η: detectors' finite quantum efficiency;

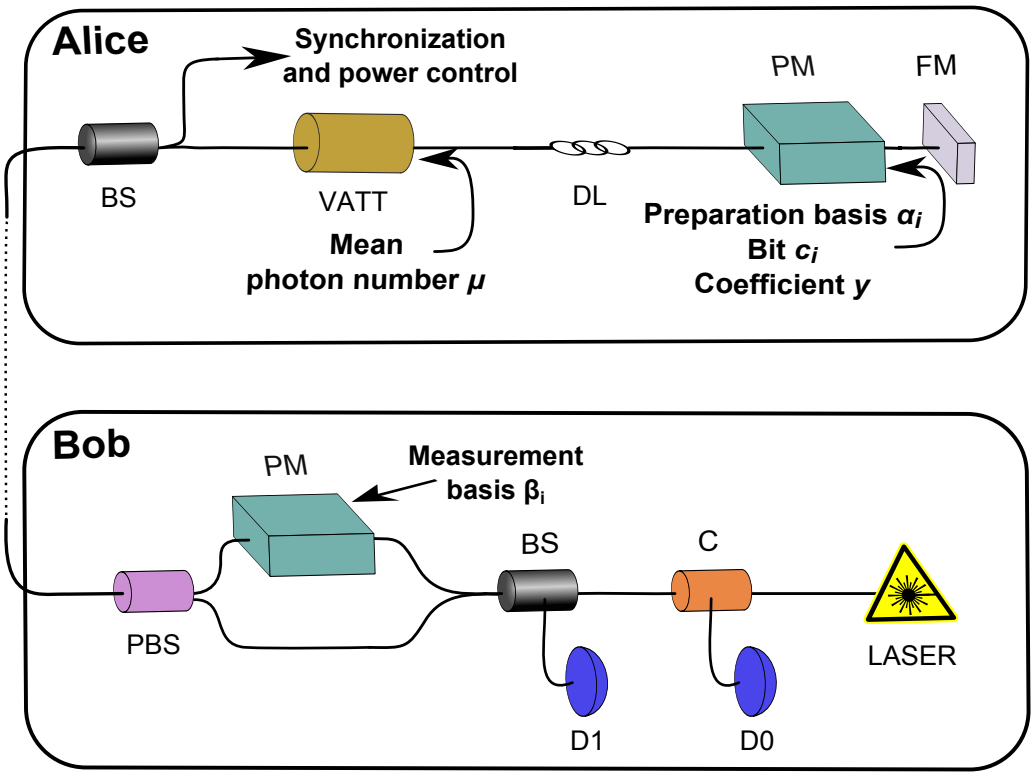
d_B: probability of detector dark count;

e: probability of wrong measurement outcome due to noise, which can be due to imperfect state preparation, channel-induced operations or detector errors.

3.4 Experimental Setup

We demonstrate our quantum coin flipping protocol using a plug&play system, which is an enhanced version of the quantum key distribution system Clavis2 of IDQuantique [12]. As we have already argued in Section 2.5, a plug&play system is a specific type of a collapsed Mach-Zehnder interferometer, that does not require continuous stabilisation and polarisation adjustment, and therefore provides a more stable solution. The experimental setup, shown in Fig. 3.2, employs a two-way approach. The laser source at Bob's setup emits photon pulses at 1550 nm, which are separated at a 50/50 beamsplitter (BS) and then recombined at a polarization beam splitter (PBS), after having traveled through a short and a long arm. The latter contains a phase modulator (not active at this stage) and an optical element that transforms horizontally polarized to vertically polarized states and vice versa. Due to these two different paths, we now have two pulses that travel at different times, first a "reference" pulse coming from the short path and vertically polarised, and then a "signal" pulse, coming from the long arm and horizontally polarised.

The pulses travel to Alice through the communication channel and get reflected on a Faraday mirror, therefore, switching their polarisations. Alice then chooses her basis and bit values, by applying a suitable phase shift with her phase modulator on the



C: Circulator, BS: Beam Splitter, D0,D1: APD detectors, PM: Phase Modulator, FM: Faraday Mirror
VATT: Variable Attenuator, PBS: Polarization Beam Splitter, BF: Bandpass Filter, DL: Delay Line

Figure 3.2: Experimental setup of the quantum coin flipping plug&play system

second pulse (that is, the "signal" pulse with the now vertical polarisation). By properly adjusting the waveplates of the modulator, she also chooses at the same time the state coefficient y. Alice also uses her variable attenuator shown in Fig. 3.2, to apply the required attenuation for a desired mean photon number per pulse μ, using a previously established calibration relationship.

Now the two pulses that travel back to Bob, pass through the PBS, therefore the "reference" pulse with the H polarisation gets reflected towards the long arm, and the "signal" pulse with the V polarisation gets transmitted towards the short arm. The "reference" pulse passes through the optical element that gives it a V polarisation (same as the "signal" pulse), and the Phase modulator allows Bob to choose a measurement basis by applying the appropriate phase on the pulse. Due to the construction of the plug&play system, the pulses now arrive simultaneously at the beamsplitter, where they interfere and get detected by two InGaAs avalanche photodiode (APD) single-photon detectors. Constructive interference leads the reconstructed signal to a circulator which diverts the signal towards Detector 0 (D0) and destructive interference leads the signal directly to Detector 1 (D1). At the end of the protocol, we derive a set of data containing

the preparation bases and bits of Alice and the measurement bases and outcomes of Bob, similarly to the raw key data obtained in quantum key distribution experiments.

Using a QKD system for an implementation of a cryptographic primitive that requires an entirely different security analysis and operates in non-standard experimental conditions necessitated several important modifications to the system. First, single-photon detectors with very low dark count rates were installed in the quantum coin flipping system; indeed, the honest abort probability is very sensitive to this parameter and so with even moderately high dark counts the quantum advantage vanishes at any distance. The dark count rate per detection gate of the detectors $D0$ and $D1$ was 7×10^{-6} and 1.6×10^{-6}, with corresponding quantum efficiency values of 7.7% and 5.2%, respectively. Second, new functionalities and control signals were added to the system to be able to apply the coin flipping protocol, in particular, those allowing us to rotate the standard BB84 states so that the optimal states for a fair protocol could be used and those allowing us to reduce the mean photon number per pulse μ at suitable values for coin flipping.

It is important to note that the values of μ in the experiment were in fact one or two orders of magnitude lower than those typically used for QKD. This last point was also crucial for many aspects of the implementation, since a very low μ value hindered the operation of several embedded calibration and testing processes of the system, which were therefore entirely redesigned. Such calibration procedures play an important role in the two-way configuration of the plug&play system, which imposes particular care in the synchronization of the phase shift and attenuation signals, and the detection gates. Among those, of particular importance is the calibration procedure involving the variable attenuator at Alice's site, which was actually the main source of the uncertainty that we will observe in our data later on, in Section 3.7. Finally, the QKD classical post-processing procedures were replaced by our software, which used as an input the raw data of quantum signal exchange between Alice and Bob, together with basis choice information. These enhancements led to the development of a practical plug&play system that is capable of performing quantum coin flipping in addition to key distribution.

3.5 Security assumptions and analysis with standard imperfections.

We first provide a security analysis when the following three assumptions are satisfied:

1. Honest Alice creates each of the four protocol states $|\Phi_{\alpha_i,c_i}\rangle$ (see Fig. 3.1) with the same probability, independently for each pulse and independently of Bob.

2. For the first pulse j that honest Bob successfully measures, the distribution of his measurement basis β_j and his bit b is uniform and independent of Alice.

3. For the first pulse j that honest Bob successfully measures, if the state of the pulse is ρ, then for each basis β_j, the probabilities of the two outcomes are $\langle\Phi_{\beta_j,0}|\rho|\Phi_{\beta_j,0}\rangle$ and $\langle\Phi_{\beta_j,1}|\rho|\Phi_{\beta_j,1}\rangle$.

We describe the optimal cheating strategies of malicious Alice and Bob and derive the corresponding cheating probabilities when the above assumptions are satisfied. As we will see in the following sections, the cheating probabilities depend on the number of rounds K, the protocol parameter y and the mean photon number μ. We can make the protocol fair, by changing the parameter y.

3.5.1 Malicious Alice

Let us assume that Alice tries to bias the coin towards the value $x = 0$ (the analysis for $x = 1$ is similar). We also assume that Bob successfully measured the first pulse, thus providing an upper bound to Alice's cheating probability. Honest Bob has therefore picked a uniformly random basis β and has detected the qubit sent by Alice. He replies with the uniformly random bit b and the index of the first detected pulse j. Note that from now on, when it is clear that we only examine the properties of the specific pulse j that Bob announces, we will be dropping the index j and only use variables α and c.

The goal of malicious Alice is to reveal a basis α and the value $c = b$ in the next step of the protocol, so that at the end the value of the coin is 0. If $\alpha \neq \beta$, Bob accepts. If $\alpha = \beta$, Bob checks whether his measurement outcome agrees with c.

Since the states used are the same as in Aharonov et al. protocol [41] that was presented in Section 3.2, we can use the rigorous analysis of Spekkens and Rudolph [66] to prove security against Malicious Alice, for the case where the bases of the two parties agree. The main difference between [41] and our protocol, is that Bob measures at a different step during the protocol. However, since Bob's choice of bit b is uniformly at random, it does not give any information to Alice about his measurement basis or outcome. It therefore does not change Alice's cheating strategy, whether he has measured before or after Alice reveals her measurement basis and bit. It will however change Alice's cheating probability, since, in the case where the bases disagree, Alice can always perfectly cheat because Bob accepts the coin flip without questioning her revealed bit and basis. A similar proof can be found in [14].

Alice's optimal strategy consists of finding the state that will maximize the average probability of revealing bit 0 or 1 (since Bob's choice b is uniform). However, when Alice reveals her committed bit, $c = 0$ or $c = 1$, she also has to reveal the basis that she supposedly used to form the state sent. This might enable Alice to increase her cheating probability by creating a state in a large Hilbert space, sending part of it to Bob and after Bob's message, performing some general operation on her part to decide which basis to reveal. It has been shown in [66] (section 6.4.1), that for any protocol where

there are two honest pure states that correspond to bit 0 and two honest pure states that correspond to bit 1 (as in our case), Alice's optimal strategy is to send the state that maximizes the average probability of revealing $(\alpha = 0, c = 0)$ and $(\alpha = 1, c = 1)$ or of revealing $(\alpha = 1, c = 0)$ and $(\alpha = 0, c = 1)$. In high level, this is true since the states in the pairs $\{|\Phi_{0,0}\rangle, |\Phi_{1,1}\rangle\}$ and $\{|\Phi_{1,0}\rangle, |\Phi_{0,1}\rangle\}$ are closer to each other than the orthogonal states in the pairs $\{|\Phi_{0,0}\rangle, |\Phi_{0,1}\rangle\}$ and $\{|\Phi_{1,0}\rangle, |\Phi_{1,1}\rangle\}$ (see Fig. 3.1).

For the first two combinations of bases and bits, a simple calculation (see [66]) shows that the optimal over all possible states is in fact the pure state $|+\rangle$; then, after reception of Bob's bit b, Alice reveals $(\alpha = b, c = b)$. For the other two combinations, the optimal state is shown to be the pure state $|-\rangle$; then, Alice reveals $(\alpha = 1 - b, c = b)$. The probability that she forces the outcome 0 is then in both cases:

$$\Pr[x = 0|\text{same bases}] = \frac{1}{2} + \sqrt{y(1-y)},$$

where y is the coefficient of the honest states. Note that Alice could also decide to prepare any mixture of the states $|+\rangle$ and $|-\rangle$ and achieve exactly the same cheating probability. When the bases are different, according to the protocol, Bob always accepts the coin. Since Bob's basis choice is uniformly random and independent of Alice, Alice can bias the coin with probability:

$$p_q^A \leq \frac{3}{4} + \frac{1}{2}\sqrt{y(1-y)} \tag{3.1}$$

3.5.2 Malicious Bob.

The optimal cheating strategy of an all-powerful Bob is complex and involves his ability to know the number of photons in each of the K pulses sent by Alice. He can then accordingly optimize his POVM on all K pulses to maximize his cheating probability. It is important to note that, under Assumption 1, honest Alice uses a uniformly random bit c_i to prepare the state in each pulse i, and all c_is are independent of each other. We upper bound Bob's cheating probability by considering that his cheating probability is 1 in all cases except for four events A_i $(i = 1, \ldots, 4)$, for which we find appropriate bounds as shown below.

Let us assume, without loss of generality, that Bob's desired outcome is $x = 0$ and let $\Pr[x = 0|A_i]$ be the probability that Bob will force his preference when event A_i has taken place, which happens with probability $\Pr[A_i]$. According to the protocol, the number of photons per pulse i follows the Poisson distribution with probability to have i photons in the pulse $p_i = \mu^i e^{-\mu}/i!$, where μ is the mean photon number. We consider the following events, for K number of rounds:

A_1 : Bob receives only vacuum pulses. This event occurs with probability $\Pr[A_1] = e^{-K\mu}$.

Since Bob has no knowledge of Alice's bit, which is uniformly random, he picks a random bit, and hence $\Pr[x=0|A_1]=1/2$.

A_2 : Bob receives vacuum pulses, at least one single-photon pulse and no two- or more-photon pulses. This event occurs with probability $\Pr[A_2]=(p_0+p_1)^K-p_0^K$. We will assume here that Bob does not actually receive any vacuum pulses, which can only increase his cheating.

To analyze cheating Bob, we use the very strong loss-tolerant properties of our coin flipping protocol. From the definition of the states of the honest protocol, we have that the density matrices for the two different choices of Alice's bit $c_i \in \{0,1\}, \forall i \in [K]$, are:

$$\begin{aligned} \rho_0 &= \frac{1}{2}|\Phi_{0,0}\rangle\langle\Phi_{0,0}| + \frac{1}{2}|\Phi_{1,0}\rangle\langle\Phi_{1,0}| \\ \rho_1 &= \frac{1}{2}|\Phi_{0,1}\rangle\langle\Phi_{0,1}| + \frac{1}{2}|\Phi_{1,1}\rangle\langle\Phi_{1,1}| \end{aligned}$$

It holds that $\rho_0 = y|0\rangle\langle 0| + (1-y)|1\rangle\langle 1|$ and $\rho_1 = (1-y)|0\rangle\langle 0| + y|1\rangle\langle 1|$, so for $y \in (\frac{1}{2}, 1]$, the maximum eigenvalue of ρ_0 and ρ_1 is equal to y and their minimum eigenvalue is equal to $(1-y)$. It holds that:

$$(1-y)\mathbb{I} \preceq \rho_m \preceq y\mathbb{I}, \quad \forall m \in \{0,1\}$$

where $\mathbb{I}$ is the identity operator and $A \preceq B$ means that the matrix $B-A$ is positive semidefinite. From the above, we can conclude that

$$\rho_0 \succeq \frac{1-y}{y}\rho_1 \quad , \quad \rho_1 \succeq \frac{1-y}{y}\rho_0.$$

Hence, we can use the positive norm-1 matrices:

$$\xi_0 = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad \xi_1 = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

to rewrite density matrices ρ_0 and ρ_1:

$$\begin{aligned} \rho_0 &= y\xi_0 + (1-y)\xi_1 \\ \rho_1 &= (1-y)\xi_0 + y\xi_1 \end{aligned} \tag{3.2}$$

Let $\{M_{i,b}\}_{i\in[K],b\in\{0,1\}}$ the POVM that Bob applies on all K pulses to determine the index j that he will announce as his first measured pulse, as well as his guess b for Alice's bit c_i. From the completeness condition we have $\sum_{i,b} M_{i,b} = \mathbb{I}$. Let

$M_i = M_{i,0} + M_{i,1}$ be the POVM element that corresponds to the event that Bob outputs i as his first measured pulse. Bob's cheating probability can be expressed as follows:

$$\Pr[x = 0|A_2] = \sum_{i\in[K]} \Pr[\text{Bob outputs } (i, b = c_i)] = \sum_i \Pr[i] \cdot \Pr[b = c_i|i]$$

For all pulses $i \in [K]$, created by Alice using basis a_i and bit c_i, Bob's density matrix is ρ_{c_i} in the register that corresponds to the i^{th} pulse and some state $\gamma_{\neg i}$ in the other registers that is independent of c_i (without loss of generality we can think of the latter as the totally mixed state $\mathbb{I}/2$). The state in the K registers is then the product state $\rho_{c_i} \otimes \gamma_{\neg i}$.

When Bob performs the above POVM and outputs index j, then after the measurement he has the (unnormalized) mixed state $M_j(\rho_{c_j} \otimes \gamma_{\neg j})$. Our goal is to determine how well Bob can guess the value c_j when he outputs the index j, in other words, how well he can distinguish the states $M_j(\rho_0 \otimes \gamma_{\neg j})$ and $M_j(\rho_1 \otimes \gamma_{\neg j})$. From the optimality of the Helstrom measurement, we have:

$$\Pr[b = c_j|j] \leq \frac{1}{2} + \frac{||a_0\sigma_0 - a_1\sigma_1||_1}{2} \tag{3.3}$$

where $a_k = \Pr[c_j = k|j] = \frac{||M_j(\rho_k\otimes\gamma_{\neg j})||_1}{||M_j(\rho_0\otimes\gamma_{\neg j})||_1 + ||M_j(\rho_1\otimes\gamma_{\neg j})||_1}$ and $\sigma_k = \frac{M_j(\rho_k\otimes\gamma_{\neg j})}{||M_j(\rho_k\otimes\gamma_{\neg j})||_1}$ for $k \in \{0, 1\}$. We therefore have:

$$a_0\sigma_0 - a_1\sigma_1 = \frac{M_j(\rho_0 \otimes \gamma_{\neg j}) - M_j(\rho_1 \otimes \gamma_{\neg j})}{||M_j(\rho_0 \otimes \gamma_{\neg j})||_1 + ||M_j(\rho_1 \otimes \gamma_{\neg j})||_1}$$

Using Eqs. 3.2 and the fact that $\rho_0 + \rho_1 = \xi_0 + \xi_1$, we have:

$$a_0\sigma_0 - a_1\sigma_1 = \frac{(2y-1)\big(M_j(\xi_0 \otimes \gamma_{\neg j}) - M_j(\xi_1 \otimes \gamma_{\neg j})\big)}{||M_j(\xi_0 \otimes \gamma_{\neg j})||_1 + ||M_j(\xi_1 \otimes \gamma_{\neg j})||_1}$$

and finally, Eq. 3.3 becomes:

$$\Pr[b = c_j|j] \leq \frac{1}{2} + \frac{1}{2} \cdot \frac{(2y-1)||M_j(\xi_0 \otimes \gamma_{\neg j}) - M_j(\xi_1 \otimes \gamma_{\neg j})||_1}{||M_j(\xi_0 \otimes \gamma_{\neg j})||_1 + ||M_j(\xi_1 \otimes \gamma_{\neg j})||_1} \leq y$$

Since the above holds for any $j \in [K]$, we conclude that:

$$\Pr[x=0|A_2] = \sum_{i\in[K]} \Pr[i]\cdot\Pr[b=c_i|i] \leq y$$

A_3 : Bob receives only vacuum pulses and one two-photon pulse. This events occurs with probability $\Pr[A_3] = Kp_2p_0^{K-1}$. Let σ_0 and σ_1 the mixed states that correspond to the two-photon pulse Bob receives when Alice's bit is 0 or 1; then, the optimal measurement to distinguish these states is given by the Helstrom measurement and simple calculations give $\Pr[x=0|A_3] = \frac{1}{2} + \frac{1}{2}||\frac{1}{2}\sigma_0 - \frac{1}{2}\sigma_1||_1 = y$.

A_4 : Bob receives vacuum pulses, one two-photon pulse and at least one single-photon pulse. This events occurs with probability $\Pr[A_4] = Kp_2[(p_0+p_1)^{K-1} - p_0^{K-1}]$. As before, we assume that Bob receives no vacuum pulses, in order to upperbound his cheating probability.

Let $\{M_{i,b}\}_{i\in[K],b\in\{0,1\}}$ the POVM that Bob applies on all K pulses to determine the index he will announce as his first measured pulse, as well as his guess b for Alice's bit. Let j the index that corresponds to the two-photon pulse. We have

$$\begin{aligned}\Pr[x=0|A_4] &= \sum_{i\in[K]} \Pr[\text{Bob outputs}(i, b=c_i)] \\ &= \Pr[j]\cdot\Pr[b=c_j|j] + \sum_{i\neq j}\Pr[i]\cdot\Pr[b=c_i|i]\end{aligned}$$

From the analysis of A_2, we know that for any single-photon pulse with index i, we have $\Pr[b=c_i|i] \leq y$. Note that again, the state that corresponds to the remaining pulses, including the two-photon one, is independent of c_i. Let $q = \Pr[j]$, then we have

$$\Pr[x=0|A_4] = q\cdot\Pr[b=c_j|j] + (1-q)y$$

Let us now study the probability that Bob can guess the bit c_j that corresponds to the two-photon pulse. Using the notation from the previous events, the overall state Bob has in case $c_j = 0$ is $\sigma_0\otimes\gamma_{\neg j}$ and the state he has in case $c_j = 1$ is $\sigma_1\otimes\gamma_{\neg j}$. The probability of guessing c_j is upperbounded by the optimal POVM on the K pulses that distinguishes the states $\sigma_0\otimes\gamma_{\neg j}$ and $\sigma_1\otimes\gamma_{\neg j}$. This is again given by the Helstrom measurement and has probability:

$$P_{opt} = \frac{1}{2} + \frac{1}{2}\left|\left|\Pr[c_j=0|j]\sigma_0\otimes\gamma_{\neg j} - \Pr[c_j=1|j]\sigma_1\otimes\gamma_{\neg j}\right|\right|_1 \leq y$$

Let us now describe a specific strategy that Bob can perform in order to guess the value c_j of the two-photon pulse: He performs the POVM $\{M_{i,b}\}_{i\in[K],b\in\{0,1\}}$ and if the output is $(j,0)$ he outputs 0, if the output is $(j,1)$ he outputs 1, and in all other cases he outputs a uniformly random bit. Let z the success probability of this strategy. Then, $z = q\Pr[b = c_j|j] + \frac{1-q}{2}$. This yields the inequality $2z-1 \leq q$. It also holds from the optimality of the Helstrom measurement that $z \leq y$. We finally have:

$$\begin{aligned}
\Pr[x=0|A_4] &\leq q\cdot\Pr[b=c_j|j] + (1-q)y \\
&= z + (1-q)(y-1/2) \\
&\leq z + (2-2z)(y-1/2) \\
&= 2z(1-y) + 2y - 1 \\
&\leq 2y(1-y) + 2y - 1 \\
&= -2y^2 + 4y - 1
\end{aligned}$$

By combining the above results, and noticing that Bob's cheating strategy is upperbounded in a similar way when he wants $x = 1$ and gives the same cheating probability, we find that Bob can bias the coin with probability:

$$p_q^B \leq \sum_{i=1}^{4}\Pr[A_i]\cdot\Pr[x=0|A_i] + \left[1-\sum_{i=1}^{4}\Pr[A_i]\right]\cdot 1 \tag{3.4}$$

3.6 Satisfying the security assumptions with the plug&play system.

The previous security analysis holds when the three security assumptions at the beginning of Section 3.5 are satisfied. In practice, however, these assumptions, which concern honest Alice and Bob, may not be fulfilled. For example, in every round $i \in [K]$, honest Alice uses a quantum random number generator (QNRG) to pick the values of the basis α_i and bit c_i. She then generates the corresponding state $|\Phi_{\alpha_i,c_i}\rangle$ by applying a suitable phase shift with a phase modulator. On his side, honest Bob uses a (QNRG) to pick the basis β_i at every round $i \in [K]$, by applying the appropriate phase shift with his phase modulator and then uses two InGaAs avalanche photodiode single-photon detectors to detect the photon. He also uses a quantum random number generator to pick the bit b. Consequently, if the QNRG of either of the two players is biased towards one outcome, then a malicious player could increase her cheating if they learn that bias.

Similarly, if Bob performs a measurement using a high-efficiency detector for one outcome and a lower-efficiency one for the other outcome, then his detection event will be biased towards one of the outcomes, a fact that Alice might use to her advantage. Last, if a different set of detectors is used for each of the two bases, again Bob's probability of successfully measuring in one basis may be much greater than in the other one. In this case, Alice can increase her cheating probability by revealing the latter basis with higher probability, thus forcing Bob to accept with higher probability.

We therefore need to assess the deviations from the security assumptions present in our system and describe the procedures that need to be performed to recover those assumptions almost perfectly and consequently the security of the implemented protocol as well.

Let us examine each of the three assumptions we previously made. We will see that the first two assumptions hold almost perfectly, since the only deviations come from the possible bias of the quantum random number generator and the variation in the capability of the phase modulator to apply different phase shift values. In order to fulfill the last assumption, however, we need to add to the protocol a symmetrization stage, in order to remedy for a big asymmetry in the two detection efficiencies.

Assumption 1: Alice's choice of states. We examine Alice's ability to generate each of the four protocol states with the same probability for each pulse. The only way to assess this in practice is by analyzing Bob's detection events. We calculate the probability that honest Alice had picked each basis over the entire set of Bob's detection events. The distribution of this basis should ideally be uniform. Based on the experimental data corresponding to the 15 km implementation, we find that the basis choice is close to uniform:

$$\Pr[\alpha = 0] = 0.5048$$
$$\Pr[\alpha = 1] = 0.4952$$

For the 25 km experiment, the corresponding probabilities are 0.5038 and 0.4962, respectively.

Next, we would like to ascertain whether the distribution of Alice's bit for each pulse is also uniform and moreover that it remains uniform even conditioned on Alice's choice of basis. Again we can only assess this by looking at the detection events of Bob. However, it is necessary that we remove the possible effects of Bob's detectors on this distribution, since Bob uses two different detectors for the two measurement outcomes (see the Experimental Setup in Fig 3.2). For this reason, we collected data again from our experiment, where this time, by appropriately adding a phase shift via Bob's phase modulator, we interchanged the role of the two detectors for each of the two bases. The

analysis of the obtained data shows that the ratio of detection events corresponding to bits 0 and 1 for each of the bases is almost perfectly inverted. This implies that Alice produces states that correspond to 0 and 1 almost uniformly, even when we condition on her basis choice (with a deviation of 0.003). This is not surprising since the state choice is performed using a quantum random number generator and a single phase modulator that applies one of four possible phase shifts.

By performing extensive tests, we can bound the deviation of Alice's state distribution from the uniform one, using a single ϵ_A:

$$\begin{aligned} &\forall k,l \in \{0,1\}, |\Pr[\alpha = k|c = l] - 1/2| \leq 0.005 \triangleq \epsilon_A \\ &\forall k,l \in \{0,1\}, |\Pr[\alpha = k, c = l] - 1/4| \leq 0.004 \leq \epsilon_A \\ &\forall k,l \in \{0,1\}, |\Pr[c = l|\alpha = k] - 1/2| \leq 0.003 \leq \epsilon_A \end{aligned} \tag{3.5}$$

Since this bound on the deviation is very small, we do not proceed in any correction as part of the experimental procedure, but we incorporate the bound ϵ_A in our complete security analysis described in a following section. This naturally slightly increases Bob's cheating probability.

Assumption 2: Bob's choice of bases and bit b. Next, we examine the probability with which Bob has chosen each basis β for the first pulse he successfully measured. Note that what is important is the distribution of the basis for the first measured pulse and not over all pulses, since this is the information which is relevant to the coin outcome. The distribution of this basis should ideally be uniform. Note that the same pair of detectors is used for measurements in both bases (see the Experimental Setup in Fig 3.2). From the analysis of the experimental data for the 15 km implementation, we find:

$$\begin{aligned} \Pr[\beta = 0] &= 0.5006 \\ \Pr[\beta = 1] &= 0.4994 \end{aligned}$$

For the 25 km experiment, the corresponding probabilities are 0.5003 and 0.4997, respectively. The above results demonstrate that the distribution of Bob's bases is indeed very close to uniform. Again, this is not surprising since, as mentioned before, the only devices that are used for the basis and bit choices in our implementation are quantum random number generators and phase modulators, which are expected to be very reliable.

Concerning the distribution of the bit b, we note that the quantum random number generator used in our experiment (IdQuantique's Quantis) provides very strong guarantees for the uniformity of each output bit and the independence between different output bits. In fact, we extensively tested the bias of the outputs of Quantis and we can bound the deviation of the probability of each bit from uniform, even conditioned on

Alice basis	Alice bit	Bob basis	Bob outcome	Detection events (15 km)	Detection events (25 km)
0	0	0	0	84071	54915
0	1	0	1	53200	34994
1	0	1	0	82825	54279
1	1	1	1	51497	34252

Table 3.1: Detection events for the experiments with channel lengths of 15 and 25 km

any number of previous bits, by $\epsilon_Q = 0.0006$.

Hence, in our implementation, for the first pulse Bob successfully measures, we can bound the deviation from uniform of his basis and bit distribution, as follows:

$$\forall k, l \in \{0,1\}, |\Pr[\beta = k, b = l] - 1/4| \leq 0.00061 \triangleq \epsilon_B \tag{3.6}$$

Again, since the deviation is very small we do not proceed in any correction in practice, however we incorporate the bound ϵ_B in our security analysis. This slightly increases Alice's cheating probability.

Assumption 3: Bob's detection. In order to calculate the detection efficiency ratio, we focus on the number of detection events that occur when Alice and Bob have used the same bases and agree on the output values. In Table 3.1, we can see the measurement results that correspond to the case when the preparation basis and bit values of Alice agree with the measurement basis and outcome of Bob[3]. It is clear that there exists a significant asymmetry in the number of detections observed by each detector, which leads to an important bias in the announced outcomes by Bob. Our previous analysis has practically excluded that this event is due to an imbalance in the states Alice prepares, hence it is predominantly due to an asymmetry in the two detection efficiencies in Bob's system.

After subtracting the events that are due to dark counts from the total number of detection events, taking also into account the slight asymmetry of Bob's choice of basis, we find that the detector efficiency ratio, for both channel lengths, is $\eta_1/\eta_0 = 0.68 \pm 0.015$, where η_0 and η_1 correspond to detectors D_0 and D_1, respectively (see Fig. 1 in main text). This difference in detection efficiencies can lead to a sophisticated attack by Alice, where she sends a different state than $|+\rangle$ or $|-\rangle$ (depending on which bit is favored by the asymmetry). This can increase her cheating probability substantially. An efficient solution proposed in Ref. [63] is the symmetrization of losses, by which Bob effectively makes the two detection efficiencies equal by throwing away some detection

[3]For the 15 km experiment, the total number of pulses that were sent was 1.1458×10^{10} and the total number of detection events is 593272. For the 25 km experiment, 7.2905×10^9 pulses were sent and 414649 detection events were registered in total.

events. More specifically, whenever Bob detects an event on detector D_0, he discards it with probability 32%. This was implemented in our experiments. Even after the symmetrization procedure, some deviation on the detection efficiency ratio may still remain, and by testing our detectors can be bounded as follows:

$$\left|\frac{\eta_1}{\eta_0} - 1\right| \leq 0.022 \triangleq \epsilon'_B \tag{3.7}$$

The bound ϵ'_B, which again holds with probability negligibly away from 1, is incorporated in the security analysis that follows and increases Alice's cheating probability.

We now compute the cheating probabilities in our implementation, taking into account the imperfections quantified by the bounds in Eqs. 3.5, 3.6 and 3.7.

3.6.1 Malicious Alice

Let us assume that Alice tries to bias the coin towards the value $x = 0$ (the analysis for $x = 1$ is similar) and that Bob successfully measures the first pulse. From Eq. 3.6, we assume that the probabilities of Bob's distribution when choosing the basis β and bit b, deviate at most ϵ_B from 1/4. We also assume that Alice has the power to choose among all these distributions the one that maximizes her cheating probability.

As in the uniform case, Alice's optimal strategy consists of finding the state that will maximize the average probability of revealing bit 0 or 1. Even in the presence of the small deviation of Bob's choices, the arguments in Ref. [66] still hold; Alice's optimal strategy is to send the state that maximizes the probability of revealing:

1. $(\alpha = 0, c = 0)$ when $b = 0$ and $(\alpha = 1, c = 1)$ when $b = 1$,

   or

2. $(\alpha = 1, c = 0)$ when $b = 0$ and $(\alpha = 0, c = 1)$ when $b = 1$.

