INDIVIDUAL ATTACK ANALYSIS OF DEVICE INDEPENDENT COUNTERFACTUAL QUANTUM KEY DISTRIBUTION

BY

SUHAILI BINTI KAMARUDDIN

A thesis submitted in fulfillment of the requirement for the degree of Doctor of Philosophy in Computational and Theoretical Sciences

Kulliyyah of Science
International Islamic University Malaysia

APRIL 2018

ABSTRACT

The study of quantum key distribution (QKD) which began in the early 80's has seen much fruition and development for almost three decades now. Ranging from security proofs and new protocols, quantum cryptography takes the limit of security definition to the most extreme especially in the context of device independent QKD. This is the scenario where even the equipment used by the legitimate parties cannot be trusted and is considered as black boxes i.e. the parties are assumed to have no knowledge of the device's full function. Further extreme is explored when the adversary, Eve is even seen to have access to physics beyond that of quantum mechanics; or commonly known as `supra-quantum' and violations of Bell inequalities become a necessary condition for security. Moving on to a recent development in a new type of protocol, namely counterfactual QKD (CQKD), quantum physics allows for the establishment of secure keys without a net transmission of signals between the legitimate parties; exploiting the single photon entanglement phenomena. We consider taking this new type of protocol to the extreme security requirements of device independence against a supra quantum Eve. We begin by exploring binary measurement based QKD with binary output within a device independent context in which we present the security analysis of the protocol against an individual attack by a supra-quantum adversary considering two different scenarios. The two scenarios involved in determining the maximal key rate are between the measurement that would maximizes the legitimate parties' correlations and those that would achieve maximal violation of Bell-type inequality. We show that higher correlation between shared raw keys at the expense of maximal Bell violation provide for better key rate for low channel disturbance. This naturally allows us to apply to the single photon entanglement QKD where we show that a non zero key rate is indeed possible. Finally, we show how, the counterfactual QKD protocol, as described in the original papers are not secure given a device independent scenario, let alone a supra-quantum adversary. Capitalizing on the results of the earlier chapters, we propose a possible framework for device independent CQKD against an individual attack by a supra-quantum Eve. We show how, at least, as an example of an equivalent protocol could provide for a secure key given a heuristic analysis within the device independent framework and how this can be used in a CQKD picture with a Bell check. We conclude the thesis with future outlooks on how the work could be developed for understanding not only in the field of quantum cryptography but also more fundamental issues in physics.

خلاصة البحث

شهدت دراسة الكمومية العمومية (QKD) التي بدأت في ثمانينيات القرن الماضي تطورا إيجابيا ملحوظاً خلال العقود الثلاثة الماضية، بدءً من تطبيقات وبراهين أمنية وبروتوكولات جديدة مدت مفهوم وتعريف نظام التشفير الكمي إلى أقصى الحدود، خاصة في سياق الجهاز العموميّ الكموميّ المستقل. هذا هو السناريوا حيث أن المعدات والجهات المستخدمة والمتاحة أو المتوفرة لا يمكن الوثوق بها وتم اعتبارها حاويات أو صناديق سوداء؛ أي يفترض أن الأطراف أو الجهات المستخدمة ليس لديهم معرفة وظيفة الجهاز الكاملة. وتم استكشاف المزيد من الطرف الأقصى حتى عند ما كان المقابل أو الخصم (Eve) موصولا بالفيزياء خارج أو وراء الميكانيكا الكم المعروف بشكل عام بسوبرا الكمومي، واصبحت انتهاكات عدم مساوات البل (Bell Inequality) حالة ضرورية للأمن. والانتقال إلى تطور حديث في نوع جديد من البروتوكول، وهي المغاير (كونتيرفاكتوالcounterfactual) في التعمية الكومية (CQKD)، يسمح الفيزياء الكمي لإنشاء مفاتيح آمنة دون انتقال كامل الإشارات بين الأطراف المتاحة أو المسموحة؛ حيث استغلال ظاهرة الفوتون ذات التشابك الواحد. واعتبر اتخاذ أو ايجاد هذا النوع الجديد من البروتوكول أحد متطلبات الأمن القصوى عند استقلال الجهاز مقابل أو ضد (supra-quantum). بدأ هذا البحث باستكشاف ثنائي القياس القائم على كد مع الانتاج الثنائي ضمن سياق الجهاز المستقل الذي نقدم تحليل أمني للبروتوكول مقابل أو ضد هجوم فردي من قبل الخصم، عدواني الكم، وذلك من خلال سيناريوهين مختلفين. وهناك سيناريوهان ينطويان على تحديد المعدل الرئيسي الأقصى بين القياس الذي من شأنه أن يزيد من ارتباطات الأطراف المتاحة أو المسموحة وتلك التي من شأنها تحقيق أقصى قدر من انتهاك عدم المساواة من نوع مبرهنة (Bell). وتبين لنا أن الارتباط العالي بين المفاتيح مواد الخام المشتركة على حساب الأقصى انتهاكاً ينص على أفضل مقياس رئيسي لاضطراب قناة منخفضة. وهذا بالطبع يسمح لنا أن نطبق على فوتون أحادي أو فردي التشابك في التعمية الكومية، حيث ظهر أن حصول معدل المفتاح غير صفر ممكن في الواقع. وأخيرا، تبين للباحث كيف، أن المغاير (counterfactual) في التعمية الكومية بروتوكول، كما هو موضح في الأوراق الأصلية، ليس آمناً، خاصة في سيناريو الجهاز المستقل، ناهيك عن نظام سوبرا الكمومي. بناء على نتائج الفصول السابقة، يقترح الباحث إطاراً ممكناً للجهاز المستقل CQKD مقابل الهجوم الفرادي بواسطة حواء سوبرا الكمومي. وتبين للباحث كيف يمكن أن توفر ما لا يقل عن مفاتيح آمنة بناء على تحليل الكشف عن مجريات الأمور في إطار مستقل الجهاز وكيف يمكن استخدامها في صورة CQKD مع التأكد من خلال جهاز (Bell). وانتهت الدراسة بتوقعات مستقبلية بشأن الكيفية التي يمكن بها تطوير العمل لفهم، ليس فقط في مجال التشفير الكم، ولكن أيضا في معظم القضايا الأساسية في علم الفيزياء.