Note that, due to the deviation ϵ_B, these two optimal strategies may not achieve the same cheating probability, which means that we need to calculate both of them and take the maximum of the two. We remind that in the case of $\epsilon_B = 0$, the two optimal strategies correspond to sending the states $|+\rangle$ and $|-\rangle$ and they both achieve the same cheating probability.

Let us analyze the first strategy (the analysis of the other one is similar). Let ρ the state sent by Alice. The probability that the protocol outputs $x = 0$ is:

$$\Pr[x = 0] \quad = \quad \sum_{k,l} \Pr[\beta = k, b = l] \Pr[x = 0 | \beta = k, b = l]$$

where β is Bob's choice of basis and b is Bob's bit, for the successfully measured pulse. According to Alice's strategy, when Bob picks $\beta \neq b$, then Alice reveals a different basis than Bob's, which means he accepts with probability 1. In other words

$$\Pr[x = 0|\beta = 0, b = 1] = \Pr[x = 0|\beta = 1, b = 0] = 1.$$

To upperbound Alice's cheating probability, we attribute the highest possible probability to these events, more precisely:

$$\Pr[\beta = 0, b = 1] = \Pr[\beta = 1, b = 0] = \frac{1}{4} + \epsilon_B$$
$$\Pr[\beta = 0, b = 0] = \Pr[\beta = 1, b = 1] = \frac{1}{4} - \epsilon_B$$

Then, we need to compute the probability that the protocol outputs 0, when Alice sends the state ρ and Bob picks $\beta = b$ for the successfully measured pulse. Note that, by definition of the first strategy, when $(\beta = 0, b = 0)$, Alice reveals $(\alpha = 0, c = 0)$ and when $(\beta = 1, b = 1)$, she reveals $(\alpha = 1, c = 1)$. Let us assume that the ratio of the detection efficiencies of Bob's system deviates from 1 by at most ϵ'_B and Alice knows this distribution. Then, the probabilities are

$$\Pr[x = 0|\beta = 0, b = 0] = \frac{\langle\Phi_{0,0}|\rho|\Phi_{0,0}\rangle\eta_0}{\langle\Phi_{0,0}|\rho|\Phi_{0,0}\rangle\eta_0 + \langle\Phi_{0,1}|\rho|\Phi_{0,1}\rangle\eta_1}$$
$$\Pr[x = 0|\beta = 1, b = 1] = \frac{\langle\Phi_{1,1}|\rho|\Phi_{1,1}\rangle\eta_1}{\langle\Phi_{1,0}|\rho|\Phi_{1,0}\rangle\eta_0 + \langle\Phi_{1,1}|\rho|\Phi_{1,1}\rangle\eta_1}$$

We can see that the maximum value of the above expressions, i.e., the maximum of Alice's cheating probability, can be achieved by a pure state that belongs to the Hilbert space defined by the honest states $|\Phi_{\alpha,c}\rangle$. This is the same result as in the uniform case, where the optimum was achieved by the states $|+\rangle$ and $|-\rangle$. Note that the expressions are concave in ρ and the extremal points of the set of density matrices are pure states; in addition, any part of ρ outside the Hilbert space of the honest states leaves the expressions unchanged.

Since $\{|\Phi_{0,0}\rangle, |\Phi_{0,1}\rangle\}$ is a basis for this space, we have that there exists a state that maximizes Alice's cheating of the form:

$$|\chi\rangle = \cos\phi|\Phi_{0,0}\rangle + \sin\phi|\Phi_{0,1}\rangle$$

We can then optimize over all angles ϕ to find an upper bound on Alice's cheating probability $p_q^A = \max\{\Pr[x = 0], \Pr[x = 1]\}$. The analysis for $x = 1$ gives the same results. Note that we have upperbounded the cheating probability by giving Alice

knowledge of the efficiency ratio and also the power to attribute in the best way the deviations.

In the case $\epsilon_B = \epsilon'_B = 0$, we find that the optimal cheating strategy is for $\phi = \pi/4 - \theta$ and we recover Alice's original optimal cheating strategy, which leads to the cheating probability in Eq. 3.1.

3.6.2 Malicious Bob

Now let us see how cheating Bob can exploit the deviation in Alice's distribution of choices. We assume that Alice's probabilities deviate from uniform by at most ϵ_A (see Eq. 3.5). We analyze the four cheating events for Bob in a very similar way as before. Bob is assumed to want a coin value $x = 0$ (the same analysis holds for $x = 1$).

A_1: Bob receives only vacuum pulses. Bob picks b equal to the most probable bit according to Alice's distribution. We have:

$$\Pr[x = 0|A_1] \leq \frac{1}{2} + \epsilon_A \tag{3.8}$$

Note again that the value of Alice's bit has deviation ϵ_A from uniform, even conditioned on any of the other bits she has encoded in different pulses.

A_2: Bob receives vacuum pulses, at least one single-photon pulse and no two- or more-photon pulses. Let ρ_0 and ρ_1 the state of a single-photon pulse corresponding to Alice's bit 0 and 1, in case her distribution is uniform and let ρ'_0 and ρ'_1 the states when Alice's distribution deviates from uniform by at most ϵ_A. We will show that there exists a $y' \in (\frac{1}{2}, 1]$, such that:

$$(1 - y')\mathbb{I} \preceq \rho'_m \preceq y'\mathbb{I}\,, \quad \forall m \in \{0, 1\}$$

where $\mathbb{I}$ is the identity matrix. Then, we can follow the same analysis as in the uniform case and conclude that $\Pr[x = 0|A_2] \leq y'$.

To compute y', we consider the different density matrices for Alice's choice of bit c (again we drop the index from both the bit and the basis, because Alice is honest and creates her states in a uniform way):

$$\begin{aligned} \rho'_0 &= \Pr[\alpha = 0|c = 0]|\Phi_{0,0}\rangle\langle\Phi_{0,0}| + \Pr[\alpha = 1|c = 0]|\Phi_{1,0}\rangle\langle\Phi_{1,0}| \\ \rho'_1 &= \Pr[\alpha = 0|c = 1]|\Phi_{0,1}\rangle\langle\Phi_{0,1}| + \Pr[\alpha = 1|c = 1]|\Phi_{1,1}\rangle\langle\Phi_{1,1}| \end{aligned}$$

Since these probabilities deviate at most ϵ_A from $1/2$, we have for $m \in \{0,1\}$

$$\begin{aligned}(1-2\epsilon_A)\rho_m &\preceq \rho'_m \preceq (1+2\epsilon_A)\rho_m \Leftrightarrow \\ (1-2\epsilon_A)(1-y)\mathbb{I} &\preceq \rho'_m \preceq (1+2\epsilon_A)y\mathbb{I} \Leftrightarrow \\ (1-(y+2\epsilon_A))\mathbb{I} &\preceq \rho'_m \preceq (y+2\epsilon_A)\mathbb{I}\end{aligned}$$

Similarly to the analysis of A_2 in the uniform case, we have

$$\Pr[x=0|A_2] \leq y + 2\epsilon_A \tag{3.9}$$

A_3: Bob receives only vacuum pulses and one two-photon pulse. Let σ_0 and σ_1 the mixed states that correspond to the two-photon pulse Bob receives when Alice's bit is 0 or 1 in case Alice's distribution is exactly uniform, and σ'_0 and σ'_1 the mixed states that correspond to the two-photon pulse Bob receives when Alice's distribution deviates from uniform by ϵ_A:

$$\begin{aligned}\sigma'_0 &= \Pr[\alpha=0|c=0](|\Phi_{0,0}\rangle\langle\Phi_{0,0}|)^{\otimes 2} + \Pr[\alpha=1|c=0](|\Phi_{1,0}\rangle\langle\Phi_{1,0}|)^{\otimes 2} \\ \sigma'_1 &= \Pr[\alpha=0|c=1](|\Phi_{0,1}\rangle\langle\Phi_{0,1}|)^{\otimes 2} + \Pr[\alpha=1|c=1](|\Phi_{1,1}\rangle\langle\Phi_{1,1}|)^{\otimes 2}\end{aligned}$$

Again, the optimal distinguishing measurement gives:

$$\begin{aligned}\Pr[x=0|A_3] &= \frac{1}{2} + \frac{1}{2}\left|\left|\Pr[c=0]\sigma'_0 - \Pr[c=1]\sigma'_1\right|\right|_1 \\ &\leq \frac{1}{2} + \frac{1}{2}\left|\left|\frac{1}{2}\sigma_0 - \frac{1}{2}\sigma_1\right|\right|_1 + \epsilon_A||\sigma_0+\sigma_1||_1 \\ &\leq y + 2\epsilon_A\end{aligned} \tag{3.10}$$

A_4: Bob receives vacuum pulses, one two-photon pulse and at least one single-photon pulse. This event occurs with probability $\Pr[A_4] = Kp_2[(p_0+p_1)^{K-1} - p_0^{K-1}]$. We will assume here as before that Bob receives no vacuum pulses, which can only increase his cheating.

Let $\{M_{i,b}\}_{i\in[K],b\in\{0,1\}}$ be the POVM that Bob applies on all K pulses to determine the index i Alice and Bob will use as well as his guess b for Alice's bit c_i. Let j the index that corresponds to the two-photon pulse. We have

$$\begin{aligned}\Pr[x=0|A_4] &= \sum_{i\in[K]} \Pr[\text{Bob outputs}(i, b=c_i)] \\ &= \Pr[j]\cdot\Pr[b=c_j|j] + \sum_{i\neq j}\Pr[i]\cdot\Pr[b=c_i|i]\end{aligned}$$

From the analysis of A_2, we know that for any single-photon pulse with index i, we have $\Pr[b = c_i|i] \leq y + 2\epsilon_A$. Let $q = \Pr[j]$, then we have

$$\Pr[x = 0|A_4] = q \cdot \Pr[b = c_j|j] + (1-q)(y + 2\epsilon_A)$$

Let us now study the probability that Bob can guess the bit c_j that corresponds to the two-photon pulse. Using the notation from the previous events, the overall state Bob has in case $c_j = 0$ is $\sigma'_0 \otimes \gamma_{\neg j}$ and the state he has in case $c_j = 1$ is $\sigma'_1 \otimes \gamma_{\neg j}$ for some state $\gamma_{\neg j}$. The optimal probability for guessing c_j is given by the optimal POVM on the K pulses that distinguishes the states $\sigma'_0 \otimes \gamma_{\neg j}$ and $\sigma'_1 \otimes \gamma_{\neg j}$. This is again given by the Helstrom measurement and gives probability

$$P_{\text{opt}} = \frac{1}{2} + \frac{1}{2}\left|\left|\Pr[c_j = 0|j]\sigma'_0 \otimes \gamma_{\neg j} - \Pr[c_j = 1|j]\sigma'_1 \otimes \gamma_{\neg j}\right|\right|_1 \leq y + 2\epsilon_A$$

Let us now describe a specific strategy that Bob can perform in order to guess the value c_j of the two-photon pulse: He performs the POVM $\{M_{i,b}\}_{i\in[K],b\in\{0,1\}}$ and if the output is $(j,0)$ he output 0, if the output is $(j,1)$ he outputs 1, and in all other cases he outputs the most probable value. Let z the success probability of this strategy. Then, $z = q\Pr[b = c_j|j] + (1-q)(\frac{1}{2} + \epsilon_A)$. This yields the inequality $\frac{2z-1-2\epsilon_A}{1-2\epsilon_A} \leq q$. Also, we have $z \leq y + 2\epsilon_A$, from the optimality of the Helstrom measurement. This gives us:

$$\begin{aligned}
\Pr[x = 0|A_4] &= q \cdot \Pr[b = c_j|j] + (1-q)(y + 2\epsilon_A) \\
&= z + (1-q)(y - 1/2 + \epsilon_A) \\
&\leq z + (1 - \frac{2z-1-2\epsilon_A}{1-2\epsilon_A})(y - 1/2 + \epsilon_A) \\
&= \frac{2}{1-2\epsilon_A}\left(z(1-y-2\epsilon_A) + y - \frac{1}{2} + \epsilon_A\right)
\end{aligned}$$

Since the coefficient of z is positive for the values of y and ϵ_A that we consider, we can upper bound this probability by using $z \leq y + 2\epsilon_A$ and get:

$$\Pr[x = 0|A_4] \leq \frac{(-2y^2 + 4y - 1) + \epsilon_A(6 - 8y - 8\epsilon_A)}{1-2\epsilon_A} \tag{3.11}$$

Note that for $\epsilon_A = 0$, we recover the initial bound.

By combining Eqs. 3.8, 3.9, 3.10 and 3.11, and noticing that Bob's cheating is the same if he wants $x = 1$, we find that Bob can bias the coin with probability:

$$p_q^B \leq \sum_{i=1}^{4} \Pr[A_i] \cdot \Pr[x=0|A_i] + \left[1 - \sum_{i=1}^{4} \Pr[A_i]\right] \cdot 1 \tag{3.12}$$

An important part of our analysis is the symmetrization procedure that results in throwing away a lot of detection events, thus requiring more rounds K in order to achieve a specific honest abort probability. This increases the cheating probability since a malicious Bob benefits from the increased number of rounds.

3.7 Results

We performed quantum coin flipping experiments using fibres of 15 and 25 km, applying several values of mean photon number μ for each channel length. Based on the data obtained from the quantum transmission part of the protocol and taking into account the symmetrization procedure, we computed the number of protocol rounds K that are required to achieve a desired honest abort probability. The number of detection events used to calculate the required rounds K for a specific honest abort probability, is sufficiently large (typically 10^6) in order to ensure negligible finite-size effects in our implementation; for instance, for $H = 0.8\%$, the probability that the honest abort probability is greater by more than 0.2% is 10^{-9}.

For the specific system parameters, the cheating probability can then be computed using the security analysis of the basic quantum coin flipping protocol pertinent to the plug&play implementation. More specifically, by inserting the specific values for $\epsilon_A, \epsilon_B, \epsilon_B'$ from our implementation, given in Eqs. 3.5, 3.6 and 3.7, we calculate the cheating probability of the protocol. This also allows us to find, for both channel lengths, the sets of values for μ, K and y that minimize the cheating probability and at the same time make the protocol fair[4].

In Table 3.2 we provide the values of the experimental parameters used in the implementations for honest abort probability $H = 0.8\%$, where optimal values are shown in bold. We can observe that the number of required rounds, and hence the protocol runtime, decreases for higher values of μ, at the expense of slightly higher cheating probabilities. The parameters correspond to a fair protocol, for which the cheating probabilities for a malicious Alice or Bob are the same; this is ensured by the choice of the coefficient y.

To perform an experiment for a specific value of the average photon number per

[4] Note that for simplicity, the y values of our experimental data have been chosen independently of the honest abort probability value; in practice, slight modifications of these values might be required to achieve a perfectly fair protocol for each specific honest abort probability.

	15 km		25 km	
Coefficient y	0.88		0.85	
μ ($\times 10^{-3}$)	2.8 ± 0.1	$\mathbf{2 \pm 0.1}$	5 ± 0.1	$\mathbf{4 \pm 0.1}$
Protocol rounds K	88000	**131000**	130000	**174000**
Cheating probability	0.916 ± 0.002	$\mathbf{0.914 \pm 0.002}$	0.947 ± 0.003	$\mathbf{0.942 \pm 0.003}$

Table 3.2: Experimental parameter values for honest abort probability $H = 0.8\%$.

pulse μ, Alice applies a control signal to her variable attenuator, according to a previously established calibration relationship. The uncertainties in Table 3.2 come from the difference between the value of μ computed from this relationship, given the specific experimental conditions in the path from Bob's laser to Alice's attenuator, and the value of μ deduced from the actual detection events and the conditions in the path between Alice's output and Bob's detectors.

In Fig. 3.3 we show the cheating probability calculated from our experimental data for 15 and 25 km, as a function of the honest abort probability. For each value of the honest abort probability, the number of rounds K and mean photon number per pulse μ has been optimized as explained previously. The values correspond to a fair protocol, while the uncertainty in the estimation of μ is illustrated by the shaded areas in the plot. To quantify the advantage offered by quantum communication, we use the classical cheating probability bound p_c, defined in [16] and shown as a solid line in Fig. 3.3. We can see that the cheating probability is strictly lower than classically possible for a distance of 15 km, for a wide range of practical values of the honest abort probability (from 0.4% to 1.45%). The area corresponding to the data obtained at 25 km is just above the classical cheating bound for all honest abort probability values, which means that a quantum advantage cannot be claimed in this case.

To obtain further insight into our results, we define a gain function, as follows:

$$G = p_c - p_q,$$

where p_c is the classical cheating probability bound [16] and p_q is the quantum cheating probability value derived from our experimental data. If the data yield a positive G for a certain honest abort probability, it means that this result cannot be obtained by any purely classical means. We can then use the gain as a figure of merit to assess the performance of our quantum coin flipping implementation in a secure communication

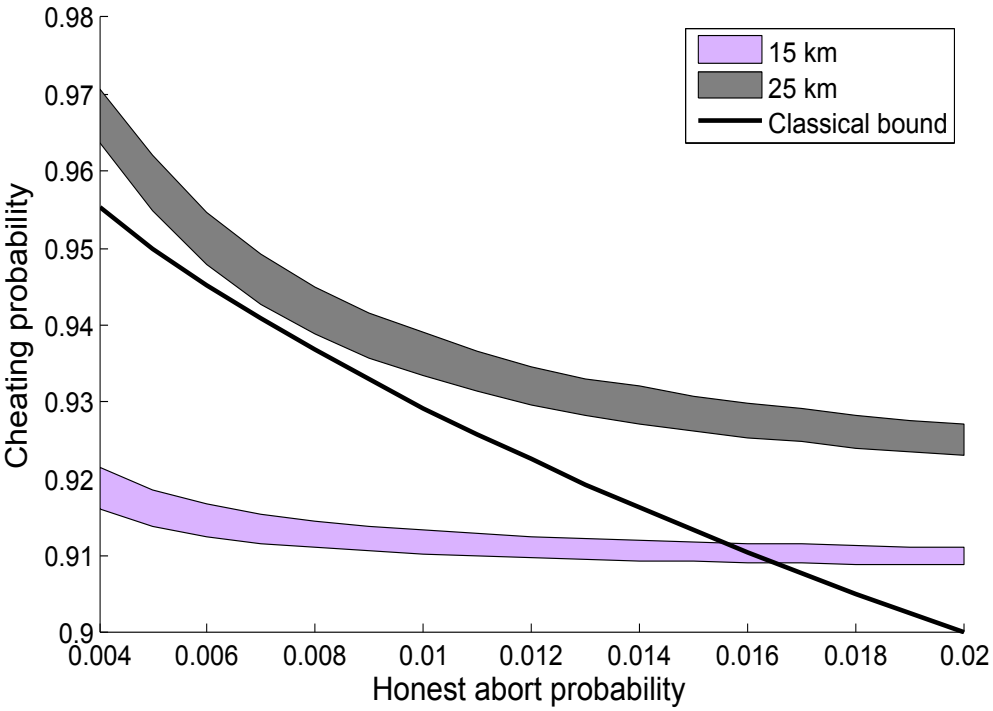


Figure 3.3: Cheating probability vs honest abort probability for 15 and 25 km

scenario. The diamonds in Fig. 3.4 correspond to the cheating probabilities achieved by our plug&play implementation for 15 and 25 km, for a fixed honest abort probability of 0.8% (also shown in bold in Table 3.2). For a channel length of 15 km, a distance which is sufficient for many applications requiring communication over metropolitan area networks, the gain is of the order of 2.5%, while for a channel length of 25 km no positive gain can be obtained. For comparison, previous experimental results based on an entangled-photon source implementation of a loss-tolerant quantum coin flipping protocol [15] are also shown in Fig. 3.4 with circles. In this work, a positive gain was experimentally obtained for a distance of 10 m, with an honest abort probability of 1.8%, while no positive gain was possible for a distance of 12 km.

Note that in the distrustful model with information-theoretic security, it is not known if it is possible for Alice and Bob to collaborate in order to increase the robustness of the implementation. This results in an inherent limitation to the attainable communication distance in our quantum coin flipping implementation. However, using better single-photon detectors with lower dark count rates for instance [68], can readily extend the range of our protocol.

Finally, in our implementation, the classical steps of the coin flipping protocol following the quantum transmission are not performed in real time. However, it is clear that the coin flipping rate will be dominated by the time that it takes for K pulses to travel from Alice to Bob. For a laser pulse repetition rate of 10 MHz, this corresponds roughly

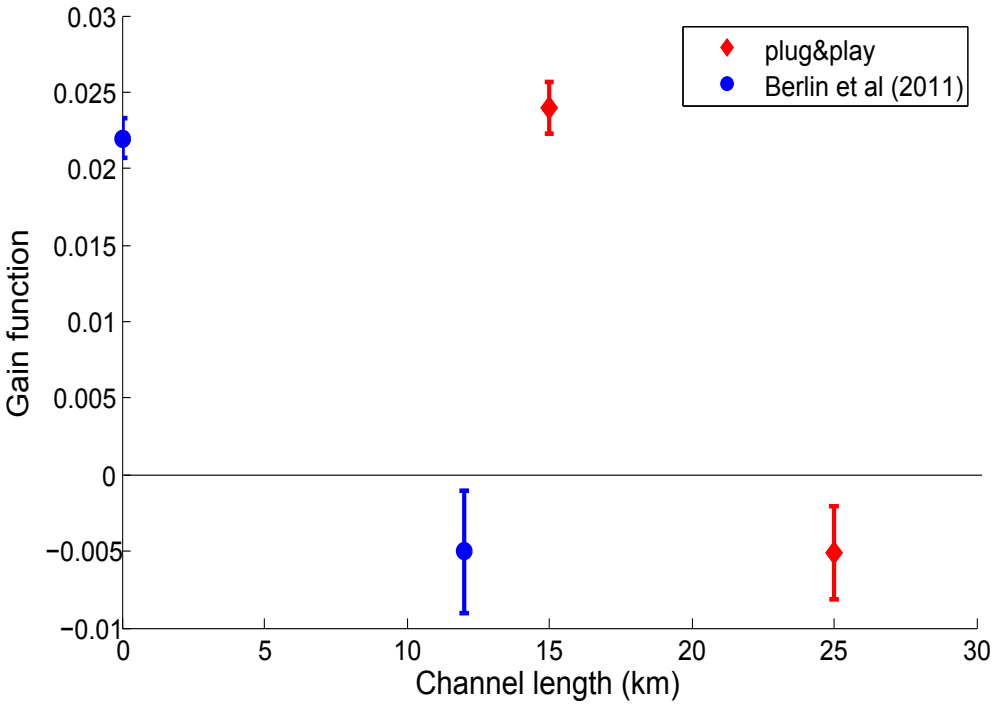


Figure 3.4: Gain as a function of channel length

to a few tens of coin flips per second. As we can see in Table 3.2, if Alice increases the average photon per pulse exiting her system, the required number of protocol rounds reduces, which also reduces the runtime for the protocol, but this comes at the expense of a slightly higher cheating probability. Again, using better single-photon detectors can result in a substantially lower number of required rounds. In a real communication scenario of two distrustful parties wishing to agree on a coin value using the plug&play system, the parties would be given a choice of gain values for a range of honest abort probabilities given their communication distance and the desired communication rate.

3.8 Enhancing the security of protocols against bounded adversaries

We have seen that our basic quantum coin flipping protocol achieves information-theoretic security, which is impossible classically. However, this security level comes at a price of a high bias; indeed, as we see in Fig. 3.3, the unbounded adversary can bias the coin with probability greater than 90%. This might not be suitable for some applications. It is then interesting to consider combining our protocol with protocols that achieve a bias asymptotically close to zero against bounded adversaries. Combining protocols with

different types of security is in fact a powerful concept, which is widely used in practice. This allows communications to remain secure not only at the present time but also in the future, accommodating at the same time for different types of adversaries with unknown or rapidly evolving technological and computational capabilities.

To construct combined protocols for quantum coin flipping, we apply the following general lines: We discern three stages, as in the commonly used protocols against bounded adversaries, including classical protocols employing one-way functions [9] and quantum protocols in the noisy quantum storage model [63, 69]. In the first stage (*commit*), which remains unchanged from the protocols against bounded adversaries, Alice and Bob exchange classical or quantum messages such that at the end of this stage each party has almost perfectly committed to one bit, S and T, respectively. In the second stage (*encrypt*), Alice and Bob encrypt their respective random bits using the committed values. In particular, Alice sends K pulses using the states $|\Phi_{\alpha_i, c_i \oplus S}\rangle$, for $i = 1, ..., K$, and Bob replies by sending $T \oplus b$ as well as j, the index of the first measured pulse, as in the basic protocol. In the third stage (*reveal*), Alice and Bob reveal (c_j, S) and (b, T), respectively, together with additional information depending on the underlying bounded adversary model and, if nobody aborts, the value of the coin is $c_j \oplus b$.

The combined protocols constructed as explained above achieve an almost perfect security against bounded adversaries, exactly as the original protocols; in addition, when the adversaries are unbounded, they still cannot cheat with a probability higher than the one provided by our basic quantum coin flipping protocol, which is strictly better than classically possible. Hence, these protocols offer the maximal possible security guarantees. Let us consider two particular cases, computationally bounded adversaries and adversaries with noisy quantum storage.

3.8.1 Computationally bounded quantum coin flipping

The computationally bounded protocol, Protocol 3.8.1, uses an injective one-way function f, upon which Alice and Bob have previously agreed [9]. In the *commit* stage of the protocol, Alice and Bob choose random strings, x_A and x_B, respectively, and commit to the bits $h(x_A)$ and $h(x_B)$ by exchanging $f(x_A)$ and $f(x_B)$, where h is a hardcore predicate of f. Hardcore predicates make it impossible to guess the value $h(x)$ from $f(x)$ with probability greater than one half. An example of a hardcore predicate function is the parity of the bits in a string, since it can be proven [9] that given the parity and the image of the string, it is not feasible to guess the string itself. Moreover, since f is an injective one-way function, by sending the values $f(x)$, neither of the two parties can lie about the value of their chosen string and thus change the value $h(x)$. Hence, at the end of this stage Alice and Bob have almost perfectly committed to $h(x_A)$ and $h(x_B)$. In the *encrypt* stage, for $i = 1, ..., K$, Alice randomly selects α_i and c_i and sends

the K quantum states $|\Phi_{\alpha_i, c_i \oplus h(x_A)}\rangle$ to Bob, prepared in the same way as in the basic quantum coin flipping protocol. Bob performs a measurement in the randomly selected bases $\{|\Phi_{\beta_i,0}\rangle, |\Phi_{\beta_i,1}\rangle\}$, and replies with the position j of the first successfully measured pulse and a random bit b encrypted as $b \oplus h(x_B)$. Finally, in the *reveal* stage, Alice and Bob reveal their strings and check that they are consistent with the function outputs exchanged during the *commit* phase. They also exchange their chosen bit and Bob aborts only if $\alpha_j = \beta_j$ and his measurement outcome does not agree with c_j. If he does not abort, the value of the coin is $c_j \oplus b$. Note that the *encrypt* stage and the first step of the *reveal* stage correspond to our basic quantum coin flipping protocol, slightly modified to fit the underlying computationally bounded model.

Alice		**Bob**
choose random string x_A	$\xrightarrow{f(x_A)}$	
	$\xleftarrow{f(x_B)}$	choose random string x_B
choose $\{\alpha_i, c_i\}_1^K$	$\xrightarrow{\|\Phi_{\alpha_i, c_i \oplus h(x_A)}\rangle}$	measure in $\{\beta_i\}_1^K$
	$\xleftarrow{j,\ b \oplus h(x_B)}$	j: first measured pulse, $b \in_R \{0,1\}$
	$\xrightarrow{x_A,\ c_j,\ \alpha_j}$	check consistency
check consistency	$\xleftarrow{x_B,\ b}$	

Protocol 3.8.1: **Computationally bounded quantum coin flipping**.

For the security analysis, if Alice is computationally bounded, then she cannot guess the value $h(x_B)$ with probability greater than one half, which means that Bob's bit b is perfectly hidden when Bob sends $b \oplus h(x_B)$. Therefore, the protocol remains almost perfectly secure against Alice. If Bob is computationally bounded, then the bits c_j are perfectly hidden as $c_j \oplus h(x_A)$, hence the protocol remains almost perfectly secure against Bob. If, on the other hand, the parties are unbounded, they can perfectly compute the hardcore predicates and the security of the protocol becomes exactly the same as the security of our basic coin flipping protocol.

3.8.2 Noisy storage quantum coin flipping

In the noisy storage model [63], Protocol 3.8.2 describes how to perform quantum coin flipping that remains secure against an adversary whose memory storage gets noisy over time. The parties first agree on an error-correcting code. This is followed by a *prepare* stage, where Alice sends to Bob $2n$ BB84 states[5]. Bob measures the states using randomly chosen bases $\{\hat{b}_i\}_1^{2n}$. At the end of this stage, Alice has a string containing the bits used to construct the states, namely $X^{2n} = X_1^n X_2^n$, and Bob has a string containing his measurement results, namely $\tilde{X}^{2n} = \tilde{X}_1^n \tilde{X}_2^n$. If the choices of the states and the measurement bases are uniformly random, then the strings agree on approximately half of the positions.

The parties then perform the main coin flipping protocol. In the *commit* stage, Alice and Bob commit to bits $D_A = \text{Ext}(X_1^n, r)$ and $D_B = \text{Ext}(\tilde{X}_2^n, \tilde{r})$, respectively, where $\text{Ext} : \{0,1\}^n \otimes R \to \{0,1\}$ is a family of 2-universal hash functions, and $(r, \tilde{r})$ are strings chosen by Alice and Bob in order to randomly pick a hash function from this family. To this end, they first calculate the syndromes $w = Syn(X_1^n)$ and $\tilde{w} = Syn(\tilde{X}_2^n)$ based on the previously agreed error-correcting code. Then they commit to the extractor function values by exchanging the syndromes and half of the bases' values they used in the measurements. In the *encrypt* stage, Alice encrypts her bit choices c_j by sending K states $|\Phi_{\alpha_j, c_j \oplus D_A}\rangle$, prepared as in the basic quantumprotocol. Bob chooses randomly β_j and measures in $\{|\Phi_{\beta_j,0}\rangle, |\Phi_{\beta_j,1}\rangle\}$. He then encrypts a bit b by sending $b \oplus D_B$ to Alice, together with the index m of the first successfully measured pulse. Finally, in the *reveal* stage, Alice and Bob reveal their string and bit values and check that for the positions with the same bases, X_2^n coincides with $\tilde{X}_2^n$ and X_1^n coincides with $\tilde{X}_1^n$, respectively. They also check that the syndromes and extractor outputs correspond to the received strings. If the measurement outcome for the first measured pulse agrees with the revealed bit for the same choice of bases or if the bases are different, they agree on the coin $c_m \oplus b$, otherwise they abort. Again, the *encrypt* stage and the first step of the *reveal* stage correspond to the basic quantum coin flipping protocol.

In order to increase their cheating probability, dishonest parties seldom do not want to measure at a specified (by the protocol) stage, but they prefer to keep their state unmeasured in case they receive extra information that will help them better decide what type of operation to perform on it. The fact that they are obliged to wait for a time preiod Δt in enough to convince them to measure their states when dictated by the protocol, since the noisy memory will destroy any information that the quantum state might hold, resulting in random noise. So Bob is forced to measure the states sent by Alice and Alice is forced to measure whatever entangled share she may have kept when sending the states to Bob.

[5] These are the same as the states used in the basic quantum coin flipping protocol, when we set $y = 1/2$.

Concerning the security analysis, if Alice has noisy storage, then she cannot guess the value D_B with probability greater than one half, hence Bob's bit b is perfectly hidden from her when Bob sends $b \oplus D_B$. Therefore, the protocol remains almost perfectly secure against Alice. If Bob has noisy storage, then again the bits c_j are perfectly hidden as $c_j \oplus D_A$ and the protocol remains almost perfectly secure against Bob. If, on the other hand, the parties have perfect memory, they can perfectly compute the values D_A and D_B and the security of the protocol reduces exactly to the security of our basic quantum coin flipping protocol.