APPROVAL PAGE

The thesis of Suhaili binti Kamaruddin has been approved by the following:

____
Jesni Shamsul Shaari
Supervisor

____
Mohamed Ridza Wahiddin
Internal Examiner

____
Hishamuddin Zainuddin
External Examiner

____
Suhairi Saharudin
External Examiner

____
Siti Zaiton Mat So’ad
Chairman

DECLARATION

I hereby declare that this thesis is the result of my own investigations, except where otherwise stated. I also declare that it has not been previously or concurrently submitted as a whole for any other degrees at IIUM or other institutions.

Suhaili binti Kamaruddin

Signature .... Date ....

INTERNATIONAL ISLAMIC UNIVERSITY MALAYSIA

DECLARATION OF COPYRIGHT AND AFFIRMATION OF FAIR USE OF UNPUBLISHED RESEARCH

INDIVIDUAL ATTACK ANALYSIS OF DEVICE INDEPENDENT COUNTERFACTUAL QUANTUM KEY DISTRIBUTION

I declare that the copyright holders of this thesis are jointly owned by the student and IIUM.

No part of this unpublished research may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without prior written permission of the copyright holder except as provided below

1. Any material contained in or derived from this unpublished research may be used by others in their writing with due acknowledgement.

2. IIUM or its library will have the right to make and transmit copies (print or electronic) for institutional and academic purposes.

3. The IIUM library will have the right to make, store in a retrieved system and supply copies of this unpublished research if requested by other universities and research libraries.

By signing this form, I acknowledged that I have read and understand the IIUM Intellectual Property Right and Commercialization policy.

Affirmed by Suhaili binti Kamaruddin

……..…………………….. ………………………..

Signature Date

ACKNOWLEDGEMENTS

In the name of Allah, the Most Gracious and the Most Merciful. Praise be to Allah for His will I managed to complete this thesis.

First of all, I would like to express my deepest gratitude to my one and only supervisor, Assoc. Prof. Dr. Jesni Shamsul Shaari for his guidance, word of encouragement and persistent help over the years of my Ph.D journey. Without his excellent supervision and astute feedback, the completion of this thesis would not have been possible.

I am also grateful to Piotr Kolenderski for his helpful discussions related to single photon entanglement mainly within the context of Mach-Zehnder interferometer.

My warmest thanks to my friends, Fazlyla Nadya Fadzlan, Sakina Nur Najah Abdul Jabar, Hafizah Bahaluddin, Nor Amirah Mohd Busul Aklan, Nur Zatul Akmar Hamzah, and Nor Azwa Zakaria, who provided me assistance and comfort in the time of distress.

I would also like to thank IIUM and Ministry of Education (MoE) for providing me financial support in pursuing Ph.D degree under the SLAB/SLAI fellowship scheme.

Finally, and most importantly, special thanks to my mother, Fatimah binti Masree, my husband, Mohd Khairi bin Sayadek, and all my family members for all the support, prayers and sacrifices, as I completed my Ph.D degree. I also want to dedicate this work to my late father, Kamaruddin bin Sulaiman who, in his lifetime, constantly reminded me the importance of knowledge and education.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

aPR box	anti-Popescu-Rohrlich box.
CQKD	Counterfactual quantum key distribution.
DI CQKD	Device independent counterfactual quantum key distribution.
DIQKD	Device independent quantum key distribution.
PR box	Popescu-Rohrlich box.
QKD	Quantum key distribution.
SDI	Single photon entanglement QKD.

LIST OF SYMBOLS

p_L	Probability of sending deterministic strategies.
p_{NL}	Probability of sending nonlocal strategies.
I_{AB}	Alice-Bob mutual information.
I_{AE}	Eve’s information of Alice’s bits.
I_{BE}	Eve’s information of Bob’s bits.
F	Fidelity of quantum states.
D	Disturbances in the quantum channel.

CHAPTER ONE

INTRODUCTION

1.1 INTRODUCTION

Confidentiality of information has been a major concern since ancient times, a concern that has given birth to a branch of study called cryptography. Examples from the ancient world includes the Caesar cipher used by Julius Caesar and the scytale used by the Spartans (Sergienko, 2005). Cryptography can be defined as the art of rendering a message unintelligible to any unauthorised party (Gisin, Ribordy, Tittel, & Zbinden, 2002). In order to achieve this, it is necessary for the communicating parties to use a cryptosystem to encrypt and decrypt their message along with a very important piece of information known as the key (Van Assche, 2006). Thus the invention and design of cryptosystems can in principle be based on the secrecy of the workings of a cryptosystem, or the secrecy of the key only, or both. Kerckhoffs principle however states that a good protocol only resides its secrecy entirely upon a key, while none rests in the knowledge of the cryptosystem (Schneier, 2007). Hence, it is assumed that the cryptosystem is always known by the adversary and only the key is to be kept secret.