Alice		**Bob**
choose $\{b_i, x_i\}_1^{2n}$	$\xrightarrow{\lvert\hat{\Phi}_{b_i,x_i}\rangle}$	measure in $\{\hat{b}_i\}_1^{2n}$
String:		String:
$X^{2n} = X_1^n X_2^n$		$\tilde{X}^{2n} = \tilde{X}_1^n \tilde{X}_2^n$
$\lvert X_1^n\rvert = \lvert X_1^n\rvert = n$,		$\lvert\tilde{X}_1^n\rvert = \lvert\tilde{X}_1^n\rvert = n$
Wait time Δt		
$w = Syn(X_1^n)$,		$\tilde{w} = Syn(\tilde{X}_2^n)$,
string r		string $\tilde{r}$
$D_A = Ext(X_1^n, r)$	$\xrightarrow{\{b_i\}_1^n,\ w,\ r}$	$D_B = Ext(\tilde{X}_2^n, \tilde{r})$
	$\xleftarrow{\{\tilde{b}_i\}_{n+1}^{2n},\ \tilde{w},\ \tilde{r}}$	
choose $\{\alpha_j, c_j\}_1^K$	$\xrightarrow{\lvert\Phi_{\alpha_j, c_j \oplus D_A}\rangle}$	measure in $\{\beta_j\}_1^K$
	$\xleftarrow{D_B \oplus b,\ m}$	m: 1st measured pulse
	$\xrightarrow{X_1^n, c_m}$	
	$\xleftarrow{\tilde{X}_2^n,\ b}$	
check:		check:
$X_2^n \sim \tilde{X_2^n}$ where bases agree		$X_1^n \sim \tilde{X_1^n}$ where bases agree
$Syn(\tilde{X}_2^n) = \tilde{w}$		$Syn(X_1^n) = w$
$Ext(\tilde{X}_2^n, \tilde{r}) = D_B$		$Ext(X_1^n, r) = D_A$

Protocol 3.8.2: **Noisy storage quantum coin flipping.**

3.9 Conclusion

We have shown that flipping a single coin with security guarantees that are strictly stronger than in any classical protocol can be achieved with present quantum technology, and more precisely with a standard attenuated laser source. This implies that quantum information can be used beyond quantum key distribution (QKD), to achieve in practice more difficult cryptographic tasks in a model where the parties do not trust each other. Even though the cheating probability of the basic quantum coin flipping protocol is higher than 90%, it provides security against the most powerful type of adversary, one who has perfect equipment, has full knowledge of the other player's errors and loss rates, and controls all imperfections in the communication channel. In future telecommunication networks, there will be several types of adversaries that could also be bounded by physical restrictions, or by their computational power. By combining our quantum coin flipping protocol with protocols secure against bounded adversaries, we enhance them with a level of information-theoretic security, assuring that an honest party will always obtain security guarantees stronger than possible by classical means.

It is also interesting to note that our protocol is based on a bit commitment scheme, augmented only by an additional classical message from Bob to Alice between the commit and reveal stages. This means that our combined coin flipping protocols can also be viewed as commitment schemes where both parties commit to some value. Hence, our security analysis can be extended in a straightforward way to hold for bit commitment in the computational models that we have considered. In the same way, our implementation indeed performs plug and play quantum bit commitment. We also note that a weaker, but still very powerful variant called weak coin flipping, with almost perfect information-theoretic security, is in theory possible with quantum technology [54, 70]. Our implementation is a first step towards making such protocols a reality, however the quantum protocols that achieve almost perfect security are not well understood and currently necessitate large-dimension entangled states. Simplifying such protocols is an important open question.

We observe that the maximal communication distance that can be achieved is significantly smaller than in QKD [44]; with the parameter values that we used, the limit to the channel length is around 20km. This is because in principle, dealing with distrustful parties is more complicated than the quantum key distribution scenario, both in theory and in practice. For example, although randomized procedures like error correction and privacy amplification that are widely employed in QKD have been used in the security analysis of protocols dealing with bounded adversaries [67], it is an open question whether such procedures can be used in the information-theoretic security setting. It is possible that any such subroutine could be used by the malicious party to his or her advantage. On the other hand, it would be particularly interesting to see if there is a

way to increase the channel length by reducing the effect of noise to the honest abort probability. We note that a priori this seems hard, since any attempt of Alice to protect the qubits, via a repetition error-correcting code for example, will immediately increase the cheating probability of Bob. Therefore, new techniques may be needed in order to deal with the imperfections of the implementation and the inherent limitations to the attainable communication distance.

It is important to note that the advantage of the plug&play system with respect to other systems providing the functionalities required by our protocol is that it offers a particularly robust and stable implementation. This specific interferometric setup compensates for all fluctuations in the channel, allowing to perform experiments at low signal level for long time duration, resulting in very reliable results and an excellent system stability. The plug&play system can also potentially be used for protocols employing decoy states [71–73]. Although the use of decoy states is a powerful tool for achieving practical long-distance quantum key distribution and for improving the performance of quantum cryptographic protocols in the noisy storage model [67], it is not known, if a protocol employing decoy states can be devised for quantum coin flipping providing security against all-powerful adversaries.

Our quantum coin flipping implementation takes explicitly into account the standard imperfections (multi-photon emission, transmission loss, detector inefficiency and dark counts) present in practical systems. We also consider imperfections related to asymmetries in the detection efficiency and basis-dependent flaws in the components of Alice's and Bob's devices, which play a crucial role for the practical security of the implementation. It is clear, however, that similarly to QKD experiments, further deviations between the security proof and the actual implementations inevitably exist and can lead to side-channel attacks by the adversary. Although an exhaustive analysis of possible side channels is out of the scope of the present work, we examine a few prominent cases known in the context of QKD demonstrations, some of which are particularly relevant for the plug&play system at the basis of our implementation.

In the setting of quantum key distribution, an efficient eavesdropping attack that also applies to the plug&play system consists in shifting in time the second pulse (see Fig. 3.2) such that this pulse is only partially modulated by Alice's phase modulator. This so-called phase remapping attack [74, 75] effectively alters the relative phase between the two pulses and allows Eve to obtain key information for ranges of quantum bit error rate values that would otherwise be considered acceptable. In the distrustful setting of quantum coin flipping, malicious Bob attempts to maximize his cheating probability by performing an optimal measurement to the received states, and so reducing the probability of distinguishing them cannot help him. Additionally, errors in the state preparation performed by Alice have been considered in detail in the security analysis of our implementation. Similarly, attacks exploiting the loophole introduced by detection

efficiency mismatch, such as the time-shift attack [76–78], are, in principle, excluded by the symmetrization procedure included in our experimental protocol. Finally, an effective countermeasure against the powerful blinding attack [79], where the single-photon detectors are brought to a classical operation regime and can be fully controlled by the adversary, consists in randomly suppressing detector gates and emitting an alarm signal in case of registered detection events during those gates. This countermeasure is implemented in our system.

In general, Bob's cheating probability depends on the mean photon number per pulse that exits Alice's system. In our security proofs, we assume that Alice can control the number of photons that she emits, using a high-precision powermeter. However, since it is Bob who has the laser source, if he can somehow manage to bypass Alice's countermeasure and increase the number of multiphoton pulses that he receives, then he can increase his cheating probability.

In addition to the aforementioned side-channel attacks, it is important to note the issue of phase randomization [80], which is an assumption typically made in security proofs and hence should be satisfied in practice. Phase randomization together with suitable intensity monitoring are also required for the characterization of an untrusted source, which is particularly relevant for the plug&play system [81]. Although all the hardware components necessary for implementing active phase randomization and source characterization at Alice's site are available in our system, these processes were not performed in real time, due mainly to the difficulty in generating random real numbers in real time and to the limited bandwidth of the threshold discriminator used for intensity monitoring. Clearly, for any real-life implementation, following such procedures is essential.

Chapter 4

Entanglement Verification

Entanglement plays a key role in the study and development of quantum information theory. It has been widely used in all aspects of quantum information and has been essential to show the advantages obtained compared to the classical setting. Initially defined for bipartite states, the notion of entanglement has been generalized to multipartite systems and despite the complexity this notion acquires in this case, many interesting properties of multipartite entangled states are known. For example, we saw in Section 2.3.2, how the quantum correlations of the Greenberger-Horne-Zeilinger (GHZ) state [17] and its n-party generalization help win a specific game with probability 1 in the quantum setting, while any classical local theory can win with probability at most 3/4 [18].

Multipartite entangled states are a fundamental resource when quantum networks are considered. Indeed, they allow network agents to create strong correlations in order to perform distributed tasks, to delegate computation to untrusted servers [19], or to compute, for example through the Measurement-Based Quantum Computation model [20]. A natural and fundamental question that arises then is whether the network agents should be required to trust the source that provides them with such multipartite entangled states or whether they are able to verify the entanglement.

Most of the work on entanglement verification has considered the case where all parties are honest. For two parties, three models have been studied:

First, the standard model, where both parties trust their devices but they do not trust the source. This model corresponds to the setting of non-separability tests, where the two parties can perform together quantum tomography on the state distributed by the source and thus verify the existence of entanglement. In a cryptographic language, this corresponds to a setting where both parties are guaranteed to be honest. A related question concerning untrusted sources in quantum key distribution protocols is discussed in [82].

Second, the device independent model, where the parties trust neither their quantum

devices nor the source. This model is related to the well known setting of the Bell nonlocality tests as well as to self-testing [83].

Third, the one-sided device independent model [84], where the security is asymmetric: one party trusts his devices but the second party's devices and the source are untrusted. This model corresponds to the setting of generalized quantum steering [85, 86], where one party is also given control of the source and tries to convince the other party, who trusts his devices, that she can create entanglement. In a cryptographic language, an honest party tries to verify entanglement in the presence of a dishonest party who controls the source. Recently, there have been experimental demonstrations in this model [87–89].

For the multipartite case, much less is known. In the standard model, pseudo-telepathy [21, 90] extends Mermin's game [18] to many parties; a maximally entangled state is used to play the game and wins with probability one, which is strictly better than in the classical case. In the device independent model, it was shown that honest parties who do not trust their devices can verify genuine multipartite entanglement by using appropriate entanglement witnesses [91]. Another interesting construction for self-testing graph states appears in [92]. Finally, in [93] the authors present a unified framework for n-party entanglement verification and provide inequalities with different bounds for the different nonlocality classes that are considered.

However, not much work has been done from a cryptographic point of view in the multiparty setting. All the above-mentioned work considered either one party (self-testing) who receives the high dimensional state, and wants to verify the entanglement in the state and/or the measurement devices, or many parties (pseudo-telepathy) who are nevertheless all honest.

In this chapter, we will consider a multi-party scenario where each party receives one qubit from a source that is untrusted. Their goal is to verify that the source is sharing a maximally entangled state. Furthermore, they do not trust each other, which means that an unbounded number of parties might form a dishonest coalition, in order to convince the honest parties to accept the shared state. In order to provide the maximal security guarantees, we will consider that the dishonest parties are controlled by the source, and therefore can strategically announce their measurement outputs, to increase the probability to achieve their goal. It should be assumed that the honest parties do not know which other parties are honest, but the dishonest parties know which parties belong to the dishonest coalition.

The structure of the chapter is the following: In Section 4.1, we discuss some closely related protocols of pseudotelepathy and communication complexity. In Section 4.2 we propose a protocol that allows a verifier to check an entangled source, under perfect conditions, i.e. there are no losses or errors present in the model. In Section 4.3, we investigate the effect of losses and noise on our protocol, and propose an enhanced version of the original protocol that can tolerate certain amounts of system imperfections.

Finally, in Section 4.4 we provide a practical experimental procedure for multiparty entangled states, that can be used in order to demonstrate the advantage of the new enhanced protocol in comparison with the old one. This procedure is currently being implemented using 3-party and 4-party entangled states [30].

4.1 Previous Work

In Section 2.3.2, we saw how three entangled parties can always win the Mermin-GHZ game, while in the absence of prior entanglement, they would not be able to win with probability one. This property of a quantum protocol, i.e. to be able to reduce or even eliminate the need for classical communication using entanglement, is called *pseudo-telepathy*. In general, given a game with a promise on the inputs, a protocol exhibits pseudo-telepathy if, with the help of shared entanglement, it wins the game with certainty on all inputs that satisfy that promise, while no such classical protocol exists. Here we present a natural multiparty extension of the Mermin-GHZ Game [21] that was the motivation for the work to be presented later in this chapter.

Pseudo-telepathy Game

n parties A_j who are not communicating between them ($n \geq 3$)

1. Each party A_j receives an input bit $x_j \in \{0,1\}$, such that

$$\sum_{j=1}^{n} x_j = 0 \pmod 2$$

2. Each party outputs bit $y_j \in \{0,1\}$

3. The game is won if

$$\bigoplus_{j=1}^{n} y_j \equiv \frac{1}{2}\sum_{j=1}^{n} x_j \pmod 2$$

It can be proven that:

Theorem 3. *If the parties are sharing a maximally entangled n-party state, then they can always win the above game.*

The proof assumes that the parties are sharing a GHZ state $|G_0^n\rangle = \frac{1}{\sqrt{2}}|0^n\rangle + \frac{1}{\sqrt{2}}|1^n\rangle$ and measure in the X direction when they get input 0, and in the Y direction when they get input 1. Without any prior entanglement, the following theorem holds:

Theorem 4. *Without any shared entanglement, the above game can not be won with probability more than* $\frac{1}{2} + 2^{-\lceil n/2 \rceil}$.

The same multiparty game can be rephrased in the context of *communication complexity*, as was done in the work of Buhrman, van Dam, Hoyer and Tapp (BDHT) [94]. In general, the communication complexity of a function f with k variables is the minimum number of classical bits required to be broadcasted from all n parties in order to know the value of f on their collective input.

BDHT Protocol
n parties A_j that are not communicating between them ($n \geq 3$),
function f with k variables

1. Each party A_j receives input $x_j \in \{0, \ldots, 2^k - 1\}$, such that

$$\sum_{j=1}^{n} x_j = 0 \pmod{2^{k-1}}$$

2. Each party broadcasts a bitstring $\mathbf{y}_j$.

3. At the end of the protocol, all parties should be able to compute the function

$$f(\mathbf{x}) = f(x_1, \ldots, x_n) = \frac{1}{2^{k-1}}\Big[\Big(\sum_{j=1}^{n} x_j\Big) \pmod{2^k}\Big]$$

Theorem 5. *If the n parties share prior entanglement, then they only need to broadcast one bit each in order for all of them to be able to compute the value of function* f. *The communication complexity is therefore n.*

The proof assumes that the parties are sharing a GHZ state $|G_0^n\rangle = \frac{1}{\sqrt{2}}|0^n\rangle + \frac{1}{\sqrt{2}}|1^n\rangle$ and each party A_j applies a phase-change operation to their qubit that depends on the input x_j: $|0\rangle \rightarrow |0\rangle$ and $|1\rangle \rightarrow exp(\frac{2\pi x_j}{2^k} i)|1\rangle$. The promise on the inputs x_j makes the resulting state to be the $\frac{1}{\sqrt{2}}(|0^n\rangle + (-1)^{f(\mathbf{x})}|1^n\rangle)$. All the parties then measure in the Hadamard basis and it is easily proven that the sum of their measurement outputs $y_1 + \cdots + y_n \pmod 2$ is equal to $f(\mathbf{x})$. This means that each parties only needs to output a single bit $y_j \in \{0, 1\}$, in order for all parties to be able to compute $f(\mathbf{x})$.

When there is no prior entanglement shared between the parties, the following theorem holds:

Theorem 6. *If the n parties do not share prior entanglement and $k \geq \log_2 n$, then the number of bits to be communicated so that every party can compute $f(\mathbf{x})$, is always more than $n \log_2 n - n$.*

We have therefore seen the advantage of sharing a maximally entangled state in two different contexts, pseudo-telepathy and communication complexity. It is worthwhile noting that the certainty of winning the game comes from the sharing of a maximally entangled state. If the state is not a perfect GHZ, or equivalently, if there is noise in the channel or the detectors, the winning probability could potentially be lower than one. The presence of imperfections in the system (errors and losses in the transmission and detection) was already briefly discussed in [21]. They provided a lower bound on the amount of errors and losses that the protocol can tolerate, in order to be sure that the results cannot be reproduced classically. Nevertheless, all parties in this scenario are considered honest, and the errors and losses are thought to be happening independently to each party.

In the next sections we will look at the multiparty Mermin game from another perspective, that of entanglement verification, where some dishonest parties are using their losses and errors to convince the honest parties that they are sharing a maximally entangled state (or equivalently, to win the game with high probability).

4.2 Entanglement Verification under perfect conditions

We start our analysis by first describing in detail our model:

Source: The source is untrusted. It is supposed to create the n-party GHZ state $|G_0^n\rangle = \frac{1}{\sqrt{2}}\left(|0^n\rangle + |1^n\rangle\right)$ and distribute it to n parties. In reality, it is allowed to share any n-party state or entangle it with any auxiliary space.

Parties: The honest parties do not know which parties are honest and which are dishonest. The dishonest parties are thought to act as one unit, controlled by the source, and they are also considered to have perfect equipment and perfect channels connecting them with other parties. Their goal is to convince the honest parties that they share a GHZ state, while in reality they actually share an ϵ-away state (we will define later what this means).

Local resources: All parties have a trusted single-qubit measurement device with two measurement settings.

Network resources: Every pair of parties shares a private classical channel, which keeps the classical communication between two honest parties secret. This is the standard setup for classical networks with dishonest parties, since in the absence of private channels we cannot guarantee security for more than a single honest party.

4.2.1 The Basic Verification Protocol

We consider a source that is sharing a state $|\Psi\rangle$ with n parties. The source wants to convince an honest party, called the Verifier, that it can actually create and share an n-party GHZ state.

Basic Verification Protocol

The source shares a state $|\Psi\rangle$ with n parties.

1. The Verifier selects for every party A_j ($j = 1, \ldots n$) a random input $x_j = \{0, 1\}$, such that
$$\sum_{j=1}^{n} x_j \equiv 0 \pmod 2 \tag{4.1}$$
and sends it to the corresponding party via a private classical channel.

2. Each party A_j measures in the basis:
$$\{|x_j^+\rangle, |x_j^-\rangle\} = \{\frac{|0\rangle + e^{i\frac{\pi}{2}x_j}|1\rangle}{\sqrt{2}}, \frac{|0\rangle - e^{i\frac{\pi}{2}x_j}|1\rangle}{\sqrt{2}}\}$$

3. Each party sends y_j to the Verifier according to the measurement outcome. If the outcome is the “positive" basis vector $|x_j^+\rangle$ then $y_j = 0$, else if the outcome is the “negative" basis vector $|x_j^-\rangle$, then $y_j = 1$.

4. The Verifier accepts the state $|\Psi\rangle$ if the test T succeeds:
$$T(|\Psi\rangle): \quad \bigoplus_j y_j = \frac{1}{2}\sum_j x_j \pmod 2 \tag{4.2}$$

We denote by $T(|\Psi\rangle)$ the outcome of the above test on state $|\Psi\rangle$ (it is equal to 1 if the state passes the test and 0 if it fails).

4.2.2 Correctness of the Basic Verification Protocol

We want to show that the GHZ state passes the previous test with probability 1. The measurements that the parties are performing are equivalent to rotation operators around the $\hat{z}$ axis:

$$R_z(x_j) = \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\frac{\pi}{2}x_j} \end{bmatrix}$$

followed by a measurement in the X (Hadamard) basis $\{\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$. After the application of the rotation operators $R_z(x_j)$ on the GHZ state, we end up with the state $\frac{1}{2}\big(|0\rangle^n + e^{-i\frac{\pi}{2}R}|1\rangle^n\big)$, where $R = \sum_{j=1}^{n} x_j \pmod 4$. From the promise on the inputs, there are two cases:

- when $R = 0 \pmod 4$ the final state is the $|G_0^n\rangle = \frac{1}{\sqrt{2}}(|0^n\rangle + |1^n\rangle)$, so when performing a Hadamard transformation to all qubits of this state, we get an equal superposition of n-bit strings that have an even number of 1's. This means that the sum of all outputs y_j when each qubit is measured in the computational basis, is equal to $0 \pmod 2$.

- when $R = 2 \pmod 4$ the final state is the $\frac{1}{\sqrt{2}}(|0^n\rangle - |1^n\rangle)$, so when performing a Hadamard transformation to all qubits this state, we get an equal superposition of n-bit strings that have an odd number of 1's. This means that the sum of all outputs y_j when each qubit is measured in the computational basis, is equal to $1 \pmod 2$.

It is evident that the test T (4.2) is always correct when the parties share a GHZ state ($T(|G_0^n\rangle) = 1$), for all inputs that respect the condition 4.1 .

4.2.3 Security in the Honest Model

First, we suppose that all n parties are honest and we want to find out what is the probability that our Test T accepts a state as a function of the distance of this state to $|G_0^n\rangle$. Denoting by $D(|\psi\rangle, |\phi\rangle)$ the trace distance between two states $|\psi\rangle$ and $|\phi\rangle$, we have:

Theorem 7 (Honest Case)**.** *Let $|\Psi\rangle$ be the state of all n parties. If $D(|\Psi\rangle, |G_0^n\rangle) = \epsilon$, then* $\Pr[T(|\Psi\rangle) = 1] \leq 1 - \frac{\epsilon^2}{2}$.

Proof. We will prove the theorem by induction on the number of the parties. In order to do that, we need to generalise our test. We therefore extend the test 4.2 in order to verify a rotated GHZ state of the form:

$$|G_R^n\rangle = \frac{1}{\sqrt{2}}\left(|0^n\rangle + e^{i\frac{\pi}{2}R}|1^n\rangle\right) \tag{4.3}$$

where $R \in \{0,1,2,3\}$ and n is the number of parties. An important property of the state $|G_R^n\rangle$ is that it can be written in the following form:

$$|G_R^n\rangle = \frac{1}{\sqrt{2}}\left(|G_a^k\rangle|G_{R-a}^{n-k}\rangle + |G_{a+2}^k\rangle|G_{R-a+2}^{n-k}\rangle\right) \tag{4.4}$$

for every subset k of the n parties and for every $a \in \{0,1\}$.

In this test, each party A_j receives an input $x_j \in \{0,1\}$. We have a promise on the inputs of the parties: $\sum_{j=1}^n x_j \equiv R \pmod 2$. The measurements of the parties are defined by their inputs in the same way as before and the verification test for the state $|G_R^n\rangle$, is the following:

$$\bigoplus_{j=1}^n y_j = \frac{\sum_{j=1}^n x_j - R}{2} \pmod 2 \tag{4.5}$$

Let $\{E_R^n, \mathbb{I}_n - E_R^n\}$ be the POVM measurement that corresponds to the combined measurements that the parties are doing, where E_R^n is the element that corresponds to the test being successful and $\mathbb{I}_n$ the 2^n-identity matrix. We will prove by induction to the number of the parties that:

$$E_R^n = |G_R^n\rangle\langle G_R^n| + \frac{1}{2}I_R^n \tag{4.6}$$

where I_R^n is the projection to the space orthogonal to $|G_R^n\rangle$ and $|G_{R+2}^n\rangle$. Note also that $E_R^n + E_{R+2}^n = \mathbb{I}_n$.

What Eq. 4.6 means, is that the state $|G_R^n\rangle$ always passes the test, its orthogonal state $|G_{R+2}^n\rangle$ never passes the test, and the rest of the vectors in the orthogonal space, pass with probability 1/2.

For n=1, party A_1 receives x_1 and wants to verify that he has the state $|G_{x_1}^1\rangle$. It holds

that $E_R^1 = |G_{x_1}^1\rangle\langle G_{x_1}^1|$ and $\mathbb{I}_1 - E_R^1 = E_{R+2}^1 = |G_{x_1+2}^1\rangle\langle G_{x_1+2}^1|$. Since the vectors $|G_{x_1}^1\rangle$ and $|G_{x_1+2}^1\rangle$ span the whole space (i.e. $I_R^1 = \emptyset$), the test in Eq. 4.5 corresponds to the POVM $\{E_R^1, \mathbb{I}_1 - E_R^1\}$, and Eq. 4.6 holds for $n = 1$.

We then assume that Eq. 4.6 is true for n and we show the statement for $n+1$. Let $\{E_R^{n+1}(x_1), \mathbb{I}_{n+1} - E_R^{n+1}(x_1)\}$ be the POVM that corresponds to the measurement of the parties for a given input x_1 of party A_1. There are two cases:

1. Party A_1 outputs $y_1 = 0$. This means that the measurement outcome is $|G_{x_1}^1\rangle\langle G_{x_1}^1|$. Then, the test that the rest of the parties need to pass is:

$$\bigoplus_{j=2}^{n+1} y_j = \frac{\sum_{j=2}^{n+1} x_j - (R - x_1)}{2} \pmod 2 \tag{4.7}$$

2. Party A_1 outputs $y_1 = 1$. This means that the measurement outcome is $|G_{x_1+2}^1\rangle\langle G_{x_1+2}^1|$. Then, the test that the rest of the parties need to pass is:

$$\bigoplus_{j=2}^{n+1} y_j = \frac{\sum_{j=2}^{n+1} x_j - (R - x_1 + 2)}{2} \pmod 2 \tag{4.8}$$

Let $R_{\neg 1} \equiv \sum_{j=2}^{n+1} x_j \pmod 4$ be the input of all parties except A_1, which means also that $R_{\neg 1} = R - x_1 \pmod 4$. From the induction for n parties, we know that Test 4.7 is equivalent to measuring $E_{R_{\neg 1}}^n$ and Test 4.8 is equivalent to measuring $E_{R_{\neg 1}+2}^n$, where we need to keep in mind that

$$E_{R_{\neg 1}+2}^n = \mathbb{I}_n - E_{R_{\neg 1}}^n = |G_{R_{\neg 1}+2}^n\rangle\langle G_{R_{\neg 1}+2}^n| + \frac{1}{2} I_R^n$$

The POVM element that passes the test:

$$\bigoplus_{j=1}^{n+1} y_j = \frac{\sum_{j=1}^{n} x_j - R}{2} \pmod 2 \tag{4.9}$$

for a given x_1, is the following:

$$
\begin{aligned}
E_R^{n+1}(x_1) &= |G^1_{x_1}\rangle\langle G^1_{x_1}| \otimes E^n_{R_{\neg 1}} + |G^1_{x_1+2}\rangle\langle G^1_{x_1+2}| \otimes (\mathbb{I}_n - E^n_{R_{\neg 1}}) \\
&= |G^1_{x_1}\rangle\langle G^1_{x_1}| \otimes |G^n_{R_{\neg 1}}\rangle\langle G^n_{R_{\neg 1}}| + |G^1_{x_1+2}\rangle\langle G^1_{x_1+2}| \otimes |G^n_{R_{\neg 1}+2}\rangle\langle G^n_{R_{\neg 1}+2}| \\
&+ \frac{1}{2}\Big(|G^1_{x_1}\rangle\langle G^1_{x_1}| + |G^1_{x_1+2}\rangle\langle G^1_{x_1+2}|\Big) \otimes I^n_R \\
&= |G^{n+1}_R\rangle\langle G^{n+1}_R| + |\Phi^{n+1}_{x_1,R}\rangle\langle \Phi^{n+1}_{x_1,R}| + \frac{1}{2}\mathbb{I}_1 \otimes I^n_R
\end{aligned}
$$

where for a given $R \in \{0,1,2,3\}$, and for $x_1 \in \{0,1\}$, we define:

$$
|\Phi^{n+1}_{x_1,R}\rangle = \frac{1}{\sqrt{2}}\Big(|G^1_{x_1}\rangle|G^n_{R-x_1}\rangle - |G^1_{x_1+2}\rangle|G^n_{R-x_1+2}\rangle\Big)
$$

and we can further expand the two states for $x_1 = \{0,1\}$:

$$
\begin{aligned}
|\Phi^{n+1}_{0,R}\rangle &= \frac{1}{\sqrt{2}}\Big(|1\rangle|0^n\rangle + e^{i\frac{\pi}{2}R}|0\rangle|1^n\rangle\Big) && (4.10) \\
|\Phi^{n+1}_{1,R}\rangle &= \frac{i}{\sqrt{2}}\Big(|1\rangle|0^n\rangle - e^{i\frac{\pi}{2}R}|0\rangle|1^n\rangle\Big) && (4.11)
\end{aligned}
$$

Since x_1 is a bit chosen uniformly at random, we have that:

$$
\begin{aligned}
E^{n+1}_R &= \frac{1}{2}\sum_{x_1=0}^{1} E^{n+1}_R(x_1) \\
&= |G^{n+1}_R\rangle\langle G^{n+1}_R| + \frac{1}{2}\Big[|\Phi^{n+1}_{0,R}\rangle\langle \Phi^{n+1}_{0.R}| + |\Phi^{n+1}_{1,R}\rangle\langle \Phi^{n+1}_{1,R}| + \mathbb{I}_1 \otimes I^n_R\Big] && (4.12)
\end{aligned}
$$

We can verify that:

$$
\begin{aligned}
\mathbb{I}_{n+1} &= \mathbb{I}_1 \otimes \mathbb{I}_n = \Big(|G^1_0\rangle\langle G^1_0| + |G^1_2\rangle\langle G^1_2|\Big) \otimes \Big(|G^n_R\rangle\langle G^n_R| + |G^n_{R+2}\rangle\langle G^n_{R+2}| + I^n_R\Big) \\
&= |G^{n+1}_R\rangle\langle G^{n+1}_R| + |G^{n+1}_{R+2}\rangle\langle G^{n+1}_{R+2}| + |\Phi^{n+1}_{0,R}\rangle\langle \Phi^{n+1}_{0,R}| + |\Phi^{n+1}_{1,R}\rangle\langle \Phi^{n+1}_{1,R}| + \mathbb{I}_1 \otimes I^n_R
\end{aligned}
$$

and we can express the projection I_R^{n+1} to the space orthogonal to $|G_R^{n+1}\rangle$ and $|G_{R+2}^{n+1}\rangle$ as:

$$\begin{aligned} I_R^{n+1} &= \mathbb{I}_{n+1} - |G_R^{n+1}\rangle\langle G_R^{n+1}| - |G_{R+2}^{n+1}\rangle\langle G_{R+2}^{n+1}| \\ &= |\Phi_{0,R}^{n+1}\rangle\langle\Phi_{0,R}^{n+1}| + |\Phi_{1,R}^{n+1}\rangle\langle\Phi_{1,R}^{n+1}| + \mathbb{I}_1 \otimes I_R^n \end{aligned}$$

Eq. 4.12 then becomes:

$$E_R^{n+1} = |G_R^{n+1}\rangle\langle G_R^{n+1}| + \frac{1}{2} I_{S_{n+1}}$$

We have therefore managed to prove that for a rotated GHZ state $|G_R^n\rangle = \frac{1}{\sqrt{2}}(|0^n\rangle + e^{i\frac{\pi}{2}R}|1^n\rangle)$, the corresponding verification test is equivalent to the POVM $\{E_R^n, \mathbb{I}_n - E_R^n\}$, where $E_R^n = |G_R^n\rangle\langle G_R^n| + \frac{1}{2} I_{S_n}$. This result holds for any $R \in \{0,1,2,3\}$, and in particular for $R = 0 \pmod 4$ which gives us the GHZ state $|G_0^n\rangle = \frac{1}{\sqrt{2}}(|0^n\rangle + |1^n\rangle)$.

Our goal is to verify that an unknown state $|\Psi\rangle$ shared by the source, is actually the GHZ state. Any state $|\Psi\rangle$ that has trace distance from the GHZ $D(|\Psi\rangle, |G_0^n\rangle) = \epsilon$, can be expressed in the following way:

$$|\Psi\rangle = \sqrt{1-\epsilon^2}|G_0^n\rangle + \epsilon_1|G_2^n\rangle + \sqrt{\epsilon^2 - \epsilon_1^2}|\mathcal{X}\rangle,$$

where $|\mathcal{X}\rangle$ is a state in the space orthogonal to $|G_0^n\rangle$ and $|G_2^n\rangle$. We then have

$$\Pr[T(|\Psi\rangle) = 1] = \mathrm{tr}(E_0^n|\Psi\rangle\langle\Psi|) = 1 - \epsilon^2 + \frac{1}{2}(\epsilon^2 - \epsilon_1^2) \leq 1 - \frac{\epsilon^2}{2}$$

and that completes our proof.

□

The result of Theorem 7 holds also for any mixed state $\rho = \{p_i, |\Psi_i\rangle\langle\Psi_i|\}$, since from the properties of the trace, we get that $\Pr[T(\rho) = 1] = \sum_i p_i \Pr[T(|\Psi_i\rangle) = 1]$ and by convexity we have:

Corollary 8. *If* $D(\rho, |G_0^n\rangle\langle G_0^n|) = \epsilon$ *then* $\Pr[T(\rho) = 1] \leq 1 - \frac{\epsilon^2}{2}$.

4.2.4 Security in the Dishonest Model

We now look at the model where the honest Verifier runs the test in the presence of dishonest parties. Since there is no way for the Verifier to know if the dishonest parties act as $n-k$ independent parties each holding one qubit or whether they have colluded to one party, the security statement should consider that the dishonest parties can apply any operator (on their space) that works to their advantage.

Theorem 9 (Dishonest Case). *Let $|\Psi\rangle$ be the state of all n parties. If $\min_U D\big((\mathbb{I}\otimes U)|\Psi\rangle, |G_0^n\rangle\big) = \epsilon$, where U is an operator on the space of the dishonest parties, then $\Pr[T(|\Psi\rangle)=1] \leq 1-\frac{\epsilon^2}{4}$.*

Proof. We will denote the set of honest parties as $\mathcal{H}$ with cardinality $k=|\mathcal{H}|$, and we also define as $\theta = \sum_{j\in\mathcal{H}} x_j \pmod 2$ the modulo-2 sum of the honest parties' inputs from the view of the dishonest parties. We will call the bit θ the "honest input" from here forth. We can always write any shared state $|\Psi\rangle$ in the form:

$$|\Psi\rangle = |G_\theta^k\rangle|\Psi_\theta\rangle + |G_{\theta+2}^k\rangle|\Psi_{\theta+2}\rangle + |\mathcal{X}\rangle \tag{4.13}$$

where the states $|G_\theta^k\rangle$, $|G_{\theta+2}^k\rangle$ and part of $\mathcal{X}$ are the honest shares of the state and the rest belong to the dishonest coalition. We consider the component of $|\mathcal{X}\rangle$ that belongs to the honest parties' subspace, to be orthogonal to both $|G_\theta^k\rangle$ and $|G_{\theta+2}^k\rangle$.

For the dishonest parties, making the Verifier accept the Test is equivalent to guessing the honest output $Y_\mathcal{H} := \sum_{j\in\mathcal{H}} y_j \pmod 2$, before announcing their measurement outcomes. The optimal probability of guessing $Y_\mathcal{H}$ given honest input θ is equal to the probability of distinguishing between $|\Psi_\theta\rangle$ and $|\Psi_{\theta+2}\rangle$:

$$Pr[\text{guess } Y_\mathcal{H}|\theta] = \frac{1}{2} + \frac{1}{2}\Big\| |\Psi_\theta\rangle\langle\Psi_\theta| - |\Psi_{\theta+2}\rangle\langle\Psi_{\theta+2}| \Big\|_1 \tag{4.14}$$

which is actually the Helstrom measurement [95]. Our goal is therefore to find an upperbound for the above norm. From Definition 4.3, we have:

$$\begin{aligned} |G_\theta^k\rangle &= \frac{1}{\sqrt{2}}\big(|0\rangle^k + e^{i\frac{\pi}{2}\theta}|1\rangle^k\big) = \frac{1+e^{i\frac{\pi}{2}\theta}}{2}|G_0^k\rangle + \frac{1-e^{i\frac{\pi}{2}\theta}}{2}|G_2^k\rangle \\ |G_{\theta+2}^k\rangle &= \frac{1}{\sqrt{2}}\big(|0\rangle^k - e^{i\frac{\pi}{2}\theta}|1\rangle^k\big) = \frac{1-e^{i\frac{\pi}{2}\theta}}{2}|G_0^k\rangle + \frac{1+e^{i\frac{\pi}{2}\theta}}{2}|G_2^k\rangle \end{aligned}$$

By substituting the above equalities in Eq.(4.13), we have that:

$$|\Psi_0\rangle = \frac{1+e^{i\frac{\pi}{2}\theta}}{2}|\Psi_\theta\rangle + \frac{1-e^{i\frac{\pi}{2}\theta}}{2}|\Psi_{\theta+2}\rangle$$
$$|\Psi_2\rangle = \frac{1-e^{i\frac{\pi}{2}\theta}}{2}|\Psi_\theta\rangle + \frac{1+e^{i\frac{\pi}{2}\theta}}{2}|\Psi_{\theta+2}\rangle$$

which means that for honest input θ, we can express the dishonest share of state $|\Psi\rangle$ as:

$$|\Psi_\theta\rangle = \frac{1+e^{-i\frac{\pi}{2}\theta}}{2}|\Psi_0\rangle + \frac{1-e^{-i\frac{\pi}{2}\theta}}{2}|\Psi_2\rangle$$
$$|\Psi_{\theta+2}\rangle = \frac{1-e^{-i\frac{\pi}{2}\theta}}{2}|\Psi_0\rangle + \frac{1+e^{-i\frac{\pi}{2}\theta}}{2}|\Psi_2\rangle$$

The two states are not orthonormal, but we can express them using two orthonormal vectors $|w_\theta\rangle$ and $|w_\theta^\perp\rangle$:

$$\begin{aligned} |\Psi_\theta\rangle &= |||\Psi_\theta\rangle||\,|w_\theta\rangle \\ |\Psi_{\theta+2}\rangle &= |||\Psi_{\theta+2}\rangle||\,|w_{\theta+2}\rangle = |||\Psi_{\theta+2}\rangle||\left(\langle w_\theta|w_{\theta+2}\rangle|w_\theta\rangle + \langle w_\theta^\perp|w_{\theta+2}\rangle|w_\theta^\perp\rangle\right) \end{aligned}$$

We define the following: $g_\theta = |||\Psi_\theta\rangle||^2$, $f_\theta = |||\Psi_{\theta+2}\rangle||^2$, $a_\theta = \langle w_\theta|w_{\theta+2}\rangle$ and $b_\theta = \langle w_\theta^\perp|w_{\theta+2}\rangle$[1]. We also denote by A the following matrix:

$$\begin{aligned} A &= |\Psi_\theta\rangle\langle\Psi_\theta| - |\Psi_{\theta+2}\rangle\langle\Psi_{\theta+2}| \\ &= g\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} - f\begin{bmatrix} aa^* & ab^* \\ a^*b & bb^* \end{bmatrix} = \begin{bmatrix} g - f|a|^2 & -fab^* \\ -fa^*b & -f|b|^2 \end{bmatrix} \end{aligned}$$

Since our goal is to upperbound the norm of matrix A, it will be useful to observe that A is Hermitian, therefore its eigenvalues are real. We also know that the trace norm of a Hermitian matrix is equal to the sum of the absolute values of its eigenvalues, so let

[1] In the following, for ease of use we will not mention the index θ for these parameters.

us try to find the eigenvalues of martix A:

$$\begin{aligned} det(A-\lambda\mathbb{I}) &= (g-f|a|^2-\lambda)(-f|b|^2-\lambda)-f^2|a|^2|b|^2 \\ &= \lambda^2+\lambda(-g+f|a|^2+f|b|^2)-fg|b|^2 \\ &= \lambda^2+\lambda(f-g)-fg|b|^2 \end{aligned}$$

since $|a|^2+|b|^2=1$. We have:

$$\lambda_{1,2} = \frac{(f-g)\pm\sqrt{(f-g)^2+4fg|b|^2}}{2} = \frac{(f-g)\pm\sqrt{(f+g)^2-4fg|a|^2}}{2}$$

$$\lambda_1\cdot\lambda_2 = \frac{1}{4}\big[(f-g)^2-((f+g)^2-4fg|a|^2)\big] = -fg(1+|a|^2)$$

In the above product of the two eigenvalues, we can see that all its components are non-negative numbers, so it holds that $\lambda_1\cdot\lambda_2\leq 0$. Since one of the two eigenvalues is smaller or equal to the other one (w.l.o.g $\lambda_2\leq\lambda_1$), we conclude that $\lambda_2\leq 0$ and $\lambda_1\geq 0$.This means that:

$$\begin{aligned} \|A\| &= |\lambda_1|+|\lambda_2| = \lambda_1-\lambda_2 \\ &= \sqrt{(f+g)^2-4fg|a|^2} \\ &= \sqrt{(\||\Psi_\theta\rangle\|^2+\||\Psi_{\theta+\pi}\rangle\|^2)^2-4|\langle\Psi_\theta|\Psi_{\theta+\pi}\rangle|^2} \end{aligned} \tag{4.15}$$

Using Eq. 4.15, we can rewrite Eq. 4.14:

$$\Pr[\text{guess } Y_{\mathcal{H}}|\theta] = \frac{1}{2}+\frac{1}{2}\sqrt{\left(\||\Psi_\theta\rangle\|^2+\||\Psi_{\theta+2}\rangle\|^2\right)^2-4|\langle\Psi_\theta|\Psi_{\theta+2}\rangle|^2} \tag{4.16}$$

If we denote by S the term under the square root, we can use the fact that $\sqrt{S}\leq\frac{S+1}{2}$ in order to give an upperbound for Eq. 4.16:

$$\Pr[\text{guess } Y_{\mathcal{H}}|\theta] \leq \frac{1}{2} + \frac{1}{2}\Big(\frac{\big(|||\Psi_\theta\rangle||^2 + |||\Psi_{\theta+2}\rangle||^2\big)^2 - 4|\langle\Psi_\theta|\Psi_{\theta+2}\rangle|^2 + 1}{2}\Big)$$
$$= 1 - \frac{1}{4}\big(1 - \big(|||\Psi_\theta\rangle||^2 + |||\Psi_{\theta+2}\rangle||^2\big)^2 + 4|\langle\Psi_\theta|\Psi_{\theta+2}\rangle|^2\big) \tag{4.17}$$

In order to upperbound the above expression, since θ can only take the values 0 and 1, we write the two expressions:

$$\Pr[\text{guess } Y_{\mathcal{H}}|\theta = 0] \leq 1 - \frac{1}{4}\big(1 - \big(|||\Psi_0\rangle||^2 + |||\Psi_2\rangle||^2\big)^2 + 4|\langle\Psi_0|\Psi_2\rangle|^2\big)$$
$$\Pr[\text{guess } Y_{\mathcal{H}}|\theta = 1] \leq 1 - \frac{1}{4}\big(1 - \big(|||\Psi_1\rangle||^2 + |||\Psi_3\rangle||^2\big)^2 + 4|\langle\Psi_1|\Psi_3\rangle|^2\big)$$

Let us define $p = |||\Psi_0\rangle||^2$ and $q = |||\Psi_2\rangle||^2$. Let also ϕ be the angle between $|\Psi_0\rangle$ and $|\Psi_2\rangle$ such that $\langle\Psi_0|\Psi_2\rangle^2 = pq\cos^2\phi$. We have $\langle\Psi_1|\Psi_3\rangle^2 = 1/4\big(\big\||\Psi_0\rangle\big\|^2 - \big\||\Psi_2\rangle\big\|^2\big)^2 = (p-q)^2/4$. We also know that $|||\Psi_1\rangle||^2 + |||\Psi_3\rangle||^2 = |||\Psi_0\rangle||^2 + |||\Psi_2\rangle||^2 = p + q \leq 1$. Since the value of bit θ is chosen uniformly at random, we have:

$$\Pr[T(|\Psi\rangle) = 1] = \frac{1}{2}\Big(\Pr[\text{guess } Y_{\mathcal{H}}|\theta = 0] + \Pr[\text{guess } Y_{\mathcal{H}}|\theta = 1]\Big)$$
$$\leq 1 - \frac{1}{8}\Big(2 - 2(p+q)^2 + 4pqcos^2\phi + (p-q)^2\Big)$$
$$= 1 - \frac{1}{4}\Big(1 - \frac{(p+q)^2 + 4pqsin^2\phi}{2}\Big) \tag{4.18}$$

We will now relate the above expression to the distance between the state $|\Psi\rangle$ and the GHZ. In order to calculate the distance, we need to consider that the dishonest parties may perform a local operation on their share of the state. Let us examine how such an operation affects their cheating probability with a simple example: Suppose that among the n parties, only party A_n is malicious and collaborates with the source. Even though the state $|\Psi\rangle = 1/\sqrt{2}(|0^{n-1}\rangle|1\rangle + |1^{n-1}\rangle|0\rangle)$ is away from the GHZ, it always passes the Verifier's test, since the last party can do a local operation on his/her bit to turn $|\Psi\rangle$ into the GHZ state.

We therefore need to allow the dishonest parties to minimize the distance of state $|\Psi\rangle$ from the GHZ by performing a local operation U on their share. We define this minimum

distance:

$$\epsilon = min_U D((\mathbb{I}\otimes U)|\Psi\rangle, |G_0^n\rangle) = min_U \sqrt{1-F^2((\mathbb{I}\otimes U)|\Psi\rangle, |G_0^n\rangle)}$$

where by $F(|\psi\rangle, |\phi\rangle)$ we denote the fidelity between two states $|\psi\rangle$ and $|\phi\rangle$. Let us define the reduced density matrices of the honest parties of $|G_n^0\rangle$ and $|\Psi\rangle$ as $\sigma_{\mathcal{H}}$ and $\rho_{\mathcal{H}}$ respectively. These can be computed by tracing out the set of dishonest parties D. It holds that there exists a local operation R on the dishonest state such that:

$$F((\mathbb{I}\otimes R)|\Psi\rangle, |G_0^n\rangle) = F(\sigma_{\mathcal{H}}, \rho_{\mathcal{H}})$$

By applying this operation R, the distance is minimized:

$$\epsilon^2 = 1-F^2((\mathbb{I}\otimes R)|\Psi\rangle, |G_0^n\rangle) = 1-F^2(\sigma_{\mathcal{H}}, \rho_{\mathcal{H}})$$

Since from Eq. 4.4 we can always express the GHZ state as $|G_0^n\rangle = \frac{1}{\sqrt{2}}(|G_0^k\rangle|G_0^{n-k}\rangle + |G_2^k\rangle|G_2^{n-k}\rangle)$, where k is the number of the honest parties, we have:

$$\sigma_{\mathcal{H}} = tr_D(G_0^n) = \frac{1}{2}\big(|G_0^k\rangle\langle G_0^k| + |G_2^k\rangle\langle G_2^k|\big)$$

From Eq. 4.13, we have that $|\Psi\rangle = |G_0^k\rangle|\Psi_0\rangle + |G_2^k\rangle|\Psi_2\rangle + |\mathcal{X}\rangle$, therefore:

$$\begin{aligned}\rho_{\mathcal{H}} &= tr_D(|\Psi\rangle\langle\Psi|)\\ &= p|G_0^k\rangle\langle G_0^k| + q|G_2^k\rangle\langle G_2^k| + \sqrt{pq}\cos\phi\big(|G_0^k\rangle\langle G_2^k| + |G_2^k\rangle\langle G_0^k|\big) + \mathrm{tr}_D|\mathcal{X}\rangle\end{aligned}$$

where we remind that $p = \||\Psi_0\rangle\|^2$, $q = \||\Psi_2\rangle\|^2$ and $\langle\Psi_0|\Psi_2\rangle^2 = pq\cos^2\phi$, where ϕ is the angle between $|\Psi_0\rangle$ and $|\Psi_2\rangle$. We can then find the fidelity of the two reduced density matrices:

$$F(\sigma_{\mathcal{H}},\rho_{\mathcal{H}}) = \mathrm{tr}(\sqrt{\sigma_H^{1/2}\rho_{\mathcal{H}}\sigma_{\mathcal{H}}^{1/2}})$$
$$= \mathrm{tr}\Big(\sqrt{\frac{1}{2}\begin{bmatrix} p & \sqrt{pq}\cos\phi & 0 & \dots & 0 \\ \sqrt{pq}\cos\phi & q & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \dots & \vdots \end{bmatrix}}\Big)$$

Then, we diagonalize the matrix keeping only the upper left non-zero part for simplicity. The determinant of the characteristic function is:

$$det\begin{bmatrix} t-p & \sqrt{pq}\cos\phi \\ \sqrt{pq}\cos\phi & t-q \end{bmatrix} = (t-p)(t-q) - pq\cos^2\phi = t^2 - t(p+q) + pq\sin^2\phi$$

Hence, the two eigenvalues of the matrix are:

$$t_{1,2} = \frac{p+q \pm \sqrt{(p+q)^2 - 4pqsin^2\phi}}{2}$$

We then have:

$$\begin{aligned} F^2(\sigma_H,\rho_H) &= \frac{1}{4}\Big(\sqrt{p+q+\sqrt{(p+q)^2-4pqsin^2\phi}} + \sqrt{p+q-\sqrt{(p+q)^2-4pqsin^2\phi}}\Big)^2 \\ &= \frac{1}{4}\Big(2p+2q+2\sqrt{\big(p+q+\sqrt{(p+q)^2-4pqsin^2\phi}\big)\big(p+q-\sqrt{(p+q)^2-4pqsin^2\phi}\big)}\Big) \\ &= \frac{1}{2}\big(p+q+\sqrt{(p+q)^2-(p+q)^2+4pqsin^2\phi}\big) \\ &= \frac{1}{2}\big(p+q+2\sqrt{pq}sin\phi\big), \end{aligned}$$

which gives

$$\epsilon^2 = 1 - \frac{p+q}{2} - \sqrt{pq}\sin\phi$$

Recall that from Eq. 4.18 we have:

$$\Pr[T(|\Psi\rangle) = 1] \leq 1 - \frac{1}{4}\Big(1 - \frac{(p+q)^2 + 4pqsin^2\phi}{2}\Big)$$

We use the fact that $(p+q)^2 \leq (p+q)$ since $p+q \leq 1$. Similarly, we use $4pq\sin^2\phi \leq 2\sqrt{pq}\sin\phi$ since $2\sqrt{pq}\sin\phi \leq 1$. From this, we conclude that:

$$\begin{aligned}\Pr[T(|\Psi\rangle) = 1] &\leq 1 - \frac{1}{4}\Big(1 - \frac{(p+q)^2 + 4pqsin^2\phi}{2}\Big) \\ &\leq 1 - \frac{1}{4}\Big(1 - \frac{p+q}{2} - \sqrt{pq}sin\phi\Big) = 1 - \frac{\epsilon^2}{4}\end{aligned}$$

and this concludes the proof of Theorem 9. □

4.3 Entanglement Verification with imperfections

In the presence of system imperfections, the Basic Verification Protocol described in paragraph 4.2.1 will occassionally output loss or fail, even when testing the ideal GHZ state in the all-honest model. This can be due to a party losing their qubit or when an error alters the outcome of the measurement for an odd number of parties. We therefore need to allow the Verifier to repeat the protocol many times in order to decide if he accepts or rejects the state, taking into account the losses and errors that appear. In order to decide the exact number of rounds, the Verifier uses S random coins. When at least one of the coins takes the value 1, he tests the state and writes the result of the test (pass, fail or loss) in his memory. When all of the coins are zero, he reads his memory in order to check consistency with system characterisation (i.e. losses and noise are not more than what they should be), and he decides if the state should be accepted or rejected. A general flow of the protocol is presented in Figure 4.1.

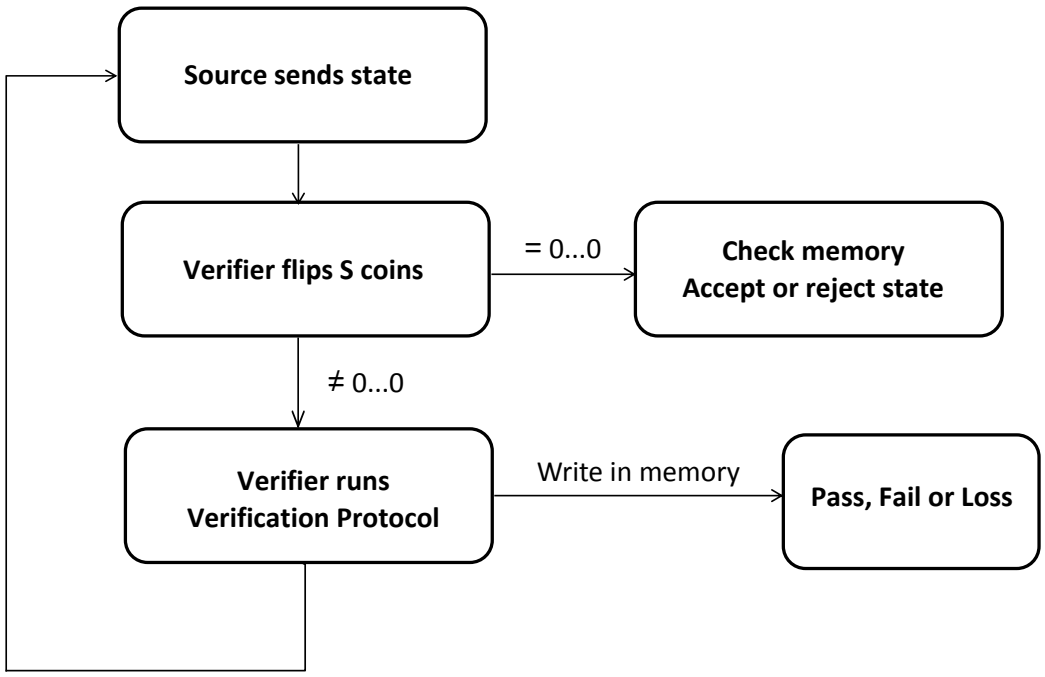


Figure 4.1: Complete Verification Scheme

Graphical Representation. In order to see how the imperfections of the system could help a dishonest adversary increase their probability of passing the test with a state that is "away" from a GHZ state, we will introduce a graphical representation of the probability of passing the test for a specific state, with respect to a given dishonest angle. Let us consider

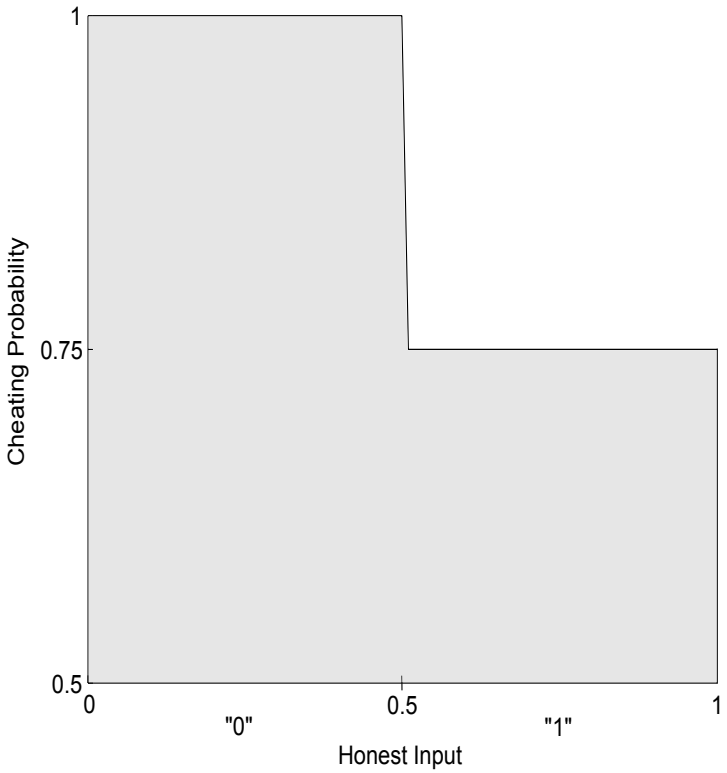


Figure 4.2: Basic Verification Protocol - Cheating probability with no losses

the example of a 3-party case, where the source sends the state $|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)|0\rangle$ to the parties, and the last party is dishonest. Note that for the specific state that we are examining, the dishonest party does not share any entanglement with the honest parties. In Figure 4.2, we have plotted the cheating probability $\Pr[T(|\Psi\rangle) = 1]$, given the choice of "honest input" (mod 2), which with probability 1/2 is 0 and with probability 1/2 is 1[2]. The two different values for the cheating probability are calculated from Eq. 4.17. For the graphical representation, we assume that the "honest input" is chosen uniformly at random in the following way: pick a number from 0 to 1 (shown in the horizontal axis of the figure), and if it is smaller than 0.5 set the input/angle to 0, while if it is bigger or equal to 0.5, set it to 1. Hence, the grey surface shown in Figure 4.2 upperbounds the bias of the protocol, and is equal to 3/8. Finally the probability that the state $|\Psi\rangle$ passes test T is given by Eq. 4.18:

$$\Pr[T(|\Psi\rangle) = 1] \leq \frac{7}{8} \tag{4.19}$$

and is exactly the result of Theorem 9 for $\epsilon = 1/\sqrt{2}$.

Now think about the case where the parties' equipment has detection efficiency 75%.

[2]The dishonest parties always know the honest angle (mod 2), from the constraint on the sum of the inputs.

If the Verifier is willing to accept each party declaring loss for $\lambda = 25\%$ of the inputs, then it is not hard to see that the strategy of a dishonest party is graphically represented in Figure 4.3; whenever the Verifier asks the dishonest party to measure in the Y basis (which means that the "honest input" is $\theta = 1$), he/she declares "loss" half of the time (thus throwing away 25% of the "bad" inputs), and tries to pass the test in the remaining rounds. For the rounds that no "loss" was declared, the probability that state $|\Psi\rangle$ passes the test T becomes:

$$\begin{aligned}\Pr[T(|\Psi\rangle) = 1|\lambda = 25\%] &= \frac{2}{3}\Pr[\text{guess } Y_H|\theta = 0] + \frac{1}{3}\Pr[\text{guess } Y_H|\theta = 1] \\ &= \frac{2}{3}\cdot 1 + \frac{1}{3}\cdot 0,75 = \frac{11}{12} \\ &\geq \Pr[T(|\Psi\rangle) = 1|\lambda = 0\%] = \frac{7}{8}\end{aligned}$$

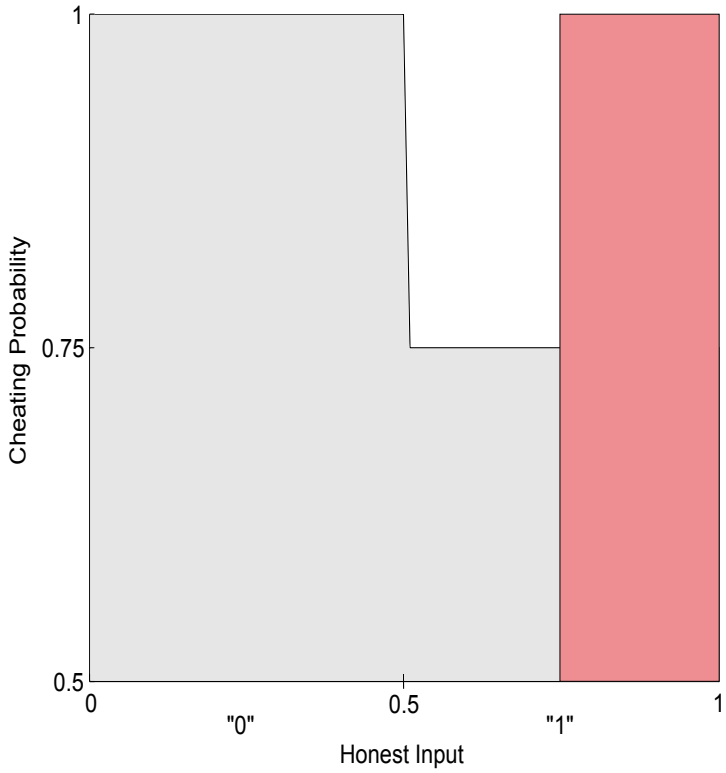


Figure 4.3: Basic Verification Protocol - Cheating probability with 25% losses

There is an important increase in the cheating probability, but a "bad" state can still be rejected if we can increase the number of protocol rounds accordingly. By repeating the protocol may times, the test will fail at some of the rounds, and the Verifier will not be convinced that the state is the GHZ. But what is happening when the losses are more than 50%? It is not difficult to see that the cheating probability, or equivalently the

probability of passing the test with the specific "bad" state $|\Psi\rangle$ is equal to 1. So how can we deal with low detection efficiencies? The answer lies in the number of measurement bases; we need to expand the set of measurement bases from which the Verifier chooses the parties' inputs, in order to increase our tolerance to losses.

4.3.1 Enhanced Verification Protocol

In this section we present a loss-tolerant protocol for entanglement verification, where again a source is sharing a state $|\Psi\rangle$ with n parties and wants to convince the Verifier that the state is actually an n-party GHZ state (up to local operations on the dishonest parties).

Enhanced Verification Protocol

1. The Verifier selects $\theta_j \in [0, \pi)$ for every party A_j, $j = 1, \ldots, n$, such that

$$\sum_j \theta_j = 0 \pmod{\pi} \tag{4.20}$$

   and sends them sequentially, waiting for each party's measurement outcome before sending the next input (we later argue that this is done to minimize the information on the honest input that the dishonest parties learn).

2. Each party A_j measures in the basis:

$$\{|\theta_j^+\rangle, |\theta_j^-\rangle\} = \{\frac{|0\rangle + e^{i\theta_j}|1\rangle}{\sqrt{2}}, \frac{|0\rangle - e^{i\theta_j}|1\rangle}{\sqrt{2}}\}$$

   and sends the bit y_j to the Verifier, where $y_j = 0$ when the measurement outcome is the basis vector $|\theta_j^+\rangle$ and $y_j = 1$ when the measurement outcome is the basis vector $|\theta_j^-\rangle$.

3. If all parties have sent their outputs and have not declared loss, the Verifier accepts the state $|\Psi\rangle$ if the test T' succeeds:

$$T'(|\Psi\rangle): \quad \bigoplus_j y_j = \frac{1}{\pi}\sum_j \theta_j \pmod{2} \tag{4.21}$$

In the same way as before, we denote by $T'(|\Psi\rangle)$ the outcome of the above test on state

$|\Psi\rangle$ (it is equal to 1 if the state passes the test and 0 if it fails).

4.3.2 Correctness of the Enhanced Protocol

We want to show that the GHZ state passes the test 4.21 with probability 1. The measurements that the parties are performing are equivalent to rotation operators around the $\hat{z}$ axis:

$$R_z(\theta_j) = \begin{bmatrix} 1 & 0 \\ 0 & e^{-i\theta_j} \end{bmatrix}$$

followed by a measurement in the Hadamard basis (or equivalent a Hadamard transformation and a measurement in the computational basis). Similar to Section 4.2.2, from the promise $\sum_j \theta_j = 0 \pmod{\pi}$, we have two cases:

- $\sum_{j=1}^{n} \theta_j \equiv 0 \pmod{2\pi}$. After the parties' rotations $R_z(\theta_j)$, the state is the GHZ state $|G_0^n\rangle$, and after the Hadamard transformations, it is the equal superposition of all bistrings with an even number of 1's, so the exclusive or of their measurement outputs, is equal to 0.
- $\sum_{j=1}^{n} \theta_j \equiv \pi \pmod{2\pi}$. After the parties' rotations $R_z(\theta_j)$, the state is the $|G_\pi^n\rangle = \frac{1}{\sqrt{2}}(|0^n\rangle - |1^n\rangle)$, and after the Hadamard transformations, it is the equal superposition of all bistrings with an odd number of 1's, so the exclusive or of their measurement outputs, is equal to 1.

It is therefore true that the test 4.21 succeeds with probability 1 on the GHZ state. It is easy to see the connection between this protocol and the one in paragraph 4.2.1, where instead of performing the stabiliser set of X and Y measurements on the $|G_0^n\rangle$ state, we perform random rotations around the $\hat{z}$-axis.

4.3.3 Security in the Honest Model

The security proof in this section is a simple extension of the proof in Section 4.2.3. Here we will provide a sketch of the proof and refer the reader to Appendix A for the complete proof.

We suppose that all n parties are honest and we want to find out what is the probability that our Test T' accepts a state $|\Psi\rangle$ as a function of the distance of this state from $|G_0^n\rangle$. Denoting by $D(|\psi\rangle, |\phi\rangle)$ the trace distance between two states $|\psi\rangle$ and $|\phi\rangle$, we can prove Theorem 7 for the Enhanced Verification Protocol:

Theorem 10 (Honest Case)**.** *Let $|\Psi\rangle$ be the state of all n parties. If $D(|\Psi\rangle, |G_0^n\rangle) = \epsilon$, then* $\Pr[T'(|\Psi\rangle) = 1] \leq 1 - \frac{\epsilon^2}{2}$.