It is well known that the security of cryptosystem can be divided into information-theoretic security and computational security (Menezes, van Oorschot, & Vanstone, 1996). If the security is based on the assumptions of the adversary's computational resources, then the cryptosystem is said to be computationally secure. This type of security relies on the difficulty of solving hard computational problem such as, factoring large integers or computing discrete logarithms. How `hard' or how `easy' a computational problem is, would be defined based on the amount of resources required to solve the problem; the main theme of the field of *computational complexity*. Given a problem with *n*-bit input, it is considered easy if the resources required to solve it is polynomial in *n* and hard otherwise. In contrast, a cryptosystem is said to be information-theoretic secure (or unconditionally secure) if there are no assumptions made on the adversary's computational power. Based on this stronger definition of security, Claude Shannon (1949) introduced the notion of *perfect secrecy*. *Perfect secrecy* means that an eavesdropper, conventionally known as Eve, would not gain any knowledge about the actual message from the ciphertext. For a cryptosystem to be considered perfectly secure, it has to fulfill three conditions: namely, the key cannot be reused, needs to be truly random and the key has to be as long as the message to be encrypted (Schneier, 2007).

Depending on the key used for encryption and decryption purposes, we can classify cryptosystems into two types of classes, that is, the symmetric-key and asymmetric-key cryptosystems.

Suppose that an encryption scheme consists of an encryption transformation $\{E_e : e \in K\}$ and its corresponding decryption transformation $\{D_d : d \in K\}$, in which K is the key space (Menezes et al., 1996). A symmetric-key cryptosystem is as such for each pair of key (e,d), the encryption key, e can be calculated from the decryption key, d and vice versa. In most symmetric algorithms, the encryption and decryption keys are the same, that is, $e = d$ hence the term symmetric-key (Schneier, 2007).

One of the most renowned example of a symmetric scheme is the one-time pad, which is invented and patented by Gilbert Vernam (1926). Shannon (1949) has proven that the security of one-time pad achieved perfect secrecy and in fact, it is the only scheme known today that achieves such level of security (Gisin et al., 2002). Let us recall that in order to ensure perfect secrecy, it is essential that the secret key has to be as long as the message itself and truly random. It is also required that the key is not to be used repetitively. These conditions, however, have become a major hurdle to one-time pad in practice due to the difficulty of key distribution between the legitimate parties (Menezes et al., 1996). A radical solution to circumvent such a problem was the invention of the asymmetric-key cryptosystem or more commonly known as public-key cryptosystem.

In contrast to symmetric-key cryptosystem, the public-key cryptosystem uses two different sets of key for encryption and decryption. To employ this scheme, one needs to create a private key that is only known to the user and its corresponding public key, which can be publicly known. The scheme works in such a way that a message can be encrypted by anyone using the public key and the encrypted message can only be decrypted by the corresponding private-key pair. The principle was first proposed by Diffie & Hellman (1976), while the actual implementation was first developed by Ronald Rivest, Adi Shamir, and Leonard Adleman in 1978 (Rivest, Shamir, & Adleman, 1978) which is widely known as RSA. This scheme did manage to avoid the key distribution problem that exist in symmetric-key cryptosystem, though unfortunately its security relies on unproven assumptions of computational complexity which is at the risk of being compromised in a near future.

While the search for efficient algorithms to factor large numbers into primes has, in the field of mathematics not seen much breakthrough, thus providing further support (not proof) for security based on computational complexity, the emergence of the field of quantum computation has brought this comfort to question. Quantum computation, a research field where quantum properties of nature are used to solve computational problems have brought about many advances including the famous `Shor's algorithm' (Shor, 1994). The algorithm has been demonstrated to be able to factor large numbers into prime factors in a much more efficient way with the use of quantum computers. Despite the fact that the latter may be seen as an ambitious enterprise, a solid research program has been built around it and to date, fears of the collapse of classical cryptosytstems may well be founded. This is especially so given emerging technologies in the direction of quantum computers, as an example the D-Wave.

A possible solution to this problem would be to implement quantum key distribution (QKD) protocol. A QKD protocol involves the transmission of information using quantum signal between two distant parties in order to establish secret keys in the presence of an eavesdropper. In principle, QKD protocol offers unconditional security in the face of an eavesdropper with unlimited computing power as it relies on the fundamental laws of physics as oppose to public-key cryptosystem which is based on the assumptions of computational complexity. Any attempt to glean information about the system in a QKD protocol by an eavesdropper, Eve results in inducing errors in the communication channel. This not only alerts the legitimate users with regards to the presence of an intruding malicious party but more importantly present a way to determine her information gain to ascertain how one could distill a secret key thereof through classical procedures of error correction and privacy amplification.

1.2 QUANTUM INFORMATION BASICS

Before we delve further into the discussions on QKD protocol, it is instructive to briefly outline certain basic elements of quantum information that we would use throughout the thesis. We refer to Nielsen & Chuang (2010) for a more comprehensive reference on the subject.

1.2.1 Quantum States

The state of a quantum mechanical system can be represented by a normalized vector in a Hilbert space. Commonly, this state is written in terms of the Dirac notation, that is, the bra-ket notation. The simplest quantum system which is defined in a two dimensional Hilbert space, is known as the quantum bit or simply qubit. A qubit can be expressed in terms of the two computational states that form an orthonormal basis as follows

$$|0\rangle \equiv \begin{pmatrix} 1 \\ 0 \end{pmatrix}; \quad |1\rangle \equiv \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \tag{1.1}$$

in which the left hand side indicate the ket notation that may also be represented as a column vector. In its most general form, a qubit can be written as a superposition of these two states described as

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \tag{1.2}$$

in which α and β are complex numbers with $|\alpha|^2 + |\beta|^2 = 1$.