Proof. (For a complete proof see Appendix A) We will need to define a verification test for a rotated GHZ state:

State: $|G_\Theta^n\rangle = \frac{1}{\sqrt{2}}\left(|0^n\rangle + e^{i\Theta}|1^n\rangle\right)$, where $\Theta \in [0, 2\pi)$

Promise on inputs: $\sum_{j=1}^n \theta_j \equiv \Theta \pmod{\pi}$

Test: $\bigoplus_{j=1}^n y_j = \frac{\sum_{j=1}^n \theta_j - \Theta}{\pi} \pmod 2$

From the promise on the inputs, we can distinguish two cases: either $\sum_{j=1}^n \theta_j - \Theta \equiv 0 \pmod{2\pi}$ or $\sum_{j=1}^n \theta_j - \Theta \equiv \pi \pmod{2\pi}$. After the parties' operations and before the measurement in the computational basis, in the first case, the state is the equal superposition of all bistrings with an even number of 1's, while in the second case, it is the equal superposition of all bistrings with an odd number of 1's. Therefore the test always succeeds on $|G_\Theta^n\rangle$, for inputs consistent with the promise.

Let us now consider the most general measurement for the parties on a state $|\Psi\rangle$. This is a POVM $\{P_\Theta^n, \mathbb{I}_n - P_\Theta^n\}$, where the first element denotes success of the test and the second failure. We will prove by induction that:

$$P_\Theta^n = |G_\Theta^n\rangle\langle G_\Theta^n| + \frac{1}{2} I_\Theta^n$$

where I_Θ^n is the projection on the space orthogonal to $|G_\Theta^n\rangle$ and $|G_{\Theta+\pi}^n\rangle$.

Induction. For n=1 we have that $P_\Theta^1 = |G_{\theta_1}^1\rangle\langle G_{\theta_1}^1|$ so the statement holds. We assume it is true for n parties and we will show the statement for $n+1$.

Let $\{P_\Theta^{n+1}(\theta_1), \mathbb{I}_{n+1} - P_\Theta^{n+1}(\theta_1)\}$ be the POVM that corresponds to the test for a given angle θ_1 of party A_1. We can differentiate between two cases according to the output of party A_1:

1. Party A_1 outputs $y_1 = 0$. Then the remaining n parties need to pass the test:

$$\bigoplus_{j=2}^{n+1} y_j = \frac{\sum_{j=2}^{n+1} \theta_j - (\Theta - \theta_1)}{\pi} \pmod 2$$

2. Party A_1 outputs $y_1 = 1$. Then the remaining n parties need to pass the test:

$$\bigoplus_{j=2}^{n+1} y_j = \frac{\sum_{j=2}^{n+1} \theta_j - (\Theta - \theta_1 + \pi)}{\pi} \pmod 2$$

Let $\Theta_{\neg 1} \equiv \Theta - \theta_1 \pmod{2\pi}$. It is evident that the first test is equivalent to the positive element $P^n_{\Theta_{\neg_1}}$ of a POVM on state $|G^n_{\Theta_{\neg_1}}\rangle$ and the second to the positive element $P^n_{\Theta_{\neg_1}+\pi}$ of a POVM on state $|G^n_{\Theta_{\neg_1}+\pi}\rangle$. From the induction we know that:

$$\begin{aligned} P^n_{\Theta_{\neg_1}+\pi} &= |G^n_{\Theta_{\neg_1}+\pi}\rangle\langle G^n_{\Theta_{\neg_1}+\pi}| + \frac{1}{2} I^n_\Theta \\ &= |G^n_{\Theta_{\neg_1}+\pi}\rangle\langle G^n_{\Theta_{\neg_1}+\pi}| + |G^n_{\Theta_{\neg_1}}\rangle\langle G^n_{\Theta_{\neg_1}}| + I^n_\Theta - |G^n_{\Theta_{\neg_1}}\rangle\langle G^n_{\Theta_{\neg_1}}| - \frac{1}{2} I^n_\Theta \\ &= \mathbb{I}_n - P^n_{\Theta_{\neg_1}} \end{aligned} \tag{4.22}$$

For the test on $(n+1)$-parties to succeed, we therefore have, for a given θ_1:

$$\begin{aligned} P^{n+1}_\Theta(\theta_1) &= |G^1_{\theta_1}\rangle\langle G^1_{\theta_1}| \otimes P^n_{\Theta_{\neg_1}} + |G^1_{\theta_1+\pi}\rangle\langle G^1_{\theta_1+\pi}| \otimes (\mathbb{I}_n - P^n_{\Theta_{\neg_1}}) \\ &= |G^1_{\theta_1}\rangle\langle G^1_{\theta_1}| \otimes |G^n_{\Theta_{\neg_1}}\rangle\langle G^n_{\Theta_{\neg_1}}| + |G^1_{\theta_1+\pi}\rangle\langle G^1_{\theta_1+\pi}| \otimes |G^n_{\Theta_{\neg_1}+\pi}\rangle\langle G^n_{\Theta_{\neg_1}+\pi}| \\ &+ \frac{1}{2}\Big(|G^1_{\theta_1}\rangle\langle G^1_{\theta_1}| + |G^1_{\theta_1+\pi}\rangle\langle G^1_{\theta_1+\pi}|\Big) \otimes I^n_\Theta \\ &= |G^{n+1}_\Theta\rangle\langle G^{n+1}_\Theta| + |\Phi^{n+1}_{\theta_1,\Theta}\rangle\langle \Phi^{n+1}_{\theta_1,\Theta}| + \frac{1}{2}\mathbb{I}_1 \otimes I^n_\Theta \end{aligned} \tag{4.23}$$

where for a given $\Theta \in [0, 2\pi)$ and $\theta_1 \in [0, \pi)$ we define:

$$|\Phi^{n+1}_{\theta_1,\Theta}\rangle = \frac{1}{\sqrt{2}}\big(|G^1_{\theta_1}\rangle|G^n_{\Theta_{\neg_1}}\rangle - |G^1_{\theta_1+\pi}\rangle|G^n_{\Theta_{\neg_1}+\pi}\rangle\big)$$

Since angle θ_1 is chosen uniformely at random in $[0, \pi)$, we have that:

$$
\begin{aligned}
P_\Theta^{n+1} &= \frac{1}{\pi}\int_0^{\pi} P_\Theta^{n+1}(\theta_1)d\theta_1 = \frac{1}{\pi}\int_0^{\pi/2}\Big[P_\Theta^{n+1}(\theta_1)+P_\Theta^{n+1}(\theta_1+\frac{\pi}{2})\Big]d\theta_1 \\
&= \frac{1}{\pi}\int_0^{\pi/2}\Big[2\times|G_\Theta^{n+1}\rangle\langle G_\Theta^{n+1}| + |\Phi_{\theta_1,\Theta}^{n+1}\rangle\langle\Phi_{\theta_1,\Theta}^{n+1}| + |\Phi_{\theta_1+\frac{\pi}{2},\Theta}^{n+1}\rangle\langle\Phi_{\theta_1+\frac{\pi}{2},\Theta}^{n+1}| + \mathbb{I}_1\otimes I_\Theta^n\Big]d\theta_1 \\
&= |G_\Theta^{n+1}\rangle\langle G_\Theta^{n+1}| + \frac{1}{2}I_\Theta^{n+1} \qquad (4.24)
\end{aligned}
$$

since it holds that (see Appendix A):

$$
I_\Theta^{n+1} = |\Phi_{\theta_1,\Theta}^{n+1}\rangle\langle\Phi_{\theta_1,\Theta}^{n+1}| + |\Phi_{\theta_1+\frac{\pi}{2},\Theta}^{n+1}\rangle\langle\Phi_{\theta_1+\frac{\pi}{2},\Theta}^{n+1}| + \mathbb{I}_1\otimes I_\Theta^n
$$

and as before I_Θ^{n+1} is the projection on the space that is orthogonal to $|G_\Theta^{n+1}\rangle$ and $|G_{\Theta+\pi}^{n+1}\rangle$.

Eq. 4.24 holds for any angle $\Theta\in[0,2\pi)$, and in particular for $\Theta = 0 \pmod{2\pi}$, so our argument that the verification test T' for the GHZ state $|G_0^n\rangle$ is equivalent to performing the POVM $\{P_0^n, \mathbb{I}_n - P_0^n\}$ is true.

Our goal is to test an unknown state $|\Psi\rangle$ shared by the source among n parties. If the state has trace distance from the GHZ $\epsilon = D(|\Psi\rangle, |G_0^n\rangle)$, we can express it as follows:

$$
|\Psi\rangle = \sqrt{1-\epsilon^2}|G_0^n\rangle + \epsilon_1|G_\pi^n\rangle + \sqrt{\epsilon^2-\epsilon_1^2}|\mathcal{X}\rangle,
$$

where $|\mathcal{X}\rangle$ is a vector orthogonal to both $|G_0^n\rangle$ and $|G_\pi^n\rangle$. We then have

$$
\Pr[T'(|\Psi\rangle)=1] = \mathrm{tr}(P_0^n|\Psi\rangle\langle\Psi|) \le 1-\frac{\epsilon^2}{2}
$$

□

4.3.4 Security in the Dishonest Model

We now investigate the case of dishonest parties, where an honest Verifier wants to run the enahnced test in order to verify a state $|\Psi\rangle$. We will prove Theorem 9 for the enhanced protocol. As before, the Verifier does not know if the dishonest parties act as $n-k$ independent parties each holding one qubit or whether they have colluded to one party, so the security statement considers that the dishonest parties can apply any operator (on their space) that works to their advantage.

Theorem 11 (Dishonest Case)**.** *Let $|\Psi\rangle$ be the state of all n parties. If $\min_U D\big((\mathbb{I}\otimes$*

$U)|\Psi\rangle, |G_0^n\rangle\big) = \epsilon$, *where* U *is an operator on the space of the dishonest parties, then* $\Pr[T'(|\Psi\rangle) = 1] \leq 1 - \frac{\epsilon^2}{4}$.

Proof. (For a complete proof see Appendix A) We can express the state that is shared by the source as:

$$|\Psi\rangle = |G_h^k\rangle|\Psi_h\rangle + |G_{h+\pi}^k\rangle|\Psi_{h+\pi}\rangle + |\mathcal{X}\rangle \tag{4.25}$$

where $|G_a^k\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle^k + e^{ia}|1\rangle^k\big)$, $\mathcal{H}$: the set of honest parties, $k = |\mathcal{H}|$: the number of honest parties and $h = \sum_{j\in\mathcal{H}} \theta_j \pmod{\pi}$: the input of all parties in $\mathcal{H}$, known to the dishonest set. States $|\Psi_h\rangle$ and $|\Psi_{h+\pi}\rangle$ are unormalised and $|\mathcal{X}\rangle$ is an arbitrary state whose "honest" part is orthogonal to $|G_h^k\rangle$ and $|G_{h+\pi}^k\rangle$.

The dishonest parties want to know in which of the two states $|G_h^k\rangle$ and $|G_{h+\pi}^k\rangle$ the honest share will collapse in after the measurement, and by consequence what will be the honest output $Y_{\mathcal{H}} = \sum_{j\in\mathcal{H}} y_j \pmod 2$. They will perform a Helstrom measurement on their share in order to distinguish between $|\Psi_h\rangle$ and $|\Psi_{h+\pi}\rangle$. This measurement is optimal and gives the following bound:

$$\Pr[\text{guess } Y_{\mathcal{H}}|h] = \frac{1}{2} + \frac{1}{2}\Big\| |\Psi_h\rangle\langle\Psi_h| - |\Psi_{h+\pi}\rangle\langle\Psi_{h+\pi}| \Big\|_1$$

To compute the above norm, we make use of a known property, that the trace norm of a Hermitian matrix is equal to the sum of the absolute values of its eigenvalues. After some simple calculations (see Appendix A), we can verify that the above probability is equal to:

$$\Pr[\text{guess } Y_{\mathcal{H}}|h] \leq 1 - \frac{1}{4}\Big(1 - \big(\,|||\Psi_h\rangle||^2 + |||\Psi_{h+\pi}\rangle||^2\,\big)^2 + 4|\langle\Psi_h|\Psi_{h+\pi}\rangle|^2\Big) \tag{4.26}$$

By doing a Schmidt decomposition of $|G_h^k\rangle|\Psi_h\rangle + |G_{h+\pi}^k\rangle|\Psi_{h+\pi}\rangle$, we can express the inner product $|\langle\Psi_h|\Psi_{h+\pi}\rangle|$ as a function of the norms of the states of the decomposition p_h and q_h, where $p_h + q_h = |||\Psi_h\rangle||^2 + |||\Psi_{h+\pi}\rangle||^2$[3] and a parameter α, which can be thought of as a characteristic of the state $|\Psi\rangle$ (for more details see Appendix A). We can therefore

[3]Here the p_h and q_h depend on h, but for ease of use in the following we do not use an index for a fixed h.

rewrite Eq. 4.26:

$$\Pr[\text{guess } Y_{\mathcal{H}}|h] \leq 1 - \frac{1}{4}\Big(1-(p+q)^2 + (p-q)^2 sin^2(h+\alpha)\Big) \tag{4.27}$$

In general, we consider that the dishonest parties can perform any local operation U on their state, to maximize their cheating probability. Thus, it is better to express the distance of $|\Psi\rangle$ from the GHZ as:

$$\epsilon = min_U D(((\mathbb{I}\otimes U)|\Psi\rangle, |G_0^n\rangle) = min_U \sqrt{1-F^2(((\mathbb{I}\otimes U)|\Psi\rangle, |G_0^n\rangle)}$$

where by $F(|\psi\rangle, |\phi\rangle)$ we denote the fidelity between two states $|\psi\rangle$ and $|\phi\rangle$. As before, if the reduced density matrices of the honest parties of the perfect and the real state are $\sigma_{\mathcal{H}}$ and $\rho_{\mathcal{H}}$ respectively, it holds that there exists a local operation R on the dishonest state such that:

$$F(((\mathbb{I}\otimes R)|\Psi\rangle, |G_0^n\rangle) = F(\sigma_{\mathcal{H}}, \rho_{\mathcal{H}})$$

By applying this operation R, we get:

$$\epsilon^2 \quad = \quad 1 - \frac{p+q}{2} - \sqrt{pq} \leq 1-(p+q)^2 + \frac{(p-q)^2}{2}$$

and since h is chosen uniformely at random and $p+q$ is constant for every h, we have that:

$$\begin{aligned}\Pr[\text{guess } Y_{\mathcal{H}}] &= \frac{1}{\pi}\int_0^{\pi} \Pr[\text{guess } Y_{\mathcal{H}}|h]dh \\ &\leq 1 - \frac{1}{4}\Big(1-(p+q)^2 + \epsilon^2 - 1 + (p+q)^2\Big) \\ &\leq 1 - \frac{\epsilon^2}{4}\end{aligned}$$

and this concludes our proof.

□

4.3.5 Losses

The dishonest parties can exploit the presence of losses by declaring they lost their qubits whenever the corresponding honest angle leads to a low cheating probability in Eq. 4.14.

Since the angles are chosen uniformely at random by the Verifier, and the dishonest parties do not know the number of protocol rounds to be executed, the optimal cheating strategy is to always reject the worst λ% of inputs, where λ is the amount of losses that each party is allowed to declare. [4]. In Eq. 4.27, we have proven that:

$$\Pr[\text{guess } Y_{\mathcal{H}}|h] \leq 1-\frac{1}{4}\big(1-(p+q)^2+(p-q)^2 sin^2(h+\alpha)\big)$$

which means that the highest probability of passing the test is when $h=-\alpha$ and since the probability in Eq. 4.27 follows the sine wave function with period π, it takes is minimum value at $-\alpha-\pi/2$ and $-\alpha+\pi/2$. This means that the best inputs for the cheating parties, are in the interval $(-\alpha-(1-\lambda)\pi/2, -\alpha+(1-\lambda)\pi/2)$. Then, the probability that the state will pass the test, on the inputs for which the dishonest parties did not declare loss, is:

$$\begin{aligned}
\Pr[T'(|\Psi\rangle)=1|\lambda] &= \frac{1}{(1-\lambda)\pi}\int_{-\alpha-\frac{1-\lambda}{2}\pi}^{-\alpha+\frac{1-\lambda}{2}\pi} \Pr[\text{guess } Y_{\mathcal{H}}|h]dh \\
&= 1-\frac{1}{4}\Big[1-(p+q)^2+\frac{(p-q)^2}{(1-\lambda)\pi}\int_{-\frac{1-\lambda}{2}\pi}^{\frac{1-\lambda}{2}\pi} sin^2 h dh\Big] \\
&= 1-\frac{1}{4}\Big[1-(p+q)^2+\frac{(p-q)^2}{2}-\frac{(p-q)^2}{2}\frac{sin((1-\lambda)\pi)}{(1-\lambda)\pi}\Big] \\
&= 1-\frac{1}{4}\Big[\epsilon^2-\frac{(p-q)^2}{2}\frac{sin((1-\lambda)\pi)}{(1-\lambda)\pi}\Big] \qquad (4.28)
\end{aligned}$$

We can bound the expression $\frac{(p-q)^2}{2}$ in two ways. When $\epsilon^2 \geq 1/2$, we can use the bound:

$$\frac{(p-q)^2}{2} \leq 1-4pq-\epsilon^2 \leq 1-\epsilon^2$$

that can be easily proven to be true by previous relations. When $\epsilon^2 \leq 1/2$, a better bound for $(p-q)^2$ is 1. In any experimental demonstration, it is normal to consider states that are at most 1/2-away from the GHZ, therefore we will use the latter bound in order to upperbound Eq. 4.28:

$$\Pr[T'(|\Psi\rangle)=1|\lambda] \leq 1-\frac{1}{4}\Big[\epsilon^2-\frac{sin((1-\lambda)\pi)}{2(1-\lambda)\pi}\Big] = 1-\frac{\epsilon^2}{4}+f(\lambda) \qquad (4.29)$$

[4]The dishonest coalition has no knowledge of the honest angle until the last dishonest party gets his measurement input, therefore, without loss of generality, we will consider that only the last dishonest party declares loss in a malicious way. We can make this assumption because the losses for the rest of the parties are uniform on the inputs, thus they don't contribute to the cheating probability and the overall amount of losses is checked by the Verifier at the end.

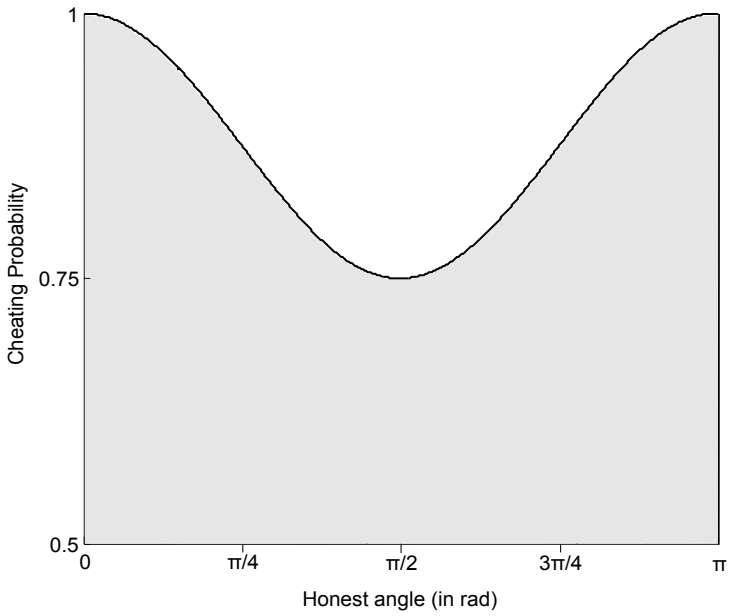


Figure 4.4: Enhanced Protocol - Cheating Probability with no losses

where $f(\lambda) = \sin(\pi - \lambda\pi)/8(\pi - \lambda\pi)$.

To be able to compare with the Basic Verification Protocol, we express graphically the cheating probability of state $|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)|0\rangle$, using the Enhanced Verification Protocol: Figure 4.4 shows how the Cheating Probability depends on the honest angle when there are no losses, while Figure 4.5 demonstrates what is happening when there is a chance of 25% for a particle to get lost.

As mentioned before, at the end of each round, the Verifier writes to his memory, either "pass", "loss" or "fail". Since a dishonest state needs to be tested in order to fail the test, we are interested in computing the probability that there was no "fail" written in the memory, given a state that is ϵ-away from the GHZ and an amount of losses λ. We have:

$$Q_\epsilon^\lambda = \lambda + (1-\lambda)\cdot(1-\epsilon^2/4 + f(\lambda)) \tag{4.30}$$

When the shared state is the GHZ, the memory of the Verifier will never contain any "fail", which means that the above probability will be 1. On the other hand, if the shared state is not the GHZ, given enough iterations, an ϵ-away state will fail some of the tests, therefore the above probability will be equal to 1, only when the losses are 100%. For losses less than 100%, and given enough rounds, the probability Q_ϵ^λ will go to 0.

4.3.6 Noise

Let us now consider what happens when there is some noise η in the system. In order for the test on the ideal GHZ state not to fail in the all-honest model, the Verifier needs

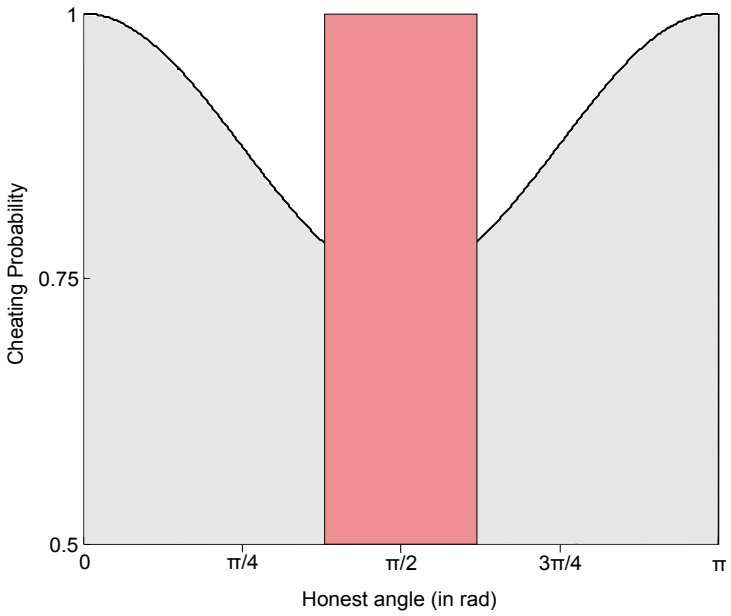


Figure 4.5: Enhanced Protocol - Cheating Probability with 25% losses

to accept η% of test fails. The dishonest parties can again try to exploit this fact by replacing all noisy equipment with perfect one, thus attributing the failure to pass the test, to noise in the system. The probability of writing "fail" in the memory is equal to $1-Q_{\epsilon}^{\lambda}$. If the amount of noise tolerated by our system in each round, is bigger than this amount, then the cheating parties can always atribute each failure of passing the test, to noise in the system. On the contrary, if the noise is smaller than this amount, then the cheating parties will be caught, given enough iterations.

In general, our goal is to compute the probability that an ϵ-away state will be accepted at any point in the protocol. We are therefore interested in computing the probability $P_{l+1}[C_{\epsilon}^{\lambda,\eta}]$ that an "ϵ-away" state has been tested l times and in the $(l+1)^{th}$ iteration, it passes some consistency check on the declared losses and errors, in order to finally accept or reject it:

$$\begin{aligned} P_{l+1}[C_{\epsilon}^{\lambda,\eta}] \quad = \quad & \Pr[\text{check consistency the } l+1 \text{ time after } l \text{ tests}] \cdot \\ & \Pr[\text{pass consistency test the } l+1 \text{ time}] \end{aligned} \tag{4.31}$$

When the Verifier decides to check for consistency, he needs to check that the individual losses of each party are not more than λ% and that the number of test fails is not bigger than the accepted amount ηl. The probability that the state passes the consistency check in the $(l+1)$-round, is given by the cumulative distribution function:

$$
\begin{aligned}
F(\eta l; l, 1-Q_\epsilon^\lambda) &= \Pr[\text{pass consistency test the } l+1 \text{ time}] \\
&= \Pr[\text{less than } \eta l \text{ fails in } l \text{ rounds}] \\
&= \sum_{i=0}^{\lfloor \eta l \rfloor} \binom{l}{i} (Q_\epsilon^\lambda)^{l-i} (1-Q_\epsilon^\lambda)^i \leq e^{-2l(1-Q_\epsilon^\lambda-\eta)^2}
\end{aligned}
$$

As we already mentioned, this function does not control for the individual amount of losses being less that λ%, which is something extra the verifier has to do. It only checks for the optimal way to use the losses to cheat. The last inequality is given by Hoeffding's inequality, when $\eta \leq 1-Q_\epsilon^\lambda$. We can now rewrite the probability 4.31 of using an ϵ-away state at step $l+1$ as:

$$
P_{l+1}[C_\epsilon^{\lambda,\eta}] \leq (1-2^{-S})^l \cdot 2^{-S} \cdot e^{-2l(1-Q_\epsilon^\lambda-\eta)^2}
$$

By integrating over the number of rounds l we can prove the following theorem:

Theorem 12. *Let $|\Psi\rangle$ be an n-party state and $\epsilon = \min_U D\big((I \otimes U)|\Psi\rangle, |G_0^n\rangle\big)$, where U is an operator on the space of the dishonest parties. For an individual loss rate λ, noise $\eta \leq 1-Q_\epsilon^\lambda$ and S a security parameter chosen by the Verifier, the probability that $|\Psi\rangle$ will be accepted by the protocol is upperbounded by $\frac{2^{-S}}{2(1-Q_\epsilon^\lambda-\eta)^2}$.*

If the Verifier wants to keep the above probability less than $1/\delta$ for a specific $\delta > 0$, he needs to choose parameter S equal to $\log \frac{\delta}{2(1-Q_\epsilon^\lambda-\eta)^2}$. It is interesting to note that when $\eta \geq 1-Q_\epsilon^\lambda$, Hoeffding's inequality does not hold anymore, and the probability to have less than ηl fails in l rounds goes to 1, for big enough l, since the average number of fails is $(1-Q_\epsilon^\lambda)l$.

4.4 Experimental Procedure

In this section, we show how, given access to a multiparty GHZ source, we can experimentally check that the enhanced protocol can provide an advantage over the basic protocol in terms of loss tolerance. We note that the described procedure is currently in the process of being experimentally demonstrated for 3-party and 4-party entangled states

created using the experimental setup of [30]. The preliminary results wil be presented in Chapter 6.

For the basic verification protocol of an n-party GHZ state, we need to be able to randomly choose the x_j input bits ($j = 1, \cdots, n-1$) that are used by the parties to measure the state and then fix the Verifier's input x_n such that the sum of all inputs is a multiple of 2.

For the enhanced verification protocol, we need to be able to randomly choose the inputs $\theta_j \in [0, \pi)$ for $j = 1, \ldots, n-1$, sent out by the Verifier to the $n-1$ parties. The last angle θ_n that the Verifier is going to use to measure his qubit, is selected according to the constraint 4.20 on the inputs: $\theta_n = -\sum_{i=1}^{n-1} \theta_i \pmod{\pi}$.

We will describe in detail four tests that can be performed on an n-party GHZ state. The first two concern the basic verification protocol, which uses two measurement settings. The last two concern the enhanced verification protocol with rotated measurements on the Bloch sphere equator.

4.4.1 Tests on an n-party GHZ state

1. Basic test for all honest parties

1. Create $|G_0^n\rangle = \frac{1}{\sqrt{2}}\big(|0^n\rangle + |1^n\rangle\big)$.
2. Run the basic Verification Protocol for n parties.
3. Collect measurement outcomes y_j.

2. Basic test for an unentangled cheating party

1. Create $|G_0^n\rangle = \frac{1}{\sqrt{2}}\big(|0^n\rangle + |1^n\rangle\big)$.
2. Run the basic Verification Protocol for $n+1$ parties, where party A_{n+1} is dishonest, unentangled with the rest and wants to convince the Verifier that the $n+1$ parties share the state $|G_0^{n+1}\rangle$.
3. Honest parties measure as dictated by the protocol and their inputs. Dishonest party A_{n+1} outputs $y_{n+1} = 0$ when $x_{n+1} = 0$ and $y_{n+1} = 1$ when $x_{n+1} = 1$.
4. Collect measurement outcomes y_j.

3. Enhanced test for all honest parties

1. Create $|G_0^n\rangle = \frac{1}{\sqrt{2}}\big(|0^n\rangle + |1^n\rangle\big)$.

2. Run the enhanced Verification Protocol for n parties.

3. Collect measurement outcomes y_j.

4. Enhanced test for an unentangled cheating party

1. Create $|G_0^n\rangle = \frac{1}{\sqrt{2}}\big(|0^n\rangle + |1^n\rangle\big)$.

2. Run the enhanced Verification Protocol for $n+1$ parties, where party A_{n+1} is dishonest, unentangled with the rest and wants to convince the Verifier that the $n+1$ parties share the state $|G_0^{n+1}\rangle$.

3. Honest parties measure as dictated by the protocol and their inputs. Dishonest party A_{n+1} outputs $y_{n+1} = 0$ when $\theta_4 \in [0, \frac{\pi}{2})$ and $y_{n+1} = 1$ when $\theta_4 \in [\frac{\pi}{2}, \pi)$.

4. Collect measurement outcomes y_j.

4.4.2 Comparing experimental results

What is happening in the dishonest case (tests 2 and 4), is that the $n+1$ parties are actually sharing the state $\frac{1}{\sqrt{2}}\big(|0^n\rangle + |1^n\rangle\big)|0\rangle$, and party A_{n+1} is dishonest and unentangled with the rest. For test 2, according to Eq. 4.17, whenever the dishonest party is asked to measure in the X basis, he can output 0, and always pass the test. On the contrary, when he is asked to measure in the Y basis, he is expected to output half of the times 0 and half of the times 1, meaning that he can be try to guess and be correct with probability 1/2.

For test 4, following Eq. 4.27 and Fig. 4.4, when the dishonest party A_{n+1} is asked to measure $\theta_{n+1} \in [0, \frac{\pi}{2})$ he can output $y_{n+1} = 0$ in order to maximize his cheating probability, and when he is asked to measure $\theta_{n+1} \in [\frac{\pi}{2}, \pi)$ he can output $y_{n+1} = 1$.

As mentioned before, when we start introducing losses in the security analysis, we need to take into account that the dishonest parties will try to exploit the losses in order to maximize their cheating probability. We want to upperbound the cheating probability of any type of dishonest party, so we will consider that their detection equipment is perfect (no losses or noise) and that they can replace the communication channels that they use, with perfect ones. For the cases that we are studying, from Eq. 4.25 and Fig. 4.4, it is evident that party A_{n+1} will declare that he lost his qubit for a fraction λ of the data with the lowest probabilities of passing the test. These are the following:

- For test 2, whenever the dishonest party is asked to measure in the Y basis (i.e. $x_{n+1} = 1$).

- For test 4, whenever the dishonest party is asked to measure in a basis which is at a distance $\frac{\lambda\pi}{2}$ from the angle $\frac{\pi}{2}$.

We expect that the loss-tolerant protocol will perform better (i.e. have lower cheating probability) in the presence of losses than the basic protocol. We can check the following for $|G_0^n\rangle$:

1. Run tests 1 and 3 and graphically show the pass probability for the all-honest model for $|G_0^n\rangle$.

2. Observe that the test 2 is completeley broken when losses exceed 50%, in comparison to test 4 that can tolerate more losses.

Since in tests 2 and 4 the dishonest party is not entangled with the honest ones, we expect to observe a difference in the probabilities of passing the tests 2 and 4 when the losses increase. The upperbound on the probability that the test 2 does not fail, can be retrieved from Fig. 4.3, since the grey and red area denotes the bias of the protocol. Therefore the probability that test 2 does not output fail for $\lambda \leq 50\%$, is equal to:

$$(\frac{1}{2}+\lambda)\times 1+(\frac{1}{2}-\lambda)\times\frac{3}{4}=\frac{7}{8}+\frac{\lambda}{4}$$

The upperbound on the probability that the test 4 does not fail, can be retrieved from Eq. 4.30, and we can compare the probabilities of not failing the two tests in Fig. 4.6. Of course, since in all experiments, the created states are always noisy, we will not be able to observe exactly these probabilities experimentally, but we should still see the difference of the two tests, when the tolerated losses increase.