As a column vector may represent a ket $|\psi\rangle$, its Hermitian adjoint which belongs the dual Hilbert space, the bra, $\langle\psi|$, may be represented by the row vector defined as

$$\langle\psi| = \left(|\psi\rangle^{\dagger}\right) = \left(\begin{array}{c} \alpha \\ \beta \end{array}\right)^{\dagger} \equiv \left(\begin{array}{cc} \alpha^{*} & \beta^{*} \end{array}\right), \tag{1.3}$$

where α^{*} and β^{*} are the complex conjugate of α and β, respectively. Hence, the outer product $|\psi\rangle\langle\psi|$ in its matrix form can be expressed as

$$|\psi\rangle\langle\psi| = \left(\begin{array}{c} \alpha \\ \beta \end{array}\right)\left(\begin{array}{cc} \alpha^{*} & \beta^{*} \end{array}\right) = \left(\begin{array}{cc} \alpha\alpha^{*} & \alpha\beta^{*} \\ \beta\alpha^{*} & \beta\beta^{*} \end{array}\right). \tag{1.4}$$

1.2.2 Multipartite Quantum States

A composite system involves the interaction of two or more quantum mechanical systems in which the states of such systems are represented by multipartite quantum states. As an explicit example, let us consider bipartite systems. Considering two (two dimensional) Hilbert spaces H_A and H_B, the vector of a composite two-qubit system is given by a state in $|\Psi\rangle \in H_A \otimes H_B$ in which $\otimes$ denotes the Kronecker or tensor product. Consider two qubits $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \in H_A$ and $|\varphi\rangle = \gamma|0\rangle + \zeta|1\rangle \in H_B$, if $|\Psi\rangle$ can be written as

$$|\Psi\rangle \equiv |\psi\rangle \otimes |\varphi\rangle = \left(\begin{array}{c} \alpha \\ \beta \end{array}\right) \otimes \left(\begin{array}{c} \gamma \\ \zeta \end{array}\right) = \left(\begin{array}{c} \alpha\gamma \\ \alpha\zeta \\ \beta\gamma \\ \beta\zeta \end{array}\right), \tag{1.5}$$

then $|\Psi\rangle$ is a separable state. Equivalently, we can also write $|\psi\rangle \otimes |\varphi\rangle$ as $|\psi\rangle|\varphi\rangle$, $|\psi,\varphi\rangle$ or $|\psi\varphi\rangle$.

However, if the composite system cannot be written in terms of the tensor product of two states as in the above, then it is said to be entangled. The famously known examples of entanglement are the maximally entangled two qubit states, known as the Bell states. The four orthogonal Bell states, which form the Bell basis are given by

$$\left|\Phi^{+}\right\rangle=\frac{\left|00\right\rangle+\left|11\right\rangle}{\sqrt{2}}, \tag{1.6}$$

$$\left|\Phi^{-}\right\rangle=\frac{\left|00\right\rangle-\left|11\right\rangle}{\sqrt{2}}, \tag{1.7}$$

$$\left|\Psi^{+}\right\rangle=\frac{\left|10\right\rangle+\left|01\right\rangle}{\sqrt{2}}, \tag{1.8}$$

$$\left|\Psi^{-}\right\rangle=\frac{\left|01\right\rangle-\left|10\right\rangle}{\sqrt{2}}. \tag{1.9}$$

1.2.3 Quantum Measurement

Suppose that $\{M_m\}$ is a collection of measurement operators that acts on the system being measured with *m* being the possible measurement results. If the state of the quantum system is $\left|\psi\right\rangle$ immediately before the measurement then the probability that result *m* occurs is given by

$$p(m)=\left\langle\psi\right| M_m^{\dagger} M_m \left|\psi\right\rangle. \tag{1.10}$$

After the measurement, the state of the system is,

$$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}}. \tag{1.11}$$

The measurement operators satisfy the completeness equation

$$\sum_m M_m^\dagger M_m = I, \tag{1.12}$$

where *I* is defined as the identity operator.

1.2.4 Density Operator

Another way of describing the state of a quantum system is by resorting to the density operator formalism. This formalism is useful to describe the ensembles of quantum states that is not completely known (i.e. not prepared in a particular known state).

Let us consider a quantum system made up of an ensemble of pure states $|\psi_i\rangle$ with respective probability p_i. Then, the density operator ρ associated to the quantum system can be written as

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \tag{1.13}$$

where $\sum_i p_i = 1$. If the quantum system ρ is measured with respect to measurement operator M_m, then the probability $p(m)$ that we obtain result *m* is

$$p(m) = \mathrm{tr}(M_m^\dagger M_m \rho), \tag{1.14}$$

with $\mathrm{tr}(\cdot)$ representing the trace. The density operator of the system that corresponds to the post measurement is given by

$$\rho_m = \frac{M_m \rho M_m^\dagger}{\mathrm{tr}(M_m^\dagger M_m \rho)}. \tag{1.15}$$

Suppose that a quantum system of state $|\psi\rangle$ is a pure state i.e. it is known exactly. Then, the density operator ρ corresponding to a pure state $|\psi\rangle$ can be defined as

$$\rho = |\psi\rangle\langle\psi|, \tag{1.16}$$

with the trace of ρ being equal to 1 i.e. $\mathrm{tr}(\rho) = 1$.