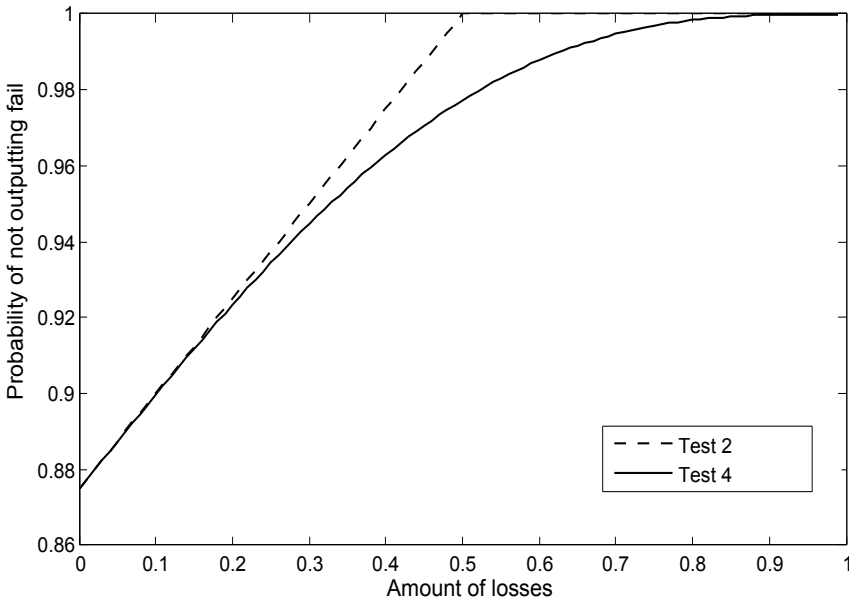


Figure 4.6: Difference in the probability of passing Tests 2 and 4

Finally, we have seen that the probability for a state to pass the test depends on both the amount of tolerated losses and the distance of the state from the GHZ (Eq. 4.29):

$$\Pr[T'(|\Psi\rangle) = 1|\lambda] \leq 1 - \frac{\epsilon^2}{4} + f(\lambda)$$

where $f(\lambda) = \sin(\pi - \lambda\pi)/8(\pi - \lambda\pi)$. It is also interesting to notice that as the Verifier increases the amount of losses that he is willing to tolerate, it will be possible for the dishonest parties to convince the honest ones that they share a noisy $(n+1)$-party GHZ state[5], while in reality they are sharing an n-party GHZ, with the dishonest parties being unentangled with the honest ones.

4.5 Conclusion

In this chapter, we have presented a verification protocol for distributed GHZ states, when the source is untrusted and collaborates with some of the parties. The protocol can tolerate high amounts of losses and noise, and therefore can remain secure in a practical implementation. In order to provide security against the worst case scenario, we assumed that the noise in the channels is controlled by the dishonest coallition, whose members have perfect equipment (i.e. no losses or noise), and can strategically announce their results, by using the amount of losses and noise that is expected from them, in order to maximize their cheating probability.

Our protocol can be useful in the scenario where some party wants to delegate parts of a complex quantum computation to a number of powerful servers, who would require some source of multipartite entanglement in order to perform the joint computation. The protocol can also be used for distributed multipartite computation using the multipartite entangled state as an initial shared resource. In this case, we need to guarantee security for all honest parties at the same time. In other words, we need to iterate the role of the Verifier so that all parties can test the state.

A priori, such a task is impossible, since any such protocol could be used to produce unbiased strong coins [11] (the parties could just measure the entangled state in the computational basis to get a common random bit). Hence, we need to assume that all parties have access to a trusted classical random source (CRS) that provides them with the same randomness. This is, of course, a powerful, but necessary, resource. One way to achieve it would be to assume that at least a third of all parties are honest, since this implies the ability to securely produce random bits only with authenticated classical communication [96]. Note that in order to achieve quantum secure multiparty

[5]The Verifier will be convinced that the honest parties are sharing a noisy $|G_0^{n+1}\rangle$, where the noise is $\epsilon^2 - 4f(\lambda)$.

computation, at least a majority of honest parties is required [97], in which case it is possible to construct a CRS.

It is interesting to note that while the Basic Verification Protocol was already known, as it is a natural generalisation of the Mermin-GHZ game, we have arrived to the Enhanced Verification Protocol without knowledge of the BDHT protocol [94]. The two protocols are in essence the same, but the reasons that led to their proposal are completely different. We were forced to introduce more measurement bases in order to tolerate more losses, while the goal of the authors of [94] was to increase the gap between quantum and classical communication complexity. Since the simple idea of increasing the measumerent bases of the parties of a game has already proven useful in two completely different scenarios, there could be other multiparty settings that could benefit from the same technique.

Finally, a point that a reader could raise while reading Section 4.3, is that a Verifier could avoid malicious use of the losses, by checking uniformity on the declared lost inputs. If a party always declares loss for a specific outcome, then the Verifier could suspect malicious activity. This can very easily be overcome by a dishonest source, since it can do local operations on the state, and "move" it on the horizontal axis of the graphical representation. This way, the source keeps the state curve the same, but changes the angles at which it takes its maximum, or equivalently where it provides the minimum cheating probabilities. Since the dishonest parties collaborate with the source, they know at each round which set of inputs they should discard (by declaring loss), since at the specific round, the specific set has the lowest cheating probability. We have not included this analysis in the chapter, since it does not change the cheating probability, but we assume that in a real-life implementation, the Verifier should check for uniformity in the lost inputs.

One important open question is whether the upper-bounds in Theorems 7 and 9, and respectively the ones in Theorems 10 and 11, can be improved. For specific states such as the orthogonal state to the GHZ, $|G_\pi^n\rangle = \frac{1}{\sqrt{2}}(|0^n\rangle - |1^n\rangle)$, it seems that the probability of passing the test in the all-honest model is 0, while in the dishonest model, it is 1, since the coalition of dishonest parties, need only output the opposite value of their measurements each time. Finally, it would be interesting to study the behavior of other entangled states, and most significantly of graph states, since the test that we are using can easily be expressed using the stabiliser formalism.

Chapter 5

Quantum Games

5.1 Introduction

Game Theory is the study of strategic decision-making processes through a well defined mathematical framework. We can think of two general subsets of games according to whether the interests of the players coincide or are conflicting. A typical example of the first type of games, which we will call *common interest* games, is when the drivers of vehicles decide on which side of the road they will drive in order to avoid accidents. We can suppose that they do not have any preference on the side, but they both want to agree on their decision. When they both decide to drive on the same side (respectively to their view of the road), they win 1 point, while when they decide on different sides, they lose 1 point (because they crash their cars).

The second type of games, which we will call *conflicting interest* games, emerge from cases where the interests of the players are different. A typical example of this type of games is the *Battle of the Sexes*, where Alice and Bob want to meet on Saturday night, but Alice prefers going to the ballet, while Bob wants to go to the theater. In this specific example, even though the players prefer to coordinate their actions rather than spend the evening alone, their preferred outcomes differ. For example, when they both go to the ballet, Alice wins 2 points and Bob 1, when they go to the theater, Alice wins 1 point and Bob 2, and when they go to different places, they do not get any points.

In Table 5.1 we can see the two aforementioned examples of the different types of two-player games in the form of a utility table, where in each cell, the first number is the utility for Alice and the second is the utility for Bob.

However, in real life scenarios, the utilities of the players might depend on other parameters as well. For example, the two players of the Battle of the Sexes might change their preferences according to whether they are angry with each other. If one of the two players is angry with the other one, then he/she might prefer to avoid a meeting either

A \ B	Left	Right
Left	(1,1)	(-1,-1)
Right	(-1,-1)	(1,1)

(a) Choosing Sides

A \ B	Ballet	Theater
Ballet	(2,1)	(0,0)
Theater	(0,0)	(1,2)

(b) Battle of the Sexes

Table 5.1: Common and Conflicting Interest Games

at the theater or the ballet. We consider that this information (what we call the *type* of a player), is only known to the player himself, and is therefore kept secret from the other player. The games that depend on the types of the players, are called games of *incomplete information*, or *Bayesian* games, after mathematician Thomas Bayes who first investigated the effect of partial information on probabilities.

Bayesian games were introduced by Harsanyi in 1967 [24] and are of great interest to quantum communication theory. In fact, all quantum games that have been shown to have an advantage compared to their classical equivalents, belong to this category of games of incomplete information. For example, the well-known CHSH game [25], where the two players, Alice and Bob, receive their inputs at random and share an entangled state, is a Bayesian game, since each player needs to decide on his output without knowing the input of the other player. The advantage that Quantum Mechanics provides compared to classical resources for Bayesian games has therefore been known for some time, with a more recent contribution appearing in [26].

However, all previous studies of quantum games, considered common interest games. The main question that we will adress in this Chapter is whether Quantum Mechanics provides an advantage for conflicting interest Bayesian games as well. We will present a two-player quantum Bayesian game that combines the Battle of the Sexes and the CHSH game. At the beginning of the game, each player will choose at random his type, which will be kept secret from the other player, but will determine the payoffs of both players.

We will study players with deterministic strategies as well as players who decide on their output based on some advice from a third party. We will examine two types of advice, in the form of a classical string and in the form of a quantum entangled state, and we will analyse the possible strategies that may be followed according to the different types of advice. By computing the payoffs for the two players, we will show that the quantum advice can lead to a fair strategy that is a point of equilibrium for the two players and that provides higher payoffs than possible by any classical advice. This quantum advantage will also be experimentally demonstrated using a commercial entangled photon source, by playing the game and analysing the measurement outcomes.

5.2 Bayesian Games

We will start by defining a Bayesian game in the two-party framework (for a more general definition of Bayesian games, refer to [27]). It comprises of:

- Two players, Alice (A) and Bob (B).
- A set $\mathcal{X} = \mathcal{X}_A \otimes \mathcal{X}_B$ of types/measurements $x = \{x_A, x_B\}$, where $x_A \in \mathcal{X}_A$, $x_B \in \mathcal{X}_B$.
- A set $\mathcal{Y} = \mathcal{Y}_A \otimes \mathcal{Y}_B$ of actions/outcomes $y = \{y_A, y_B\}$, where $y_A \in \mathcal{Y}_A$, $y_B \in \mathcal{Y}_B$.
- A utility function $u_i : \mathcal{X}_A \times \mathcal{X}_B \times \mathcal{Y}_A \times \mathcal{Y}_B \to \mathbb{R}$ for each player $i \in \{A, B\}$ and for all combinations of types and actions of the two players.
- A probability distribution[1] on the types of the players, $P : \mathcal{X} \to [0, 1]$.

The utility functions u_A and u_B for each combination of the players' types can be viewed in the form of a table: the rows correspond to the possible values of variable y_A and the columns correspond to the possible values of variable y_B. The numbers in each cell are the players' utilities (u_A, u_B) according to their types and actions. In case the utilities differ for different types of the two players, then we need to introduce more than one tables. In general, each player $i \in \{A, B\}$ is interested in maximizing his average payoff F_i defined as follows:

$$F_i = \sum_{\substack{x \in \mathcal{X} \\ y \in \mathcal{Y}}} P(x) \Pr(y|x) u_i(x, y) \tag{5.1}$$

The game is played as shown in Fig. 5.1. The inputs of the players are chosen following a product probability distribution $P = P_A \times P_B$, therefore each player $i \in \{A, B\}$ acquires a type x_i according to the probability distribution P_i. They also receive an advice from a source which is independent of the chosen inputs x_i. Finally, they decide on their action/output y_i, according to a chosen strategy.

There exist three types of classical strategies that each player $i \in \{A, B\}$ can follow, with only the third one being dependent on the advice received by the source:

1. A pure strategy $\sigma_i : \mathcal{X}_i \to \mathcal{Y}_i$, where the action of the player depends deterministically on his type (or in other words, only one action is played with positive probability). If both players follow a pure strategy $\sigma = (\sigma_A, \sigma_B)$, the average payoff for player $i \in \{A, B\}$ becomes:

[1] In our game, P will be a product probability distribution, $P = P_A \times P_B$, since the players choose their types uniformely at random. However, in games like the Mermin game of Section 2.3.2, there is a correlation between the types of the players, given by a specific constraint.

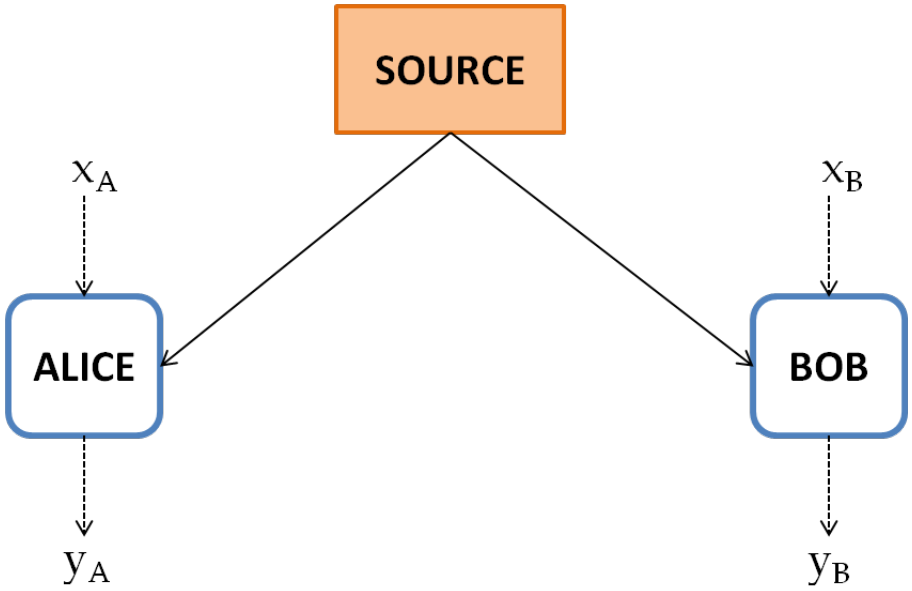


Figure 5.1: The Bayesian Game for two players

$$F_i(\sigma) = \sum_{x \in \mathcal{X}} P(x) u_i(x_A, x_B, \sigma_A(x_A), \sigma_B(x_B)) \tag{5.2}$$

2. A mixed strategy, $\pi_i : \mathcal{X}_i \otimes \Omega_i \to \mathcal{Y}_i$, where Ω_i is the space of advice given to player i by the source. The source chooses the advice $r = (r_A, r_B)$ from the space $\Omega = \Omega_A \times \Omega_B$ following a product probability distribution $p = p_A \times p_B$. If both players follow a mixed strategy $\pi = (\pi_A, \pi_B)$, the average payoff for player $i \in \{A, B\}$ becomes:

$$F_i(\pi) = \sum_{x \in \mathcal{X}} \sum_{\substack{r_A \in \Omega_A \\ r_B \in \Omega_B}} P(x) p(r_A) p(r_B) u_i(x_A, x_B, \pi_A(x_A, r_A) \pi_B(x_B, r_B)) \tag{5.3}$$

3. A correlated strategy $c_i : \mathcal{X}_i \otimes \Omega_i \to \mathcal{Y}_i$, where Ω_i is the space of advice given to player i by the source. The source chooses the advice $r = (r_A, r_B)$ from the space $\Omega = \Omega_A \times \Omega_B$ following a probability distribution q that may not be a product distribution (i.e. the advices given to the two parties can be correlated). If both players follow a correlated strategy $c = (c_A, c_B)$, the average payoff for player $i \in \{A, B\}$ becomes:

$$F_i(c) = \sum_{x \in \mathcal{X}} \sum_{\substack{r_A \in \Omega_A \\ r_B \in \Omega_B}} P(x) q(r) u_i(x_A, x_B, c_A(x_A, r_A), c_B(x_B, r_B)) \tag{5.4}$$

Finally, when the players are quantum devices and receive a quantum state as advice from a third party:

4. A quantum strategy $\mathcal{M} = (\mathcal{A}, \mathcal{B}, \rho)$, where $\mathcal{A} = \{\mathcal{A}_0, \mathcal{A}_1\}$, $\mathcal{B} = \{\mathcal{B}_0, \mathcal{B}_1\}$, that consists of Alice and Bob applying respectively the observables $\mathcal{A}_{x_A} = \{A^0_{x_A}, A^1_{x_A}\}$ and $\mathcal{B}_{x_B} = \{B^0_{x_B}, B^1_{x_B}\}$ on the quantum state ρ shared between them. The probability of the two players producing as output y given x, is $\Pr(y|x) = \mathrm{tr}(M^y_x \rho)$, where $M^y_x = A^{y_A}_{x_A} \otimes B^{y_B}_{x_B}$. The average payoff for player $i \in \{A, B\}$ becomes:

$$F_i(\mathcal{M}) = \sum_{\substack{x \in \mathcal{X} \\ y \in \mathcal{Y}}} P(x) \mathrm{tr}(M^y_x \rho) u_i(x, y) \tag{5.5}$$

It is important to note that any kind of advice, either classical, like the choice of r or quantum, in the form of a state, must be independent of the choice of types x_A and x_B. In essence this condition is what is called "*non-signaling*" in the quantum mechanical context, because it does not allow for one player to instantaneously communicate with the other players:

$$\Pr(y_i|x_A, x_B) = \Pr(y_i|x_i), \qquad \forall i \in \{A, B\}$$

We know from classical Game Theory that correlated strategies provide at least as good average payoffs for the players as pure or mixed ones. We also know that for *complete information* games, where the players have complete information on the types of the other players, quantum correlations do not provide any advantage compared to classical correlations [23]. For games of incomplete information though, Brunner and Linden [26] gave several examples of Bayesian games, where the players' average payoffs are higher when they share entanglement. These examples were restricted to common interest games, where the players always prefer the same action (or have no preference). In Table 5.2 we can see the payoff functions of the two-player game of Example 1 in [26], where Alice and Bob have two types each, $x_A, x_B \in \{0, 1\}$ and follow actions $y_A, y_B \in \{0, 1\}$. Since the utility functions of both players are the same, the strategy that maximizes one player's payoff also maximizes the other player's playoff, therefore the two players have common interests. Note that in [26], the authors also present games where the payoff functions are not the same for the two players, but they are all common interest games, since the players prefer the same actions for given inputs and advices.

A \ B	0	1
0	(4,4)	(-4,-4)
1	(-4,-4)	(4,4)

(a) $x_A \wedge x_B = 0$

A \ B	0	1
0	(-4,-4)	(4,4)
1	(4,4)	(-4,-4)

(b) $x_A \wedge x_B = 1$

Table 5.2: Common Interest Game

5.3 Nash Equilibria

Some pairs of strategies are points of equilibrium for the two players, since none of them has any incentive to change their strategy. The specific pairs of strategies are called *Nash Equilibria* (N.E.), after the American mathematician John Nash who redefined the notion of equilibirum introduced by von Neumann and Morgenstern [98], in order to prove that any game with finite actions has an N.E. [99]. Below we give the definitions of the pure, mixed and correlated classical N.E. for two player games, in accordance to the different classical strategies that the players can adopt.

Definition 1. *A pure Nash Equilibrium is a strategy $\sigma = \{\sigma_A, \sigma_B\}$ such that no player $i \in \{A, B\}$ can gain a higher payoff by choosing a strategy different than σ_i, given that the other player $\neg i$ adheres to his strategy.*

$$F_i(\sigma_i, \sigma_{\neg i}) \geq F_i(\sigma_i', \sigma_{\neg i}), \quad \forall i \in \{A, B\}$$

Definition 2. *A mixed Nash Equilibrium is a strategy $\pi = \{\pi_A, \pi_B\}$ based on advice $r = (r_A, r_B)$ that follows a product probability distribution, such that no player i can gain a higher payoff by choosing another probability distribution different than π_i, given that the other player $\neg i$ adheres to his strategy.*

$$F_i(\pi_i, \pi_{\neg i}) \geq F_i(\pi_i', \pi_{\neg i}), \quad \forall i \in \{A, B\}$$

Definition 3. *A Nash-Bayes (or Correlated) Equilibrium is a strategy $c = (c_A, c_B)$ based on advice $r = (r_A, r_B)$ that follows a probability distribution that may not be a product, such that no player i can gain a higher payoff by choosing a strategy different than c_i, given that the other player $\neg i$ adheres to his strategy.*

$$F_i(c_i, c_{\neg i}) \geq F_i(c_i', c_{\neg i}), \quad \forall i \in \{A, B\}$$

Finally, we give the definition of a Quantum Nash Equilibrium, that depends on the advice in the form of a quantum state, that the players receive from the source:

Definition 4. *A Quantum Equilibrium is a strategy $\mathcal{M} = (\mathcal{A}, \mathcal{B}, \rho)$, such that no player can gain a higher payoff by choosing a strategy different than $\mathcal{A}$ (for Alice) or $\mathcal{B}$ (for Bob), given that the other player adheres to his strategy. In other words, for $i \in \{A, B\}$:*

$$\begin{aligned} F_i(\mathcal{A}, \mathcal{B}, \rho) &\geq F_i(\mathcal{A}', \mathcal{B}, \rho) \\ F_i(\mathcal{A}, \mathcal{B}, \rho) &\geq F_i(\mathcal{A}, \mathcal{B}'\rho) \end{aligned}$$

5.4 The Game

Let us examine more closely the Battle of the Sexes, shown in Table 5.1b. This game is a complete knowledge conflicting interest game with two pure Nash Equilibria strategies, the strategies (Ballet, Ballet) and (Theater, Theater). A common problem for the players of such games, is how to choose a strategy that is a Nash Equilibrium, given that the players have conflicting interests (i.e. here Alice prefers the first N.E. and Bob the second). Classical correlations in the form of a classical bit send to both players, can resolve this problem, by helping the players choose with half probability the first N.E. and with half probability the second.

Here we will study the effect of classical and quantum correlations in incomplete knowledge conflicting interest games by examining a Bayesian game that combines the "Battle of the Sexes" and the CHSH game. The game is defined by the payoffs of the two players as described by the utility tables in Figure 5.2. We have two utility tables, depending on the logical AND of the types of the players.

y_A \ y_B	0	1
0	(1,1/2)	(0,0)
1	(0,0)	(1/2,1)

(a) $x_A \wedge x_B = 0$

y_A \ y_B	0	1
0	(0,0)	(3/4,3/4)
1	(3/4,3/4)	(0,0)

(b) $x_A \wedge x_B = 1$

Figure 5.2: Conflicting Interest Game

We will study the different classical and quantum strategies mentioned in the previous section, and examine if there exist quantum correlations resulting in quantum strategies that perform better than the classical ones. We will also examine if there exist strategies

that are quantum equilibria, and compare them to the classical correlated equilibria of the players. From the analysis of the quantum game, we will find a single point of quantum equilibrium that provides fair average payoffs for the two players (i.e. $F_A = F_B$), and is strictly better than any fair classical strategy, either pure, mixed or correlated.

5.5 Classical Strategies

In general, we will consider that the players choose their types at random: $\Pr(x_i = 0) = \Pr(x_i = 1) = 1/2$, for $i \in \{A, B\}$. We will examine both pure and correlated strategies, where the source gives to each player $i \in \{A, B\}$ an advice in the form of a bit r_i at the beginning of the game[2].

We can find three pure Nash Equilibria for our Bayesian game, that do not depend on any advice, classical or quantum. Let us first analyse the pure joint strategy for Alice and Bob that leads to equal classical average payoffs ($F_A = F_B$), and also examine why this strategy is a Nash Equilibrium.

Fair pure classical N.E.
Alice outputs $y_A = \sigma_A(x_A) = x_A$ and Bob outputs $y_B = \sigma_B(x_B) = 1 - x_B$

From Eq. 5.2 we can compute the average payoffs of the two players for this pure strategy and verify that it is indeed a fair classical strategy that attains average payoffs $F_A = F_B = \frac{9}{16} = 0.5625$. We would like to examine if it is also a pure Nash equilibrium (N.E.), meaning that no player has an incentive to change their strategy, given that the other player conforms to the strategy by applying the action dictated by it.

Fix Alice's strategy

Let's assume that Alice has a fixed action and examine if Bob can increase his average payoff by changing his strategy. If $x_B = 0$, then Bob knows that his payoff is calculated with respect to the Table 5.2a. If $x_B = 1$, then he is no longer sure with respect to which table his utility function is derived. If the players are choosing their inputs at random, then Alice gets input x_A equal to 0 or 1 with probability $1/2$. Let us compute the utility functions $u_B(x_A, x_B, y_A, y_B)$ for the different values of $x = (x_A, x_B)$.

- $x_B = 0$: $\begin{cases} \text{If } x_A = 0, & \text{then } u_B(0,0,0,1) = 0 \text{ and } u_B(0,0,0,0) = 1/2 \\ \text{If } x_A = 1, & \text{then } u_B(1,0,1,1) = 1 \text{ and } u_B(1,0,1,0) = 0 \end{cases}$

[2]The advice needs not contain more than one bit for each player, since there are only two different actions for every player.

- $x_B = 1$: $\begin{cases} \text{If } x_A = 0, & \text{then } u_B(0,1,0,0) = 1/2 \text{ and } u_B(0,1,0,1) = 0 \\ \text{If } x_A = 1, & \text{then } u_B(1,1,1,0) = 3/4 \text{ and } u_B(1,1,1,1) = 0 \end{cases}$

The first utility function is the one that results from Bob following the strategy, while the second one is for Bob outputting the opposite from what the strategy dictates. For $x_B = 1$, we can see that Bob has no incentive to change his strategy, since his utility would be equal to zero, for both inputs of Alice. For $x_B = 0$, since $\Pr[x_A = 0] = \Pr[x_A = 1] = 1/2$, Bob would again decrease his average payoff if he decided to change his strategy.

Fix Bob's strategy

Similarly, let's assume that Bob has a fixed action and examine if Alice can increase her payoff function by changing her action. Again, Bob gets his input x_B equal to 0 or 1 with probability $1/2$.

- $x_A = 0$: $\begin{cases} \text{If } x_B = 0, & \text{then } u_A(0,0,0,1) = 0 \text{ and } u_A(0,0,1,1) = 1/2 \\ \text{If } x_B = 1, & \text{then } u_A(0,1,0,0) = 1 \text{ and } u_A(0,1,1,0) = 0 \end{cases}$
- $x_A = 1$: $\begin{cases} \text{If } x_B = 0, & \text{then } u_A(1,0,1,1) = 1/2 \text{ and } u_A(1,0,0,1) = 0 \\ \text{If } x_B = 1, & \text{then } u_A(1,1,1,0) = 3/4 \text{ and } u_A(1,1,0,0) = 0 \end{cases}$

Again, the first utility function is the one that results from Alice following the strategy, while the second one is for Alice outputting the opposite from what the strategy dictates. For $x_A = 1$, we can see that Alice has no incentive to change her strategy, since her utility function is equal to zero for both of Bob's inputs. For $x_A = 0$, since $\Pr[x_B = 0] = \Pr[x_B = 1] = 1/2$, Alice again does not increase her payoff by changing her strategy.

Let us now present the two remaining pure Nash Equilibria:

Pure classical Nash Equilibria

1. Alice: $\sigma_A(x_A) = 0$, Bob: $\sigma_B(x_B) = x_B$
2. Alice: $\sigma_A(x_A) = 1 - x_A$, Bob: $\sigma_B(x_B) = 1$

The first joint strategy provides the following average payoffs to the two players: $F_A = 0.6875$, $F_B = 0.4273$ and the second $F_A = 0.4273$ and $F_B = 0.6875$.

In the case of mixed or correlated strategies, where each player $i \in \{A, B\}$ receives some classical advice from the source in the form of a bit r_i, the average payoff of player $i \in \{A, B\}$ according to 5.4, is the following:

$$F_i(c) = \sum_{x \in \mathcal{X}} \sum_{\substack{r_A \in \Omega_A \\ r_B \in \Omega_B}} P(x) q(r) u_i(x_A, x_B, c_A(x_A, r_A), c_B(x_B, r_B))$$

where c_i is a correlated strategy $c_i : \mathcal{X}_i \otimes \Omega_i \to \mathcal{Y}_i$, Ω_i is the space of advice given to player i by the source and q is the probability distribution used by the source to choose the advice $r = (r_A, r_B)$ from the space $\Omega = \Omega_A \times \Omega_B$. Since q is not assumed to be a product distribution, the advice shared between the players is possibly correlated.

In general, we assume that when the two players receive some classical advice from the source, they know the probability distribution that the source is using. If it is a product probability distribution, then there is no correlation between the players' strategies, and the source can be substituted by a coin that each player flips, in order to decide on his action. On the other hand, if the probability distribution with which the source chooses the bits, is not a product, then the strategies of the two players are correlated.

For example, when the advice is a common coin r sent to both Alice and Bob, there are 6 correlated Nash Equilibria that provide the following three combinations of payoffs (the same combination of payoffs can result from two different correlated strategies):

1. $F_A = 0.625, \quad F_B = 0.5$
2. $F_A = 0.5, \quad F_B = 0.625$
3. $F_A = 0.5625, \quad F_B = 0.5625$

In order to find all the correlated equilibria of the game, we can solve our optimisation problem using linear programming. By examining all possible strategies for all types of classical advice, we observe that the average payoff for any player cannot exceed the value $\frac{3}{4}$, for any form of advice sent by the source. Furthermore, the two players cannot have their average payoff functions achieve their maximum at the same time; when $F_A = \frac{3}{4}$, it holds that $F_B = \frac{3}{8}$ and equivalently the other way around. We can finally verify that:

$$F_A + F_B \leq \frac{9}{8} = 1.125$$

for any classical strategy that the two players decide to follow, either with or without advice.

5.6 Quantum Strategies

Now let us consider the case where the source is sending quantum advice to the two players, in the form of a 2-qubit quantum state shared between the two parties. We will first examine a set of quantum measurements in the case of a maximally entangled EPR pair, and then we will examine what happens when the shared state is not maximally entangled.

5.6.1 Maximally Entangled Strategy

First suppose that the shared state is an EPR pair $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. In Section 5.2, we have seen that a quantum strategy consists of the state $|\Phi\rangle$ and the observables that Alice and Bob apply to the state. The average payoff for each player is then given by Eq. 5.5. Similar to the analysis of the CHSH game by Cleve et al [28], if the players, depending on their inputs, use the projective measurements:

$$\begin{aligned}
\mathcal{A}_0^a &= |\phi_a(0)\rangle\langle\phi_a(0)| \\
\mathcal{A}_1^a &= |\phi_a(\frac{\pi}{4})\rangle\langle\phi_a(\frac{\pi}{4})| \\
\mathcal{B}_0^b &= |\phi_b(\frac{\pi}{8})\rangle\langle\phi_b(\frac{\pi}{8})| \\
\mathcal{B}_1^b &= |\phi_b(-\frac{\pi}{8})\rangle\langle\phi_b(-\frac{\pi}{8})|
\end{aligned}$$

for $a, b \in \{0,1\}$, where $\phi_0(\theta) = \cos\theta|0\rangle + \sin\theta|1\rangle$ and $\phi_1(\theta) = -\sin\theta|0\rangle + \cos\theta|1\rangle$, we have:

$$\Pr(y_A, y_B|x_A, x_B) = \frac{1}{2}\mathrm{tr}(\mathcal{A}_{x_A}^{y_A}, \mathcal{B}_{x_B}^{y_B}) = \frac{1}{2}\cos^2\frac{\pi}{8}$$

Then, for $i \in \{A, B\}$, Eq. 5.5 becomes:

$$F_i = \frac{1}{8}\cos^2\frac{\pi}{8}\sum_{\substack{x\in\mathcal{X}\\ y\in\mathcal{Y}}} u_i(x,y) = \frac{3}{4}\cdot 0.85$$

We can use Semidefinite programming (SDP) [100–102] with appropriate constraints, in order to show that the specific quantum strategy $\mathcal{M} = (\mathcal{A}, \mathcal{B}, |\Phi\rangle)$, which consists of the maximally entangled state $|\Phi\rangle$ and the set of measurements defined above, is a quantum Nash Equilibrium point, since if any of the two players changes his measurements, this will only result in a lower payoff for the specific player.