1.2.5 Shannon Entropy

Let us consider a random variable X with probability distribution, $p_1 \ldots p_n$. The Shannon entropy of a random variable X, $H(X)$ can be described as a measure of uncertainty about X before we learn of its outcome. This entropy can simply be written as

$$H(X) \equiv H(p_1, \ldots, p_n) \equiv -\sum_x p_x \log_2 p_x. \tag{1.17}$$

Alternatively, we can view eq. (1.17) as the amount of information that we would have acquired after we have learned of its outcome. The entropy of a random variable that only has two outcomes with probabilities p and $1-p$, is known as the binary entropic function written as follows

$$h(p) \equiv -p\log_2 p - (1-p)\log_2(1-p). \tag{1.18}$$

The binary entropic function would be highly relevant to our work, as we will consider the case of binary outcomes.

1.3 QUANTUM KEY DISTRIBUTION

According to Nielsen & Chuang (2010), the idea of quantum cryptography originated in the late 1960s, in a work proposed by Wiesner (1983). This work, that was only published a decade later, introduced the idea of utilizing the laws of quantum physics to realize quantum money that is impossible to counterfeit. Inspired by this concept, Bennett & Brassard (1984) developed the first quantum key distribution (QKD) protocol that is famously known as BB84, as a secure way of distributing or establishing secure keys between parties which is based on quantum theory.

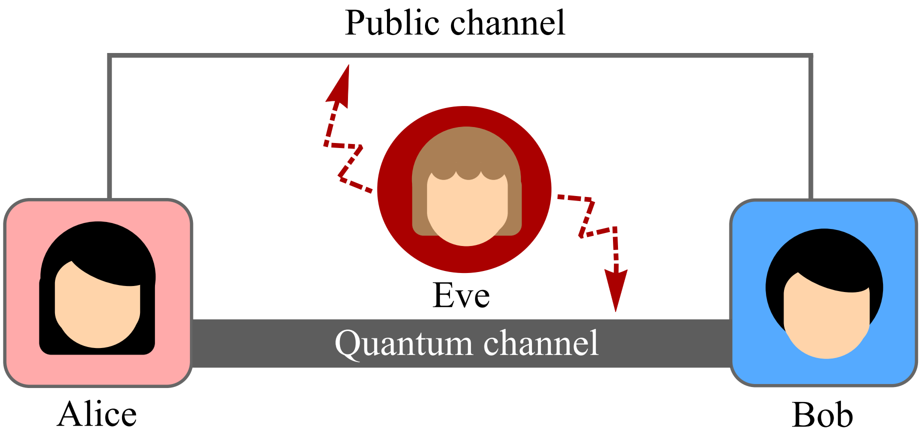

Figure 1.1 Generic diagram of a QKD protocol.

The basic framework of a QKD protocol usually involves two distant parties, conventionally called Alice and Bob, connected by two types of communication channel, that is, the quantum channel and the public channel as shown in Figure 1.1. A third party, say Eve, can listen to the communication on the public channel but she cannot tamper with it. However, any communication over the quantum channel is susceptible to a malicious Eve's interference.

The process of extracting a secure key in a QKD protocol can generally be divided into two phases. The first phase requires the legitimate parties to communicate over the quantum channel, which involves the transmission of information carriers (i.e. qubit). In the BB84 protocol, Alice would first prepare a qubit in one of two randomly chosen mutually unbiased bases (i.e. two orthonormal bases in which measuring a state of one basis in the other basis would result in a random outcome) before sending it to Bob through the quantum channel. As Bob receives the qubit, he would need to perform a measurement chosen randomly in either one of the two mutually unbiased bases. It is obvious to note that in the absence of noise, they will share a perfectly correlated result provided that both of them measure in the same basis. Hence, the legitimate parties can definitely share a string of bits called the raw key. To obtain the final secret key, Alice and Bob proceed to the second phase of the protocol, which takes place over the public channel.

During the second phase, Bob would publicly declare his choice of measurement bases corresponding to each run. Consequently, Alice will reveal whether or not his measurement match to hers over the public channel. Any measurement in a different basis will result in an uncorrelated bit. They will eventually discard the uncorrelated bits and keep a shorter string of correlated bits called the sifted key. In a more realistic scenario, the sifted key may contain errors as all channels are noisy. The noisy channel may either be the result of Eve's attempt to eavesdrop or simply due to technical imperfections. However, to err on the side of caution, Alice and Bob will always assume the worse, i.e. this is due to the presence of an eavesdropper. Conventionally, Alice and Bob will then reveal their bits from a random subset of the sifted key to each other to estimate the amount of errors and then they will commit to an error correction procedure so that the errors in the key can be corrected. In this way, they can also estimate the amount of information that Eve may gain and ultimately use this estimation to reduce Eve's information in the remaining subset to obtain the final secure key. The process of reducing Eve's information can be achieve via the procedure known as privacy amplification.

Since the first publication of this QKD protocol, there are a number of variants of BB84 protocol that have been proposed. Some of the more widely known examples include the B92 protocol proposed by Bennett (1992) in which Alice prepares the key in one of two non-orthogonal states and the six-state protocol (Bruß, 1998) that encodes the key in one of six states selected randomly from three mutually unbiased bases. A more comprehensive review is provided in Gisin et al. (2002).

Ekert (1991) had presented a different QKD protocol than that of BB84. In contrast to BB84 protocol, Ekert proposed to use a pair of entangled particles, one for each party, to establish the secret key. In addition to that, the security of the so-called E91 protocol is guaranteed by observing the violation of Bell inequality (Freedman & Clauser, 1972), particularly, the CHSH inequality (Clauser, Horne, Shimony, & Holt, 1969). However, Bennett, Brassard, & Mermin (1992) argued that the E91 protocol was in fact equivalent to the BB84 protocol, with the former just being an entanglement version of the latter. This claim is not completely false considering that one would use two-qubit states and perform measurement in mutually unbiased bases.

As pointed out by Scarani (2012), detailed investigations has shown that E91 protocol cannot be reproduced by local variable, unlike BB84 and its entangled version, BBM92 protocol proposed by Bennett et al. (1992). This security advantage of E91 protocol has become the basis to achieve device independent security in which would be further discussed in the next section.

Up till now, our discussion on QKD protocol revolves around the idea of transmitting information carrier through the quantum channel in order to distribute a secret key bit. However, Noh (2009) had introduced a contrasting protocol (we refer to it as the counterfactual QKD or CQKD in short) in which information is being transferred from one party to another without any qubit travelling between them. The CQKD protocol utilizes the counterfactual phenomena, in which we can infer the presence of an object effectively without having to measure it (Noh, 2009). A proper description of such a notion can be found in (Vaidman, 2016).

In the case of counterfactual protocol presented by Noh (2009), given a photon sent to Bob over the quantum channel, it would either blocked by Bob or otherwise. Alice can infer whether Bob is blocking the path or not without even being near the blockade. In order for this phenomena to take effect, one requires as a resource, a single photon entanglement which can be attained by submitting a single photon to a beam splitter. The single photon entanglement refers to a phenomena of entanglement between the photon numbers in two spatially separated modes where one mode is connected to Bob as the quantum channel while the other remains with Alice. Given a 50:50 beam splitter, photons can be found half of the time on the quantum channel.

Events where a photon actually travels to Bob would be discarded, while the events where the photon has been assuredly blocked by Bob would be considered as part of the raw key. A detailed description of the CQKD is deferred to Chapter 4. The discussions concerning the counterfactual protocol includes analyzing its security proof (Li, 2014; Yin, Li, Chen, Han, & Guo, 2010), improving its efficiency (Sun & Wen, 2010) and also modifications (Shenoy, Srikanth, & Srinivas, 2013). The protocol proposed by Noh (2009) has also been implemented experimentally (Brida, Cavanna, Degiovanni, Genovese, & Traina, 2012).

Despite the various schemes afforded thus far, the most pessimistic demands would not be satisfied as these schemes rely strongly on the requirement that the exploited degrees of freedom lies within the control of the legitimate users. Relaxing such a requirement has led to the birth of "device independent QKD" or simply DIQKD protocol.

1.3.1 Analyzing security of a QKD

The main objective in analyzing eavesdropping attack is to find security proofs for a QKD protocol (Gisin et al., 2002). Basically, Eve's attack strategies in a generic QKD protocol can be divided into three classes, namely the individual, collective, and the coherent attacks. However, in this work we are only focusing on the individual attack scenario and we dedicate a brief discussion on the collective and coherent attack in the context of future direction. The individual attacks is defined as such Eve would probe and measures Alice's and Bob's quantum system using the same strategy, separately and independently (Gisin et al., 2002).

The Csiszár-Körner theorem (Csiszár & Körner, 1978) states that Alice and Bob can distill a secret key if and only if $I_{AB} \geq I_{AE}$ or $I_{AB} \geq I_{BE}$ where I_{AB} represents Alice-Bob mutual information while I_{AE} and I_{BE} represent Eve's information on Alice's and Bob's raw key, respectively. Practically, the raw key needs to be converted to one where $I_{AB} = 1$ and $I_{AE} = 0$. This can be achieved by first correcting any possible errors between Alice and Bob and subsequently a contraction of the key to eradicate any possible information Eve may have. The process of establishing a secret key from a raw key thus involves an error correction procedure, as noted in the earlier section, to be executed between Alice and Bob as well as suppressing Eve's information to arbitrarily low levels through privacy amplification. According to Shannon, the amount of perfectly correlated bit that can be extracted from the raw keys for a one-way communication is given by, $I_{AB} = H(A) - H(A|B)$ where $H(\cdot)$ is the Shannon entropy (Scarani et al., 2009). This can be understood as having a preshared key of that amount to encode any bits transmitted between the legitimate parties committing to error corrections. As for privacy amplification, the commonly used procedure is for Alice and Bob to agree on a randomly selected hash functions to operate on their respective raw keys. The set of hash functions used would be the two-universal hash function (Gisin et al., 2002). Thus, the achievable secret key rate, K using one-way classical postprocessing (Csiszár & Körner, 1978; Gisin et al., 2002) is

$$K = \max\left\{ I_{AB} - I_{AE}, I_{AB} - I_{BE} \right\}. \tag{1.19}$$

1.4 DEVICE-INDEPENDENT QUANTUM KEY DISTRIBUTION

In most QKD protocols (Gisin et al., 2002), Alice and Bob are assumed to have perfect control of their apparatuses (at least the dimension of the degree of freedom used for measurements) and that the devices are ultimately trusted. Though, in reality, this is usually not the case as devices are prone to various imperfections and a more paranoid view would even suggest Eve to be the person who manufactures Alice's and Bob's devices. Given this, there has been a growing interest in developing protocols where the legitimate parties are not required to trust their devices, that is, the device independent QKD (DIQKD) protocol. The only set of assumptions for security analysis of this protocol, which is also necessary for all QKD protocols, requires that (Pironio et al., 2009):

1. confidential information cannot escape to the outside of the legitimate parties' site;
2. random number generator used can be trusted;
3. classical devices such as memories and computing devices used by the legitimate parties can be trusted;
4. the parties share an authenticated public channel;
5. quantum theory is correct.