We also note that this specific strategy is fair for both players, since it gives equal

average payoffs. However, in the previous section we have seen that there exist classical not fair strategies that give higher average payoffs for a single player than the quantum fair one. But if we look instead at the payoff sum, we have that $F_A^{fair}+F_B^{fair} = \frac{3}{2}\cdot 0.85$ which is always larger than $\frac{9}{8}$, the upperbound for the sum of the payoffs of any classical strategy, with or without advice from a third party. We can therefore observe the advantage provided by the sharing of an entangled state, if we look at both players' average payoffs at the same time.

5.6.2 Non-maximally entangled strategy

In the case where the shared state is not the maximally entangled one, there are specific strategies that maximize the sum of the payoffs $F_A + F_B$. We can also define and solve an SDP in order to find the measurements that maximize the sum of the payoffs for all amounts of entanglement. We only consider pure states of the form:

$$|\Psi\rangle = \sqrt{a}|00\rangle + \sqrt{1-a}|11\rangle$$

where $a \in [0,1]$ since these give the highest amount of correlations and help us visualise the limit of the quantum advantage on our Bayesian game. If the shared state is a mixed state, then the payoffs of the game would lie in the space bounded by the pure states. For any $a \in (0,1)$, we can find strategies that achieve a higher sum for the players' payoffs than classically possible.

However, none of the non-maximally entangled strategies that maximize the sum of the payoffs is a quantum N.E., since for any fixed strategy, there is always a set of measurements for one of the players, that increases his payoff. Note also that in the case where the quantum state is separable, any quantum strategy is equivalent to a classical correlated strategy, therefore, the sum of the payoffs does not exceed the classical limit of $\frac{9}{8}$.

In the case where the shared state is in the form of a Werner state: $\rho = \alpha|GHZ\rangle\langle GHZ| + (1-\alpha)\mathbb{I}$, then there exists at least one quantum Equilibrium, which is also fair since it provides equal average payoffs for the two players.

5.7 Experiment

The game that we have previously defined, allows to test the quantum advantage experimentally in a straightforward way, using a commercial Entanglement Generator Device (EGD) from QuTools [29]. The source creates entangled pairs, which we will use to play our game. We measure each state using the same bases as the ones defined in the

previous section, depending on each player's input. More specifically, Alice measures in $\{\mathcal{A}^0_{x_A}, \mathcal{A}^1_{x_A}\}$ and Bob measures in $\{\mathcal{B}^0_{x_B}, \mathcal{B}^1_{x_B}\}$. For each input (x_A, x_B), we want to find:

$$\Pr(y_A, y_B|x_A, x_B) = \frac{\text{number of detections } (\mathcal{A}^{y_A}_{x_A}, \mathcal{B}^{y_B}_{x_B})}{\text{total number of detections for } (x_A, x_B)}$$

The EGD has two output channels that have been connected to a Time-to-Digital Converter (TDC), in order to count the produced coincidences between the detectors of Alice and Bob. The TDC gives us access to both the individual counts of each detector (Channels 1 and 2) and to the coincidences between them (Channel 1/2). An example of the outcomes registered by the TDC for a random choice of inputs and measurements can be seen in Fig. 5.3.

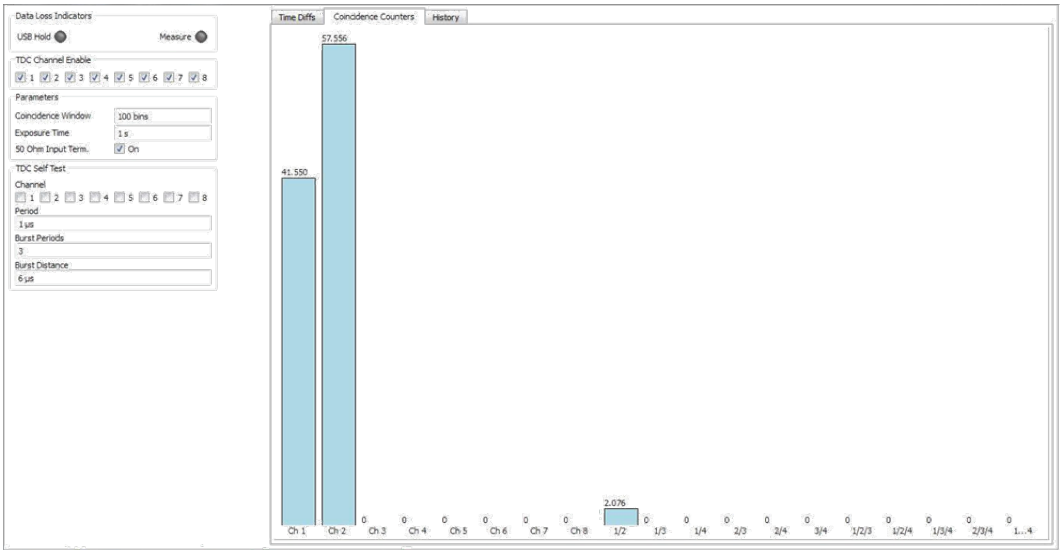


Figure 5.3: TDC coincidence output

In Table 5.3 we report the detection probabilities for the different types/inputs of the two players, when they follow the fair strategy of Section 5.6.1. The fidelity of the shared state to the EPR pair $|\Phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ has been measured to be 0.92113, while the CHSH value (see Eq. 2.2) is 2.5757.

x_A	x_B	$\Pr(00\|x_A, x_B)$	$\Pr(01\|x_A, x_B)$	$\Pr(10\|x_A, x_B)$	$\Pr(11\|x_A, x_B)$
0	0	0.4273228	0.0530423	0.0722661	0.4473687
0	1	0.3872412	0.1363457	0.1033597	0.3730534
1	0	0.3494993	0.1198082	0.1221244	0.408568
1	1	0.0573576	0.4456929	0.4491154	0.047834

Table 5.3: Detection probabilities for the fair strategy

However, the reported coincidences also contain some errors due to the so-called dark counts of the single-photon detectors. We introduce the following method in order to remove the effect of the detectors' dark counts and find the "true" coincidence count. We take a second output from Channel 1 of EGD and connect it to Channel 3 of the TDC. The output of this channel is delayed with respect to the outputs of Channels 1 and 2, by using a wire that is 5 meters larger than the others. Given that the coincidence window is kept sufficiently narrow so that the time delay introduced in this way exceeds it, the coincidences registered in Channel 2/3 are only due to the detectors' dark counts. Figure 5.4 shows the TDC's output, when the above procedure is followed.

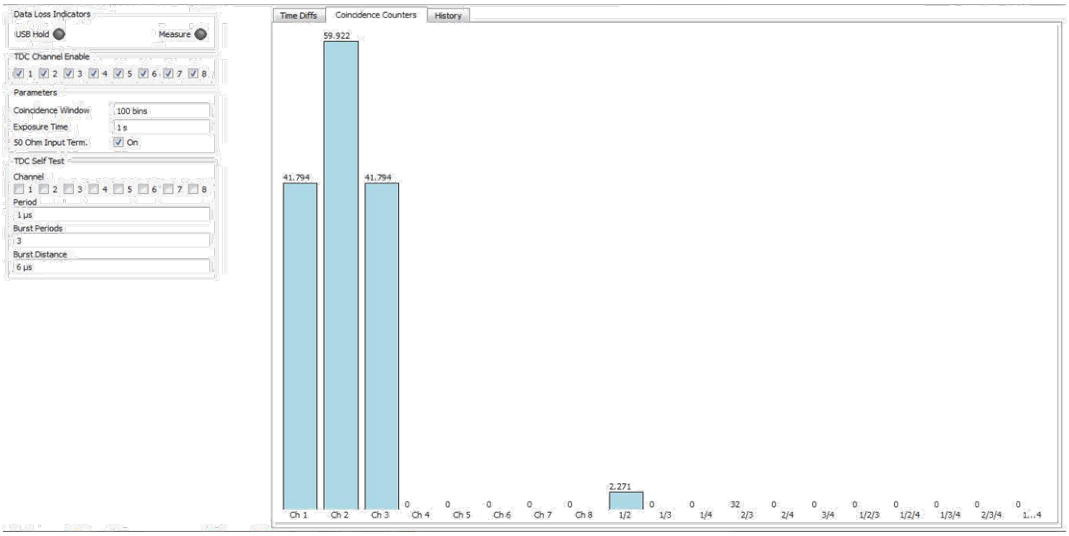


Figure 5.4: TDC coincidence output showing dark counts

We can then subtract that amount from the Channel 1/2 count and find the coincidence counts that result solely from the entangled state created by the EGD. As expected, the computed fidelity and the CHSH value are slightly better than before, since we have removed any errors that occured from the dark counts. More specifically, the fidelity of the shared state to $|\Phi\rangle$ is found to be 0.925 and the CHSH value 2.645.

x_A	x_B	$\Pr(00\|x_A,x_B)$	$\Pr(01\|x_A,x_B)$	$\Pr(10\|x_A,x_B)$	$\Pr(11\|x_A,x_B)$
0	0	0.4491658	0.0686175	0.0475147	0.4347020
0	1	0.3961272	0.1310704	0.103023	0.369779
1	0	0.3522228	0.1122319	0.1168883	0.418657
1	1	0.0556158	0.4384785	0.4633638	0.042542

Table 5.4: Detection probabilities after removal of dark counts

Table 5.4 contains the detection probabilities for combinations of inputs and mea-

surements, when the previously mentioned procedure of subtracting the dark counts has been implemented. Finally, in Table 5.5, we show the average payoff functions for both players with fixed inputs (x_A, x_B) before and after the removal of the dark counts ($F_i(x_A, x_B)$ and $F_i'(x_A, x_B)$ respectively), for both players $i \in \{A, B\}$.

x_A	x_B	$F_A(x_A, x_B)$	$F_B(x_A, x_B)$	$F_A'(x_A, x_B)$	$F_B'(x_A, x_B)$
0	0	0.6510072	0.66103	0.6665168	0.6592849
0	1	0.5737679	0.566674	0.5810169	0.567843
1	0	0.5537833	0.5833176	0.5615513	0.5947684
1	1	0.6711062	0.6711062	0.6763817	0.6763817

Table 5.5: Comparison of detection probabilities before and after removal of dark counts

We can now compute the average quantum payoffs of both players before and after the removal of dark counts:

$$F_A = \frac{1}{4}\sum_{x_A,x_B} F_A(x_A, x_B) = 0.612416, \quad F_B = \frac{1}{4}\sum_{x_A,x_B} F_B(x_A, x_B) = 0.620532$$

$$F_A' = \frac{1}{4}\sum_{x_A,x_B} F_A'(x_A, x_B) = 0.621367, \quad F_B' = \frac{1}{4}\sum_{x_A,x_B} F_B'(x_A, x_B) = 0.624569$$

and check that the sum of the payoffs is well above the classical value 1.125 ($F_A + F_B = 1.232948$ and $F_A' + F_B' = 1.245936$). Both these sums are slightly below the maximum value imposed by quantum mechanics, as expected due to the distance of the generated state from the EPR pair.

In Figure 5.5 we compare the optimal classical strategies with the quantum joint strategies that maximize the sum of payoffs, and also show the fair quantum strategy that is also a Nash Equilibrium. Furthermore, we report the experimental data obtained after the removal of the dark counts, and verify that the results lie above the classical limit, but below the optimal quantum one, since the fidelity to the EPR pair is smaller than one.

5.8 Conclusion

In this Chapter, we have presented and analysed a two-player Bayesian game with conflicting interests. We showed that if the players receive advice from an entangled source (in the form of a shared entangled state), they can increase their payoffs by exploiting the correlations of the quantum state. This is done by performing specific measurements

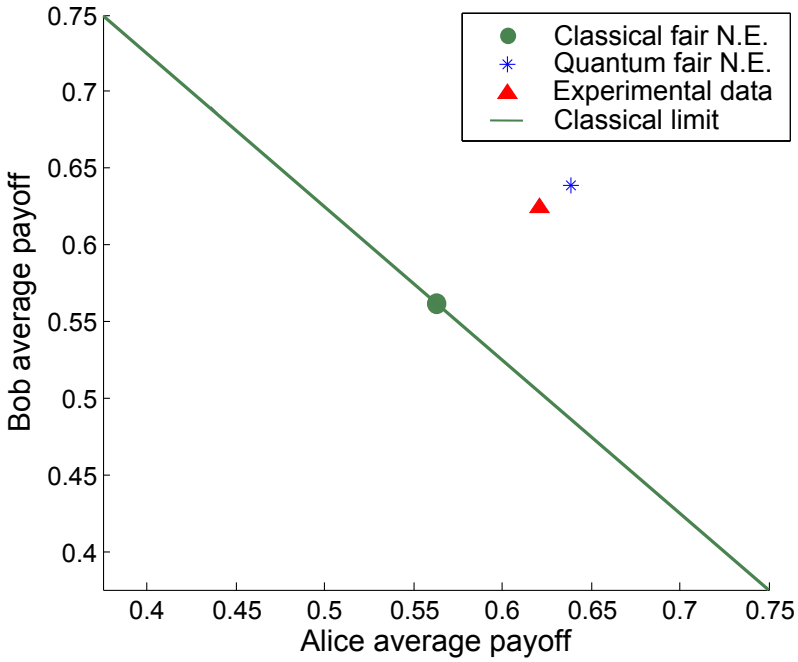


Figure 5.5: Comparison of classical and quantum strategies

according to the shared quantum state and choosing their actions according to the outcomes of these measurements. We then used a commercial entangled photon source to play the game and compute the average payoffs of the players. We demontrated a clear advantage of quantum communication, since the sum of the payoffs achieved in our experiment is higher than any classical strategy, pure or correlated, could achieve.

Since the players have conflicting interests, the preferred action of one player will reduce the payoff of the other player. Consequently, this means that it could be hard to find joint quantum strategies on which both players will agree to commit to. Indeed, from the examined joint strategies that maximize the sum of payoffs, we only found one Nash Equilibrium, which is precisely the one equivalent to the CHSH game [25] for a maximally entangled state. Of course, if the shared state is a noisy maximally entangled state, in the form $\rho = \alpha|\Phi\rangle\langle\Phi| + (1-\alpha)\mathbb{I}$, where $\mathbb{I}$ is the identity matrix, then we can find Nash Equilibria on the diagonal of the fair payoffs (i.e. $F_A = F_B$).

An interesting open question is therefore to examine if there exist more quantum Nash Equilibria, other than the fair one that we already found. Finally, it would also be interesting to study conflicting interest quantum games in a multiparty setting [103].

Chapter 6

Summary and Perspectives

6.1 Summary

This thesis aims to provide a practical approach to theoretical multiparty quantum cryptographic protocols and games. The new results can be summed up in three directions, each comprising of one of the three main chapters of the thesis:

1. A quantum coin flipping protocol is implemented over 15 and 25km of optical fiber using a commercial plug&play system. Extensive security proofs are given that incorporate all types of errors of the implementation and provide security against the most powerful adversaries.

2. A loss-tolerant entanglement verification protocol is proposed that remains secure in the presence of certain amounts of noise.

3. A two-player quantum game with conflicting interests is presented and implemented using an entangled photon source. The classical and quantum strategies are analysed and the quantum advantage is reported both from the theoretical analysis and from the experimental data.

6.2 Future Perspectives

We are currenlty trying to extend several of the results of this thesis. Concerning the quantum game proposed in Chapter 5, we are in the process of providing a more complete analysis of the classical and quantum Nash Equilibria of our game, and also examine in more detail the effects of losses and noise in the game.

Another research direction related to Chapter 4 that we are pursuing is the extention of our results in order to be able to verify more general entangled states, and particularly

graph states. We are also collaborating with the Quantum Optics Group of the University of Bristol, in order to experimentally demonstrate the entanglement verification results of the same Chapter. Using a entangled state that has distance $\epsilon = \sqrt{0.23 \pm 0.01}$ from the GHZ, and is produced using the experimental setup of [30], we are in the process of implementing both the basic and the enhanced verification protocols, and assert the advantages of the latter, given the losses and noise in the system.

More specifically, we will implement the experimental procedure described in Section 4.4.1 for $n = 3$ and $n = 4$. Preliminary data from the basic and the enhanced verification protocol on the 3-party state is available and can be summarised by the following figures:

- Figure 6.1 shows the results from Test 1, i.e. 3 honest parties that perform X and Y measurements on the $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ state.
- Figure 6.2 shows the results of Test 2, i.e. 4 parties, 3 honest and 1 dishonest, perform X and Y measurements on the $\frac{1}{2}(|000\rangle + |111\rangle)(|0\rangle + |1\rangle)$ state.
- Figure 6.3 shows the results from Test 3, i.e. 3 honest parties that perform "rotated" measurements on the $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ state.
- Figure 6.4 shows the results from Test 4, i.e. 4 parties, 3 honest and 1 dishonest, that perform "rotated" measurements on the $\frac{1}{2}(|000\rangle + |111\rangle)(|0\rangle + |1\rangle)$ state.

To better understand the experimental results, it is convenient to compare the figures that result from the data with the ones in Chapter 4, specifically Figure 6.2 with Figure 4.2 and Figure 6.4 with Figure 4.4. We can confirm that the upperbounds on the cheating probability given by the Theorems in Chapter 4 are verified by the experimental data.

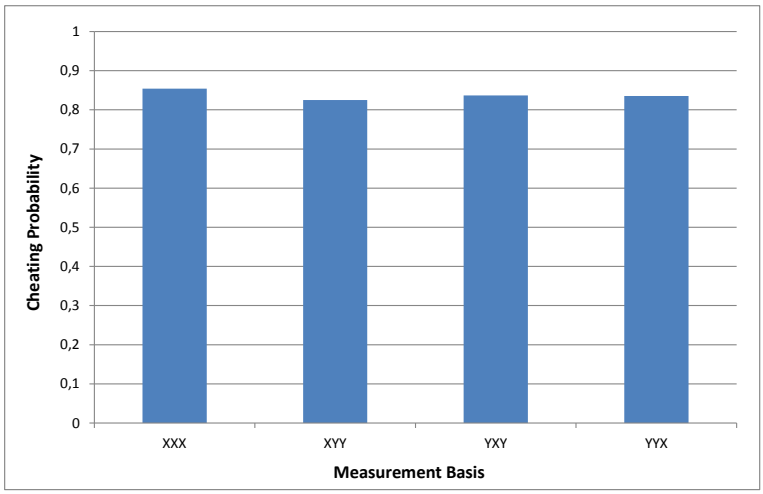


Figure 6.1: Basic Protocol for the all-honest case

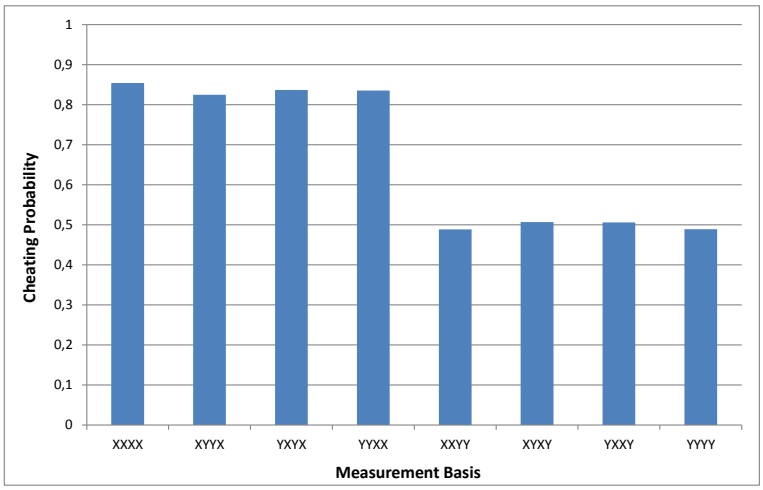


Figure 6.2: Basic Protocol for the 3 honest, 1 dishonest case

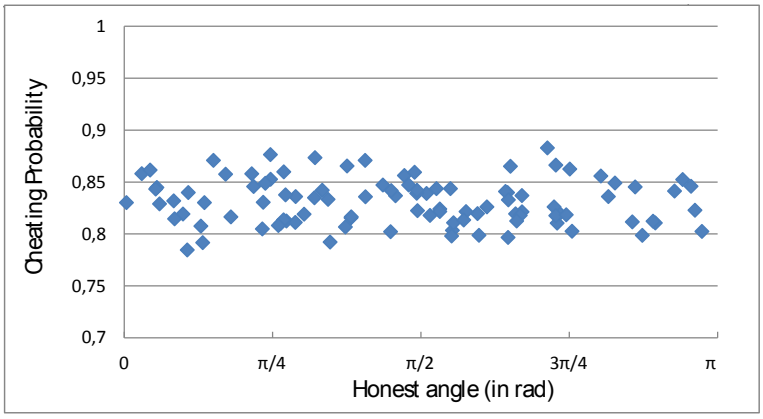


Figure 6.3: Enhanced Protocol for the all-honest case

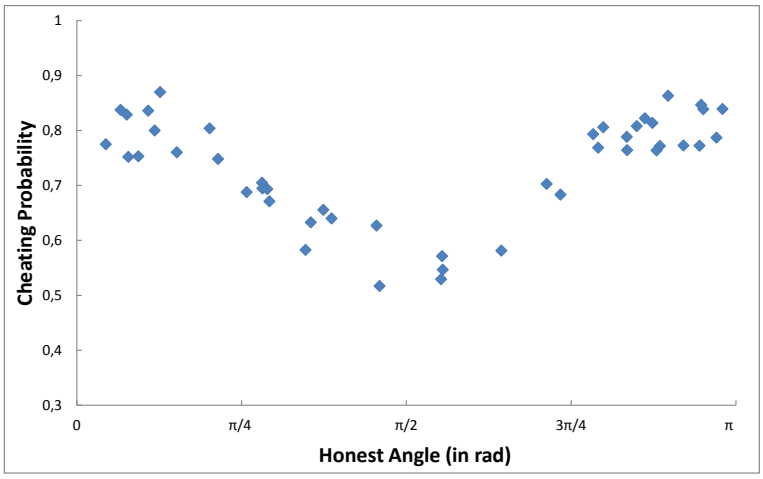


Figure 6.4: Enhanced Protocol for the 3 honest, 1 dishonest case

Finally, several results and techniques in this thesis could prove useful for the study of other cryptographic primitives. For example, it would be interesting to see if the Quantum Coin Flipping protocol proposed in Chapter 3 can be used to perform leader election, or if the techniques used to address the imperfections in the system can be used for other primitives like oblivious transfer.

Appendix A

Entanglement Verification

A.1 Security of the Enhanced Verification Protocol

A.1.1 Security in the Honest Model

Suppose all parties are honest and they want to verify that the state shared by the source is "close" to the GHZ state. We will prove the following theorem:

Theorem 8 (Honest Case). *Let $|\Psi\rangle$ be the state of all n parties. If $D(|\Psi\rangle, |G_0^n\rangle) = \epsilon$, then* $\Pr[T'(|\Psi\rangle) = 1] \leq 1 - \frac{\epsilon^2}{2}$.

Proof. We will start by defining a test in order to verify a rotated GHZ state:

$$|G_\Theta^n\rangle = \frac{1}{\sqrt{2}}\left(|0^n\rangle + e^{i\Theta}|1^n\rangle\right)$$

where $\Theta \in [0, 2\pi)$. Here, the promise on the inputs θ_j of the parties is the following:

$$\sum_{j=1}^{n} \theta_j \equiv \Theta \pmod{\pi} \tag{A.1}$$

We want to find an appropriate verification test that always outputs 1, when testing the correct state the $|G_\Theta^n\rangle$. We propose the test:

$$\bigoplus_{j=1}^{n} y_j = \frac{\sum_{j=1}^{n} \theta_j - \Theta}{\pi} \pmod{2} \tag{A.2}$$

Similar to Section 4.3.2, from the promise A.1, we have two cases:

- $\sum_{j=1}^{n} \theta_j \equiv \Theta \pmod{2\pi}$. The state after the parties' transformations, and before the measurements, is the equal superposition of all bistrings with an even number of 1's, so the exclusive or of their measurement outputs, is equal to 0.
- $\sum_{j=1}^{n} \theta_j \equiv \Theta + \pi \pmod{2\pi}$. The state after the parties' transformations, and before the measurements, is the equal superposition of all bistrings with an odd number of 1's, so the exclusive or of their measurement outputs, is equal to 1.

It is therefore true that the test A.2 is always true for the state $|G_\Theta^n\rangle$.

We now consider the measurement that the parties are doing on a state $|\Psi\rangle$ in the most general form, that of a POVM. Let $\{P_\Theta^n, \mathbb{I}_n - P_\Theta^n\}$ be the elements of the POVM that correspond to the test A.2, where the first element denotes success of the test, $T'(|\Psi\rangle) = 1$, and the second reject, $T'(|\Psi\rangle) = 0$. We will prove by induction that:

$$P_\Theta^n = |G_\Theta^n\rangle\langle G_\Theta^n| + \frac{1}{2} I_\Theta^n$$

where I_Θ^n is the projection on the space orthogonal to $|G_\Theta^n\rangle$ and $|G_{\Theta+\pi}^n\rangle$.

For n=1 we have that $P_\Theta^1 = |G_{\theta_1}^1\rangle\langle G_{\theta_1}^1|$ so the statement holds. We assume it is true for n parties and we will show the statement for $n+1$.

Let $\{P_\Theta^{n+1}(\theta_1), \mathbb{I}_{n+1} - P_\Theta^{n+1}(\theta_1)\}$ be the POVM that corresponds to the test for a given angle θ_1 of party A_1. There are two cases where the $n+1$ parties pass the test:

1. Party A_1 outputs $y_1 = 0$, meaning that the outcome of the measurement is $|G_{\theta_1}^1\rangle\langle G_{\theta_1}^1|$. Then the remaining n parties need to pass the test:

$$\bigoplus_{j=2}^{n+1} y_j = \frac{\sum_{j=2}^{n+1} \theta_j - (\Theta - \theta_1)}{\pi} \pmod 2$$

2. Party A_1 outputs $y_1 = 1$, meaning that the outcome of the measurement is $|G_{\theta_1+\pi}^1\rangle\langle G_{\theta_1+\pi}^1|$. Then the remaining n parties need to pass the test:

$$\bigoplus_{j=2}^{n+1} y_j = \frac{\sum_{j=2}^{n+1} \theta_j - (\Theta - \theta_1 + \pi)}{\pi} \pmod 2$$

Let $\Theta_{\neg 1} \equiv \Theta - \theta_1 \pmod{2\pi}$. It is evident that the first test is equivalent to the positive element $P^n_{\Theta_{\neg 1}}$ of a POVM on state $|G^n_{\Theta_{\neg 1}}\rangle$ and the second to the positive element $P^n_{\Theta_{\neg 1}+\pi}$ of a POVM on state $|G^n_{\Theta_{\neg 1}+\pi}\rangle$. From the induction we know that:

$$\begin{aligned} P^n_{\Theta_{\neg 1}+\pi} &= |G^n_{\Theta_{\neg 1}+\pi}\rangle\langle G^n_{\Theta_{\neg 1}+\pi}| + \frac{1}{2} I^n_{\Theta_{\neg 1}} \\ &= |G^n_{\Theta_{\neg 1}+\pi}\rangle\langle G^n_{\Theta_{\neg 1}+\pi}| + |G^n_{\Theta_{\neg 1}}\rangle\langle G^n_{\Theta_{\neg 1}}| + I^n_{\Theta_{\neg 1}} - |G^n_{\Theta_{\neg 1}}\rangle\langle G^n_{\Theta_{\neg 1}}| - \frac{1}{2} I^n_{\Theta_{\neg 1}} \\ &= \mathbb{I}_n - P^n_{\Theta_{\neg 1}} \end{aligned} \tag{A.3}$$

For the test on $n+1$ parties to succeed, we therefore have for a given $\theta_1 \in [0, \pi)$:

$$\begin{aligned} P^{n+1}_{\Theta}(\theta_1) &= |G^1_{\theta_1}\rangle\langle G^1_{\theta_1}| \otimes P^n_{\Theta_{\neg 1}} + |G^1_{\theta_1+\pi}\rangle\langle G^1_{\theta_1+\pi}| \otimes (\mathbb{I}_n - P^n_{\Theta_{\neg 1}}) \\ &= |G^1_{\theta_1}\rangle\langle G^1_{\theta_1}| \otimes |G^n_{\Theta_{\neg 1}}\rangle\langle G^n_{\Theta_{\neg 1}}| + |G^1_{\theta_1+\pi}\rangle\langle G^1_{\theta_1+\pi}| \otimes |G^n_{\Theta_{\neg 1}+\pi}\rangle\langle G^n_{\Theta_{\neg 1}+\pi}| \\ &+ \frac{1}{2}\Big(|G^1_{\theta_1}\rangle\langle G^1_{\theta_1}| + |G^1_{\theta_1+\pi}\rangle\langle G^1_{\theta_1+\pi}|\Big) \otimes I^n_{\Theta_{\neg 1}} \end{aligned} \tag{A.4}$$

Now, since

$$|G^1_{\theta_1}\rangle\langle G^1_{\theta_1}| + |G^1_{\theta_1+\pi}\rangle\langle G^1_{\theta_1+\pi}| = \mathbb{I}_1$$

we need to find a way to express the remaining two tensor products in Eq. A.4. We know that:

$$|G^n_{\Theta}\rangle = \frac{1}{\sqrt{2}}\Big(|G_{\theta_1}\rangle|G_{\Theta_{\neg 1}}\rangle + |G_{\theta_1+\pi}\rangle|G_{\Theta_{\neg 1}+\pi}\rangle\Big)$$

If we define, for a given $\Theta \in [0, 2\pi)$ and $a \in [0, \pi)$:

$$|\Phi^{n+1}_{a,\Theta}\rangle = \frac{1}{\sqrt{2}}\Big(|G^1_a\rangle|G^n_{\Theta-a}\rangle - |G^1_{a+\pi}\rangle|G^n_{\Theta-a+\pi}\rangle\Big)$$

we can check that the following holds:

$$|G^1_{\theta_1}\rangle\langle G^1_{\theta_1}| \otimes |G^n_{\Theta_{\neg 1}}\rangle\langle G^n_{\Theta_{\neg 1}}| + |G^1_{\theta_1+\pi}\rangle\langle G^1_{\theta_1+\pi}| \otimes |G^n_{\Theta_{\neg 1}+\pi}\rangle\langle G^n_{\Theta_{\neg 1}+\pi}| = |G^n_{\Theta}\rangle\langle G^n_{\Theta}| + |\Phi^{n+1}_{\theta_1,\Theta}\rangle\langle \Phi^{n+1}_{\theta_1,\Theta}|$$

and we finally have:

$$P^{n+1}_{\Theta}(\theta_1) = |G^n_{\Theta}\rangle\langle G^n_{\Theta}| + |\Phi^{n+1}_{\theta_1,\Theta}\rangle\langle \Phi^{n+1}_{\theta_1,\Theta}| + \frac{1}{2}\mathbb{I}_1 \otimes I^n_{\Theta_{\neg 1}}$$

In the same way, we define:

$$|\Psi^{n+1}_{a,\Theta}\rangle = \frac{1}{\sqrt{2}}\big(|G^1_a\rangle|G^n_{\Theta-a+\pi}\rangle - |G^1_{a+\pi}\rangle|G^n_{\Theta-a}\rangle\big)$$

and we can now express a projection on the $n+1$-dimensional Hilbert space:

$$\begin{aligned}
\mathbb{I}_{n+1} &= \mathbb{I}_1 \otimes \mathbb{I}_n \\
&= \Big(|G^1_{\theta_1}\rangle\langle G^1_{\theta_1}| + |G^1_{\theta_1+\pi}\rangle\langle G^1_{\theta_1+\pi}|\Big) \otimes \Big(|G^n_{\Theta_{\neg 1}}\rangle\langle G^n_{\Theta_{\neg 1}}| + |G^n_{\Theta_{\neg 1}+\pi}\rangle\langle G^1_{\Theta_{\neg 1}+\pi}| + I^n_{\Theta_{\neg 1}}\Big) \\
&= |G^n_\Theta\rangle\langle G^n_\Theta| + |G^n_{\Theta+\pi}\rangle\langle G^n_{\Theta+\pi}| + |\Phi^{n+1}_{\theta_1,\Theta}\rangle\langle\Phi^{n+1}_{\theta_1,\Theta}| + |\Psi^{n+1}_{\theta_1,\Theta}\rangle\langle\Psi^{n+1}_{\theta_1,\Theta}| + \mathbb{I}_1 \otimes I^n_{\Theta_{\neg 1}} \quad \text{(A.5)}
\end{aligned}$$

The newly defined states $|\Phi^{n+1}_{a,\Theta}\rangle$ and $|\Psi^{n+1}_{a,\Theta}\rangle$ are used to "complete" the Hilbert space. Now what is really interesting and will prove indispensable in completing our proof, is the following equation:

$$\begin{aligned}
|\Phi^{n+1}_{\theta_1+\frac{\pi}{2},\Theta}\rangle &= \frac{1}{\sqrt{2}}\big(|G^1_{\theta_1+\frac{\pi}{2}}\rangle|G^n_{\Theta_{\neg 1}-\frac{\pi}{2}}\rangle - |G^1_{\theta_1-\frac{\pi}{2}}\rangle|G^n_{\Theta_{\neg 1}+\frac{\pi}{2}}\rangle\big) \\
&= \frac{i}{\sqrt{2}}\big(e^{i\theta_1}|1\rangle|0^n\rangle - e^{i\Theta_{\neg 1}}|0\rangle|1^n\rangle\big) \\
&= i|\Psi^{n+1}_{\theta_1,\Theta}\rangle
\end{aligned}$$

because this means that $|\Phi^{n+1}_{\theta_1+\frac{\pi}{2},\Theta}\rangle\langle\Phi^{n+1}_{\theta_1+\frac{\pi}{2},\Theta}| = |\Psi^{n+1}_{\theta_1,\Theta}\rangle\langle\Psi^{n+1}_{\theta_1,\Theta}|$, and from Eq. A.5 we have that:

$$I^{n+1}_\Theta = |\Phi^{n+1}_{\theta_1,\Theta}\rangle\langle\Phi^{n+1}_{\theta_1,\Theta}| + |\Phi^{n+1}_{\theta_1+\frac{\pi}{2},\Theta}\rangle\langle\Phi^{n+1}_{\theta_1+\frac{\pi}{2},\Theta}| + \mathbb{I}_1 \otimes I^n_{\Theta_{\neg 1}} \quad \text{(A.6)}$$

where as before I^{n+1}_Θ is the projection on the space orthogonal to $|G^{n+1}_\Theta\rangle$ and $|G^{n+1}_{\Theta+\pi}\rangle$.