The basis for security guarantee of this framework lies in the establishment of nonlocal correlations.

1.4.1 Nonlocal Correlation

In 1935, Albert Einstein, Boris Podolsky and Nathan Rosen proposed a thought experiment (Einstein, Podolsky, & Rosen, 1935), aiming to argue the incompleteness of quantum mechanics. For a theory to be considered as complete, Einstein et al. (1935) states that it should contain element which corresponds to an element in physical reality. Without going into the details, it is nevertheless worth noting that the work is built upon the assumption that Nature obeys the principle of local realism, made up of the following two principles; the principle of realism, in which the existence of physical properties are independent of observation; and the principle of locality, in which the measurement made by distant parties does not influence each other (Nielsen & Chuang, 2010). With respect to these assumptions, John Bell (1964) formulated a thought experiment describing how the Nature was supposed to behave in accordance to Einstein et al. (1935), with which he comes up with Bell inequality. In his experiment, two systems that may have been produced by the same source are each given to two distant parties, Alice and Bob to be measured as depicted by Figure 1.2.

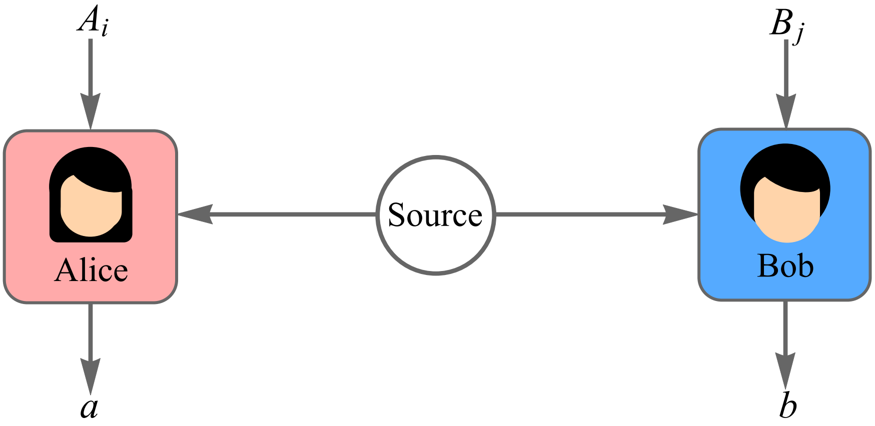

Figure 1.2 Illustration of a bipartite system in Bell experiment.

Suppose we consider a bipartite system in which we represent the binary input settings by A_1 and A_2 for Alice and, B_1 and B_2 for Bob with binary outcomes a and b, respectively. Let us denote $E(A_i, B_j)$ as the expectation value of the correlation A_iB_j and consider the following correlation function

$$S = E(A_1, B_1) + E(A_2, B_1) + E(A_1, B_2) - E(A_2, B_2), \tag{1.20}$$

in which $E(A_i, B_j) = p(a = b \mid A_i, B_j) - p(a \neq b \mid A_i, B_j)$ with $p(ab \mid A_i, B_j)$ represent the probability of obtaining outcomes a and b given that inputs A_i and B_j were measured.

Bell (1964) states that if the correlation function of eq. (1.20) satisfies local realism principle, then we will necessarily obtain the following

$$-2 \leq S \leq 2, \tag{1.21}$$

which is often known as the CHSH inequality (Clauser et al., 1969). Now, let us consider a quantum physics scenario where Alice and Bob are allowed to share a maximally entangled system of two qubits state $|\psi\rangle$. The correlation of A_i and B_j can then be written as

$$E_Q(A_i, B_j) = \langle\psi| A_i \otimes B_j |\psi\rangle, \tag{1.22}$$

in which A_i and B_j are operators and the subscript Q represent the quantum scenario. With appropriate measurements, it can be easily shown that in quantum physics description, $S = 2\sqrt{2}$ (Cirel'son, 1980); a value which is greater than that predicted in eq. (1.21). The violation of eq. (1.21) implies that at least one of the local realism assumptions is incorrect, a phenomena we refer to as nonlocality.

Nonlocality or nonlocal correlations may be understood as a correlation resulting from measurements of a number of systems that cannot be reproduced by any local theory. Thus, measurements made by two parties, Alice and Bob on such systems may result in nonlocal correlations though it should be clear that such correlations are nevertheless no-signaling. Suppose that Alice's measurement choice is x with outcome a while Bob's measurement choice is labelled as y and its output as b. Writing $\Pr(ab \mid xy)$ as the probability of getting outcomes a and b when measuring x and y, respectively. The no-signaling condition states that the marginal probability of one party is independent of the other party's choice of measurement input, which can simply be written as (Acín, Massar, & Pironio, 2006)

$$\sum_a \Pr(ab\,|\,xy) = \Pr(ab\,|\,x'y) = \Pr(b\,|\,y) \quad \forall b,x,x',y, \tag{1.23}$$

$$\sum_b \Pr(ab\,|\,xy) = \Pr(ab\,|\,xy') = \Pr(a\,|\,x) \quad \forall a,x,y,y'. \tag{1.24}$$

Under the no-signalling condition, the CHSH inequality is shown to be equivalent to another variant of Bell inequality namely, the Clauser-Horne (CH) inequality (Clauser & Horne, 1974) by Mermin (1995) and Cereceda (2001) as pointed out by Renou, Rosset, Martin, & Gisin (2016).