Since angle θ_1 is chosen uniformely at random in $[0,\pi)$, we have that:

$$
\begin{aligned}
P_{\Theta}^{n+1} &= \frac{1}{\pi}\int_0^{\pi} P_{\Theta}^{n+1}(\theta_1)d\theta_1 \\
&= \frac{1}{\pi}\int_0^{\pi/2}\Big[P_{\Theta}^{n+1}(\theta_1)+P_{\Theta}^{n+1}(\theta_1+\frac{\pi}{2})\Big]d\theta_1 \\
&= \frac{1}{\pi}\int_0^{\pi/2}\Big[2\times|G_{\Theta}^{n+1}\rangle\langle G_{\Theta}^{n+1}|+|\Phi_{\theta_1,\Theta}^{n+1}\rangle\langle\Phi_{\theta_1,\Theta}^{n+1}|+|\Phi_{\theta_1+\frac{\pi}{2},\Theta}^{n+1}\rangle\langle\Phi_{\theta_1+\frac{\pi}{2},\Theta}^{n+1}|+\mathbb{I}_1\otimes I_{\Theta_{\neg 1}}^{n}\Big]d\theta_1 \\
&= |G_{\Theta}^{n+1}\rangle\langle G_{\Theta}^{n+1}|+\frac{1}{2}I_{\Theta}^{n+1}
\end{aligned}
$$

For $\Theta = 0 \pmod{2\pi}$, we can infer the basic argument that leads to the proof of Theorem 10, namely that our test T' is equivalent to performing the POVM $\{P_0^n, \mathbb{I}_n - P_0^n\}$.

□

A.1.2 Security in the Dishonest Model

Theorem 9 (Dishonest Case)**.** *Let $|\Psi\rangle$ be the state of all n parties. If $\min_U D\big((I\otimes U)|\Psi\rangle, |G_0^n\rangle\big) = \epsilon$, where U is an operator on the space of the dishonest parties, then $\Pr[T'(|\Psi\rangle)=1] \leq 1-\frac{\epsilon^2}{4}$.*

Proof. Suppose, without loss of generality, the state that is shared by the source is:

$$
|\Psi\rangle = |G_h^k\rangle|\Psi_h\rangle + |G_{h+\pi}^k\rangle|\Psi_{h+\pi}\rangle + |\mathcal{X}\rangle \tag{A.7}
$$

where $|G_a^k\rangle = \frac{1}{\sqrt{2}}\big(|0\rangle^k + e^{ia}|1\rangle^k\big)$, $k = |\mathcal{H}|$ is the number of honest parties and $h = \sum_{j\in\mathcal{H}}\theta_j \pmod{\pi}$ is the input of all parties in $\mathcal{H}$, known to the dishonest set. States $|\Psi_h\rangle$ and $|\Psi_{h+\pi}\rangle$ are unormalised and $|\mathcal{X}\rangle$ is an arbitrary state whose "honest" part is orthogonal to $|G_h^k\rangle$ and $|G_{h+\pi}^k\rangle$.

The dishonest parties want to know in which of the two states $|G_h^k\rangle$ and $|G_{h+\pi}^k\rangle$ the honest share will collapse in after the measurement, and by consequence what will be the honest output $Y_{\mathcal{H}} = \sum_{j\in\mathcal{H}} y_j \pmod 2$. They will perform a Helstrom measurement on their share in order to distinguish between $|\Psi_h\rangle$ and $|\Psi_{h+\pi}\rangle$. This measurement is optimal and gives the following bound:

$$
\Pr[\text{guess } Y_H|h] = \frac{1}{2}+\frac{1}{2}\Big\||\Psi_h\rangle\langle\Psi_h| - |\Psi_{h+\pi}\rangle\langle\Psi_{h+\pi}|\Big\|_1
$$

To compute the above norm, we make use of a known property, that the trace norm of a density matrix is equal to the sum of the absolut values of its eigenvalues. After some simple calculations[1] we can verify that the above probability is equal to:

$$\begin{aligned}\Pr[\text{guess } Y_H|h] &= \frac{1}{2} + \frac{1}{2}\sqrt{\left(\||\Psi_h\rangle\|^2 + \||\Psi_{h+\pi}\rangle\|^2\right)^2 - 4|\langle\Psi_h|\Psi_{h+\pi}\rangle|^2} \\ &\leq \frac{1}{2} + \frac{1}{2}\left(\frac{\left(\||\Psi_h\rangle\|^2 + \||\Psi_{h+\pi}\rangle\|^2\right)^2 - 4|\langle\Psi_h|\Psi_{h+\pi}\rangle|^2 + 1}{2}\right) \\ &= 1 - \frac{1}{4}\left(1 - \left(\||\Psi_h\rangle\|^2 + \||\Psi_{h+\pi}\rangle\|^2\right)^2 + 4|\langle\Psi_h|\Psi_{h+\pi}\rangle|^2\right) \end{aligned} \tag{A.8}$$

We now do a Schmidt decomposition of $|G_h^k\rangle|\Psi_h\rangle + |G_{h+\pi}^k\rangle|\Psi_{h+\pi}\rangle$:

$$|G_h^k\rangle|\Psi_h\rangle + |G_{h+\pi}^k\rangle|\Psi_{h+\pi}\rangle = |A_h^0\rangle|B_h^0\rangle + |A_h^1\rangle|B_h^1\rangle \tag{A.9}$$

where $\langle A_h^0|A_h^1\rangle = \langle B_h^0|B_h^1\rangle = 0$. We use the following normalization: $\||A_h^0\rangle\|^2 = \||A_h^1\rangle\|^2 = 1$, $\||B_h^0\rangle\|^2 = p$, $\||B_h^1\rangle\|^2 = q$[2]. We can then write:

$$|A_h^0\rangle = z_0|G_h^k\rangle + z_1|G_{h+\pi}^k\rangle \quad \text{and} \quad |A_h^1\rangle = z_1^*|G_h^k\rangle - z_0^*|G_{h+\pi}^k\rangle$$

where $|z_0|^2 + |z_1|^2 = 1$, which gives us:

$$\begin{aligned} &|A_h^0\rangle|B_h^0\rangle + |A_h^1\rangle|B_h^1\rangle \\ &= (z_0|G_h^k\rangle + z_1|G_{h+\pi}^k\rangle)|B_0\rangle + (z_1^*|G_h^k\rangle - z_0^*|G_{h+\pi}^k\rangle)|B_1\rangle \\ &= |G_h^k\rangle(z_0|B_h^0\rangle + z_1^*|B_h^1\rangle) + |G_{h+\pi}^k\rangle(z_1|B_h^0\rangle - z_0^*|B_h^1\rangle) \end{aligned}$$

and from Eq. A.9 we have:

$$\begin{aligned} |\Psi_h\rangle &= z_0|B_h^0\rangle + z_1^*|B_h^1\rangle \\ |\Psi_{h+\pi}\rangle &= z_1|B_h^0\rangle - z_0^*|B_h^1\rangle \end{aligned}$$

Since $|A_h^0\rangle$ and $|A_h^1\rangle$ are on the same subspace as $|G_h^k\rangle$ and $|G_{h+\pi}^k\rangle$, they are also of the

[1] It suffices to notice that the term under the root is non-negative, and that it can be upperbounded by itself plus 1, divided by 2.

[2] Here p and q depend on the honest input h, but we do not use an index for ease of use. The same holds for other parameters, like z_0 and z_1, further down in this proof, since we consider that for any fixed h, there always exist such parameters, so again we will omit the index h.

following form:

$$|A_h^0\rangle = x|0^k\rangle + y|1^k\rangle \quad \text{and} \quad |A_h^1\rangle = y^*|0^k\rangle - x|1^k\rangle$$

where $x^2 + |y|^2 = 1$ (we can assume that $x \in \mathbb{R}$ for up to a global phase on $|A_0\rangle$ and $|A_1\rangle$). Then:

$$|z_0|^2 = |\langle A_h^0|G_k^h\rangle|^2 = \frac{1}{2}|x + ye^{ih}|^2$$

and since $y \in \mathcal{C}$, we rewrite $y = |y|e^{i\alpha}$ and get:

$$|z_0|^2 = \frac{1}{2}\left|x + |y|e^{ih+\alpha}\right|^2 = \frac{1}{2}(1 + 2x|y|\cos(h+\alpha))$$

Using $|z_0|^2 + |z_1|^2 = 1$, we have $|z_1|^2 = \frac{1}{2}(1 - 2x|y|\cos(h+\alpha))$. Also, from $x^2, |y|^2 \geq 0$ and $x^2 + |y|^2 = 1$, we have that $x^2|y|^2 \leq 1/4$. This gives us:

$$\begin{aligned} |\langle\Psi_h|\Psi_{h+\pi}\rangle|^2 &= (p-q)^2|z_0|^2|z_1|^2 = (p-q)^2\frac{1}{4}(1 - 4x^2|y|^2\cos^2(h+\alpha)) \\ &\geq (p-q)^2\frac{1}{4}(1 - \cos^2(h+\alpha)) = (p-q)^2\frac{1}{4}\sin^2(h+\alpha) \end{aligned} \tag{A.10}$$

We can finally revisit Eq. A.8:

$$\Pr[\text{guess } Y_{\mathcal{H}}|h] \leq 1 - \frac{1}{4}\big(1 - (p+q)^2 + (p-q)^2 sin^2(h+\alpha)\big) \tag{A.11}$$

In general, the dishonest parties can perform a local operation on their state, in order to maximize their cheating probability. Thus, the distance of the dishonest state from the correct one is : $\epsilon = min_U D((\mathbb{I}\otimes U)|\Psi\rangle, |G_0^n\rangle) = min_U \sqrt{1 - F^2((\mathbb{I}\otimes U)|\Psi\rangle, |G_0^n\rangle)}$, where by $F(|\psi\rangle, |\phi\rangle)$ we denote the fidelity between two states $|\psi\rangle$ and $|\phi\rangle$. If the reduced density matrices of the honest parties of the perfect and the real state are $\sigma_{\mathcal{H}}$ and $\rho_{\mathcal{H}}$ respectively, it holds that there exists a local operation R on the dishonest state such that:

$$F((\mathbb{I}\otimes R)|\Psi\rangle, |G_0^n\rangle) = F(\sigma_{\mathcal{H}}, \rho_{\mathcal{H}})$$

By applying this operation R, the distance is minimized:

$$\epsilon^2 = 1 - F^2((\mathbb{I} \otimes R)|\Psi\rangle, |G_0^n\rangle) = 1 - F^2(\sigma_{\mathcal{H}}, \rho_{\mathcal{H}})$$

Let us decompose $|G_0^n\rangle$ in the same orthonormal bases for the honest parties, as we did for $|\Psi\rangle$. We have $|G_0^n\rangle = |A_h^0\rangle|C^0\rangle + |A_h^1\rangle|C^1\rangle$. Then:

$$\sigma_{\mathcal{H}} = \frac{1}{2}\big(|A_h^0\rangle\langle A_h^0| + |A_h^1\rangle\langle A_h^1|\big)$$
$$\rho_{\mathcal{H}} = p|A_h^0\rangle\langle A_h^0| + q|A_h^1\rangle\langle A_h^1| + \mathrm{tr}_D|\mathcal{X}\rangle$$

and $F^2(\sigma_{\mathcal{H}}, \rho_{\mathcal{H}}) = \frac{1}{2}(\sqrt{p} + \sqrt{q})^2$, which gives:

$$\begin{aligned} \epsilon^2 &= 1 - \frac{p+q}{2} - \sqrt{pq} \leq 1 - \frac{(p+q)^2}{2} - 2pq \\ &= 1 - (p+q)^2 + \frac{(p-q)^2}{2} \end{aligned}$$

because $(p+q)^2 \leq (p+q)$ for $p+q \leq 1$ and $2pq \leq \sqrt{pq}$. Let us note here that whatever decomposition we do to the state $|\Psi\rangle$, the sum $(p+q)$ (where p and q are different and depend on the is a constant that always equals $\||\Psi_h\rangle\|^2 + \||\Psi_{h+\pi}\rangle\|^2$ for all h. It follows that $(p-q)^2$ is lowerbounded by the constant $2(\epsilon^2 - 1 + (p+q)^2)$. Since h is chosen uniformely at random, we have that:

$$\begin{aligned} \Pr[\text{guess } Y_{\mathcal{H}}] &= \frac{1}{\pi}\int_0^{\pi} \Pr[\text{guess } Y_{\mathcal{H}}|h]dh \\ &\leq 1 - \frac{1}{4}\Big(1 - (p+q)^2 + \frac{1}{\pi}\int_0^{\pi}(p-q)^2\sin^2(h+\alpha)dh\Big) \\ &\leq 1 - \frac{1}{4}\Big(1 - (p+q)^2 + \epsilon^2 - 1 + (p+q)^2\Big) \\ &\leq 1 - \frac{\epsilon^2}{4} \end{aligned}$$

and this concludes our proof.

□

Bibliography

[1] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.*, 47:777–780, 1935.

[2] John Steward Bell. On the einstein-podolsky-rosen paradox. *Physics*, 1(195), 1964.

[3] Alain Aspect, Philippe Grangier, and Gérard Roger. Experimental realization of einstein-podolsky-rosen-bohm *Gedankenexperiment*: A new violation of bell's inequalities. *Phys. Rev. Lett.*, 49:91–94, 1982.

[4] Stephen Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, 1983.

[5] C. H. Bennett and G. Brassard. *in* Proceeding of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, , page 175, IEEE, New York, 1984.

[6] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, 41:303–332, 1999.

[7] A. R. Dixon, Z. L. Yuan, J. F. Dynes, A. W. Sharpe, and A. J. Shields. Gigahertz decoy quantum key distribution with 1 mbit/s secure key rate. *Opt. Express*, 16 (23):18790–18979, 2008.

[8] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, 2009.

[9] Oded Goldreich. *Foundations of Cryptography, volume I, Basic Tools*. Cambridge University Press, 2003.

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

[11] H.-K. Lo and H. F Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. Physica D, 120:177–187, 1998.

[12] http://www.idquantique.com.

[13] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden. Quantum key distribution over 67 km with a plug&play system. *New J. Phys.*, 4:41, 2002.

[14] Guido Berlin, Gilles Brassard, Felix Bussières, and Nicolas Godbout. Fair loss-tolerant quantum coin flipping. *Phys. Rev. A*, 80:062321, 2009.

[15] Guido Berlin, Gilles Brassard, Felix Bussières, Nicolas Godbout, Joshua Slater, and Wolfgang Tittel. Experimental loss-tolerant quantum coin flipping. *Nature Communications*, 2:561, 2011.

[16] Esther Hänggi and Jurg Wüllschleger. Tight bounds for classical and quantum coin flipping. In *Proceedings of the 8th Theory of Cryptography Conference*, volume 6597, Springer, 2011.

[17] Daniel M. Greenberger, Michael A. Horne, and Anton Zeilinger. Going beyond bell's theorem. In *Bell's Theorem, Quantum Theory, and Conceptions of the Universe, M. Kafatos (Ed.), Kluwer, Dordrecht*, pages 69–72, 1989.

[18] N. David Mermin. Extreme quantum entanglement in a superposition of macroscopically distinct states. *Phys. Rev. Lett.*, 65:1838–1840, 1990.

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

[20] Robert Raussendorf and Hans J. Briegel. A one-way quantum computer. *Phys. Rev. Lett.*, 86:5188–5191, 2001.

[21] Gilles Brassard, Anne Broadbent, and Alain Tapp. Multi party pseudo-telepathy. In *Proceedings of the 8th International Workshop on Algorithms and Data Structures*, volume 2748, pages 1–11, 2003.

[22] Jens Eisert, Martin Wilkens, and Maciej Lewenstein. Quantum games and quantum strategies. *Phys. Rev. Lett.*, 83:3077–3080, 1999.

[23] Shengyu Zhang. Quantum strategic game theory. *Quantum Information Processing (QIP 2011)*, Preprint at http://arxiv.org/abs/1012.5141.

[24] John C. Harsanyi. Games with incomplete information played by bayesian players, i-iii. *Management Science 14 (3): 159-183 (Part I), 14 (5): 320-334 (Part II), 14 (7): 486-502 (Part III)*, 1967/1968.

[25] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed experiment to test local hidden-variable theories. *Phys. Rev. Lett.*, 23:880–884, 1969.

[26] Nicolas Brunner and Noah Linden. Connection between bell nonlocality and bayesian game theory. *Nature Communications*, 4:2057, 2013.

[27] Martin J. Osborne. *An Introduction to Game Theory*. Oxford University Press, 2003.

[28] R. Cleve, P. Hoyer, B. Toner, and J. Watrous. Consequences and limits of nonlocal strategies. In *Proceedings of the 19th IEEE Annual Conference on Computational Complexity*, pages 236–249, 2004.

[29] http://www.qutools.com.

[30] B. A. Bell, M. S. Tame, A. S. Clark, R. W. Nock, W. J. Wadsworth, and J. G. Rarity. Experimental characterization of universal one-way quantum computing. *New Journal of Physics*, 15:053030, 2013.

[31] A. Pappa, A. Chailloux, E. Diamanti, and I. Kerenidis. Practical quantum coin flipping. *Phys. Rev. A*, 84:052305, 2011.

[32] A. Pappa, A. Chailloux, S. Wehner, E. Diamanti, and I. Kerenidis. Multipartite entanglement verification resistant against dishonest parties. *Phys. Rev. Lett.*, 108: 260502, 2012.

[33] A. Pappa, P. Jouguet, T. Lawson, A. Chailloux, M. Legré, P. Trinkler, I. Kerenidis, and E. Diamanti. Experimental plug and play quantum coin flipping. *Nature Communications*, 5:3717, 2014.

[34] M.A. Nielsen and I.L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.

[35] John Watrous. *Theory of Quantum Computation*. Lecture Notes, 2011. URL https://cs.uwaterloo.ca/~watrous/CS766/LectureNotes/all.pdf.

[36] Boris S. Cirel'son. Quantum generalizations of bell's inequality. *Letters in Mathematical Physics*, 4:93–100, 1980.

[37] Mark Hillery, Vladimír Bužek, and André Berthiaume. Quantum secret sharing. *Phys. Rev. A*, 59:1829–1834, 1999.

[38] David N. Mermin. Quantum mysteries revisited. *American Journal of Physics*, 58 (8):731, 1990.

[39] Elham Kashefi and Iordanis Kerenidis. Statistical zero knowledge and quantum one-way functions. *Theoretical Computer Science*, 378:101–116, 2007.

[40] A. Chailloux and I. Kerenidis. Optimal bounds for quantum bit commitment. In *Proceedings of 52nd IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 354–362, 2011.

[41] Dorit Aharonov, Amnon Ta-Shma, Umesh Vazirani, and Andrew Yao. Quantum bit escrow. In *STOC 2000, The 32nd Annual ACM Symposium on Theory of Computing, Portland, OR, USA*, pages 705–714, 2000.

[42] Dirk Bouwmeester, Artur K. Ekert, and Anton Zeilinger (Eds.). *The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation*. Springer-Verlag, 2000.

[43] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin. Plug and play" systems for quantum cryptography. *Applied Physics Letters*, 1997.

[44] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81 (3):1301, 2009.

[45] Manuel Blum. Coin flipping by telephone: a protocol for solving impossible problems. In *Advances in Cryptology; a Report on CRYPTO'81*, pages 11–15, Santa Barbara, California, USA, 1981.

[46] Adrian Kent. Coin tossing is strictly weaker than bit commitment. *Phys. Rev. Lett.*, 83:5382–5384, 1999.

[47] Andris Ambainis. A new protocol and lower bounds for quantum coin flipping. *J. Comput. Syst. Sci.*, 68:398–416, 2004.

[48] Robert Spekkens and Terry Rudolph. Quantum protocol for cheat-sensitive weak coin flipping. *Phys. Rev. Lett.*, 89(22):1–4, 2002.

[49] Roger Colbeck. An entanglement-based protocol for strong coin tossing with bias 1/4. Phys. Rev. A, 362(5-6):390–392, 2007.

[50] Ashwin Nayak and Peter Shor. Bit-commitment-based quantum coin flipping. *Phys. Rev. A*, 67(1):012304, 2003.

[51] Alexei Kitaev. Quantum coin-flipping. *Quantum Information Processing (QIP 2003) MSRI, Berkeley, CA, 1317 Dec 2002*, unpublished.

[52] André Chailloux and Iordanis Kerenidis. Optimal quantum strong coin flipping. In *50th Annual Symposium on Foundations of Computer Science, FOCS 2009, October 25-27, 2009, Atlanta*, IEEE Computer Society, 2009.

[53] Carlos Mochon. Quantum weak coin-flipping with bias of 0.192. In *Proceedings of the 45th Annual IEEE Symposium on Foundations of Computer Science (FOCS04), Washington DC, 2004*, pages 2–11, IEEE, Piscataway, NJ, 2004.

[54] Dorit Aharonov, André Chailloux, Maor Ganz, Iordanis Kerenidis, and Loïck Magnin. A simpler proof of existence of quantum weak coin flipping with arbitrarily small bias. Preprint at http://arxiv.org/abs/1402.7166 (2014).

[55] Gilles Brassard, Norbert Lütkenhaus, Tal Mor, and Barry Sanders. Limitations on practical quantum cryptography. *Phys. Rev. Lett.*, 85(5):1330–1333, 2000.

[56] André Chailloux. Improved loss-tolerant quantum coin flipping. In *AQIS*, 2010.

[57] N. Aharon, S. Massar, and J. Silman. A family of loss-tolerant quantum coin flipping protocols. Phys. Rev. A, 82:052307, 2010.

[58] Adrian Kent. Large n quantum cryptography. In *Proceedings of the 6th International Conference on Quantum Communication, Measurement and Computing, QCMC02, 2002*, Rinton Press Inc, 2003.

[59] Jonathan Barrett and Serge Massar. Quantum coin tossing and bit-string generation in the presence of noise. Phys. Rev. A, 69:022322, 2004.

[60] L. P. Lamoureux, E. Brainis, D. Amans, J. Barrett, and S. Massar. Provably secure experimental quantum bit-string generation. *Phys. Rev. Lett.*, 94:050503, Feb 2005.

[61] G. Molina-Terriza, A. Vaziri, R. Ursin, and A. Zeilinger. Experimental quantum coin tossing. *Phys. Rev. Lett.*, 94:040501, 2005.

[62] A. T. Nguyen, J. Frison, K. Phan Huy, and S. Massar. Experimental quantum tossing of a single coin. *New J. Phys.*, 10:083087, 2008.

[63] Nelly Huei Ying Ng, Siddarth K. Joshi, Chia Chen Ming, Christian Kurtsiefer, and Stephanie Wehner. Experimental implementation of bit commitment in the noisy storage model. *Nature Communications*, 3:1326, 2012.

[64] C. Erven, N. Ng, N. Gigov, R. Laflamme, S. Wehner, and G. Weihs. An experimental implementation of oblivious transfer in the noisy storage model. *preprint arXiv:1308.5098*, 2013.

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

[66] Robert Spekkens and Terry Rudolph. Optimization of coherent attacks in generalizations of the bb84 quantum bit commitment protocol. *Quantum Information and Computation*, 2(1):66–96, 2002.

[67] S. Wehner, M. Curty, C. Schaffner, and H.-K. Lo. Implementation of two-party protocols in the noisy-storage model. *Phys. Rev. A*, 81:052336, 2010.

[68] Chandra M. Natarajan, Michael G. Tanner, and Robert H. Hadfield. Superconducting nanowire single-photon detectors: physics and applications. *Superconductor Science and Technology*, 25:063001, 2012.

[69] Stephanie Wehner, Christian Schaffner, and Barbara Terhal. Cryptography from noisy storage. *Phys. Rev. Lett.*, 100:220502, 2008.

[70] Carlos Mochon. Quantum weak coin flipping with arbitrarily small bias. Preprint at http://arxiv.org/abs/0711.4114 (2007).

[71] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. Decoy state quantum key distribution. *Phys. Rev. Lett.*, 94:230504, Jun 2005.

[72] Xiang-Bin Wang. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.*, 94:230503, Jun 2005.

[73] Yi Zhao, Bing Qi, Xiongfeng Ma, Hoi-Kwong Lo, and Li Qian. Experimental quantum key distribution with decoy states. *Phys. Rev. Lett.*, 96:070502, 2006.

[74] Chi-Hang Fred Fung, Bing Qi, Kiyoshi Tamaki, and Hoi-Kwong Lo. Phase-remapping attack in practical quantum-key-distribution systems. *Phys. Rev. A*, 75: 032314, Mar 2007.

[75] Feihu Xu, Bing Qi, and Hoi-Kwong Lo. Experimental demonstration of phase-remapping attack in a practical quantum key distribution system. *New J. Phys.*, 12:113026, 2010.

[76] Vadim Makarov, Andrey Anisimov, and Johannes Skaar. Effects of detector efficiency mismatch on security of quantum cryptosystems. *Phys. Rev. A*, 74:022313, 2006.

[77] Bing Qi, Chi-Hang Fred Fung, Hoi-Kwong Lo, and Xiongfeng Ma. Time-shift attack in practical quantum cryptosystems. *Quantum Information and Computation*, 7: 73, 2007.

[78] Yi Zhao, Chi-Hang Fred Fung, Bing Qi, Christine Chen, and Hoi-Kwong Lo. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A*, 78:042333, 2008.

[79] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nature Photonics*, 4(10):686–689, 2010.

[80] Yi Zhao, Bing Qi, and Hoi-Kwong Lo. Experimental quantum key distribution with active phase randomization. *Appl. Phys. Lett.*, 90:044106, 2007.

[81] Yi Zhao, Bing Qi, Hoi-Kwong Lo, and L Qian. Security analysis of an untrusted source for quantum key distribution: passive approach. *New J. Phys.*, 12:023024, 2010.

[82] Yi Zhao, Bing Qi, and Hoi-Kwong Lo. Quantum key distribution with an unknown and untrusted source. *Phys. Rev. A*, 77:052327, 2008.

[83] Matthew McKague, Tzyh Haur Yang, and Valerio Scarani. Robust self-testing of the singlet. *J. Phys. A*, 45:455304, 2012.

[84] Cyril Branciard, Eric G. Cavalcanti, Stephen P. Walborn, Valerio Scarani, and Howard M. Wiseman. One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering. *Phys. Rev. A*, 85:010301, 2012.

[85] H. M. Wiseman, S. J. Jones, and A. C. Doherty. Steering, entanglement, nonlocality, and the einstein-podolsky-rosen paradox. *Phys. Rev. Lett.*, 98:140402, 2007.

[86] S. J. Jones, H. M. Wiseman, and A. C. Doherty. Entanglement, einstein-podolsky-rosen correlations, bell nonlocality, and steering. *Phys. Rev. A*, 76:052116, 2007.

[87] A. J. Bennet, D. A. Evans, D. J. Saunders, C. Branciard, E. G. Cavalcanti, H. M. Wiseman, and G. J. Pryde. Arbitrarily loss-tolerant einstein-podolsky-rosen steering allowing a demonstration over 1 km of optical fiber with no detection loophole. *Phys. Rev. X*, 2:031003, 2012.

[88] B. Wittmann, S. Ramelow, F. Steinlechner, N. K. Langford, N. Brunner, H. M. Wiseman, R. Ursin, and A. Zeilinger. Loophole-free einstein–podolsky–rosen experiment via quantum steering. *New Journal of Physics*, 14:053030, 2012.

[89] D. H. Smith, G. Gillett, M. P. de Almeida, C. Branciard, A. Fedrizzi, T. J. Weinhold, A. Lita, B. Calkins, T. Gerrits, S.-W. Nam, and A. White. Conclusive quantum steering with superconducting transition edge sensors. *Nature Communications*, 3:625, 2011.

[90] Anne Broadbent Gilles Brassard and Alain Tapp. Recasting mermin's multi-player game into the framework of pseudo-telepathy. *Quantum Information and Computation*, 5(7):538–550, 2005.

[91] Jean-Daniel Bancal, Nicolas Gisin, Yeong-Cherng Liang, and Stefano Pironio. Device-independent witnesses of genuine multipartite entanglement. *Phys. Rev. Lett.*, 106:250404, 2011.

[92] Matthew McKague. Self-testing graph states. Preprint at http://arxiv.org/abs/1010.1989 (2010).

[93] E. G. Cavalcanti, Q. Y. He, M. D. Reid, and H. M. Wiseman. Unified criteria for multipartite quantum nonlocality. *Phys. Rev. A*, 84:032115, 2011.

[94] Harry Buhrman, Wim van Dam, Peter Høyer, and Alain Tapp. Multiparty quantum communication complexity. *Physical Review A*, 60(4):2737, 1999.

[95] Carl Helstrom. Quantum detection and estimation theory. *J. Stat. Phys.*, 1:231, 1969.

[96] David Chaum, Claude Crépeau, and Ivan Damgård. Multiparty unconditionally secure protocols (extended abstract). In *Proceedings of the 20th Annual ACM Symposium on Theory of Computing (STOC)*, pages 11–19, 1988.

[97] M. Ben-Or, C. Crépeau, D. Gottesman, A. Hassidim, and A. Smith. Secure multiparty quantum computation with (only) a strict honest majority. In *Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS 2006)*, pages 249–260, 2006.

[98] John von Neumann and Oscar Morgenstern. *Theory of Games and Economic Behavior*. Princeton University Press, 1953.

[99] John F. Nash. Non-cooperative games. *The Annals of Mathematics*, 54:286–295, 1951.

[100] Miguel Navascues, Stefano Pironio, and Antonio Acin. Bounding the set of quantum correlations. *Phys. Rev. Lett.*, 98:010401, 2007.

[101] Miguel Navascues, Stefano Pironio, and Antonio Acin. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New J. Phys.*, 10:073013, 2008.

[102] Stefano Pironio, Miguel Navascues, and Antonio Acin. Convergent relaxations of polynomial optimization problems with non-commuting variables. *SIAM Journal on Optimization*, 20:2157, 2010.

[103] Simon C. Benjamin and Patrick M. Hayden. Multi-player quantum games. *Physical Review A*, 64(3):030301, 2001.