1.4.2 Nonlocality as a Resource

The possibility of exploiting the nonlocal resource as a security measures was initially highlighted in Ekert (1991) protocol, in which he proposed the idea of basing the protocol's security on Bell inequality. However, it would be Mayers & Yao (1998) idea of self-testing device that points out its potential in a device independent context.

The preliminary work in the direction of DIQKD was first proposed to demonstrate security proof against a general attack by an eavesdropper constrained only by the no-signaling principle (Barrett, Hardy, & Kent, 2005). Even though the protocol is proven to be inefficient, it follows from this idea that (Acín, Gisin, & Masanes, 2006) proposed a binary input-output scheme namely, the CHSH protocol (in which further detail was given in Scarani et al. (2006) that is secure against an individual attack by an adversary who is supra-quantum, i.e. not limited by the dictates of quantum theory though bounded by the no-signaling principle. The individual attack assumes that Eve would try to gain information on each quantum systems separately and independently. The attack requires Eve, to distribute strategies extracted from the no-signaling polytope which is described by 8 extremal deterministic points plus one nonlocal point given by the nonlocal Popescu and Rohrlich (PR) box (Popescu & Rohrlich, 1994). The PR box is defined as the joint probability for the output pairs given relevant measurement input pairs as follows

$$\Pr_{PR}(ab\,|\,xy) = \begin{cases} \tfrac{1}{2}, & a \oplus b = xy \\ 0, & \text{otherwise} \end{cases}, \tag{1.25}$$

in which $\oplus$ is addition modulo 2. It can be easily verified that the PR box violates the CHSH value up to algebraic maximum of 4 (Popescu & Rohrlich, 1994), a value that is beyond the Tsirelson bound of $2\sqrt{2}$ (Cirel'son, 1980) for quantum physics.

The protocol has the very interesting feature according to which no assumptions are made regarding the nature of measurements by Alice and Bob, which can be seen as black boxes. However, an implementation of the CHSH protocol within the quantum framework results in nonperfect overlapping of measurement basis for key extraction purposes, thus resulting in a noisy channel in the absence of an eavesdropper.

While the framework for device independent scenario in protocols that essentially sees one party submitting a signal to the other party for measurement already existed, the counterfactual QKD protocol on the other hand does not have such framework. In order to develop the device independent framework for counterfactual QKD, it is instructive to have a proper understanding of CHSH like protocol i.e. a binary measurement based protocol, especially in the context of single photon entanglement QKD. In the following we will present our approach and objectives.

1.5 RESEARCH APPROACH AND OBJECTIVES

In this thesis, we aim to ultimately develop a device independent framework for counterfactual QKD. As we have stated before, the single photon entanglement is essential in explaining the counterfactual phenomena. In order to help our understanding of the single photon entanglement, we start off by understanding the binary measurement QKD using the following maximally entangled states:

$$|\Psi\rangle = \frac{|10\rangle - |01\rangle}{\sqrt{2}}, \tag{1.26}$$

and how it could be use in the context of single photon entanglement. With this knowledge, we hope to apply it to the device independent scenario. The key rates can be derived based on the Csiszár-Körner theorem (Csiszár & Körner, 1978) in which the details will be provided in the ensuing chapters. Note that throughout the thesis we will use the term framework and scenario interchangeably.

This research aims to achieve the following three objectives:

1. To optimize a binary measurement QKD.
2. To formulate a device independent framework and determine the relevant secret key rate for single photon entanglement QKD.
3. To formulate counterfactual QKD in a device independent scenario.

1.6 THESIS OUTLINE

This thesis is divided into five chapters. The first chapter serves as an introduction for the whole thesis.

In Chapter 2, we consider an optimal quantum key distribution setup based on minimal number of measurement bases with binary yields used by parties against an eavesdropper limited only by the no-signaling principle. We compare between two versions in which Version I would represent the case where only Alice would reveal her measurement bases over a public channel and another scenario, which we refer to as Version II, would be for both to disclose their bases. In both cases, the parties will determine the security of the protocol by means of checking for violation of Bell inequality, particularly the CHSH inequality, on a subset of the measurement results. We also consider a simpler form of Version II by having a maximal correlation between Alice and Bob in one set of bases' choice by setting $\beta = 0$. This idea of overlapping measurement bases would have immediate use in the next chapter. Parts of this work has already been published in Kamaruddin & Shaari (2016).

As a preliminary step, in Chapter 3, we briefly review the quantum mechanical description of a beam splitter and its role in the homodyne detection scheme. We then present a quantum key distribution scheme based on the protocol by Lee, Lee, Chung, Lee, & Kim (2003) which exploits an unbalanced homodyne detection scheme to demonstrate its security through observation of violation of the CH inequality. We describe our analysis of security against individual attack within a device-independent scenario where Eve is constrained only by the no-signaling principle. Parts of this work has already been published in Kamaruddin & Shaari (2015).

We start off Chapter 4 by describing the counterfactual protocol as presented by Noh (2009). We proceed to show that the protocol is insecure in a device independent scenario. Consequently, we propose a framework for device independent counterfactual QKD with the main ingredient being the single photon entanglement QKD protocol presented in Chapter 3. We then provide a heuristic security analysis of the proposed protocol. Here we acknowledge that we benefit very much from discussions about the single photon entanglement mainly within the context of Mach-Zehnder interferometer with Piotr Kolenderski.

In Chapter 5, we provide a summary of this research and offer some suggestions for future research.

CHAPTER TWO

OPTIMAL DEVICE INDEPENDENT QUANTUM KEY DISTRIBUTION

2.1 PUBLICATION

The findings reported in this chapter have been published in the journal Scientific Reports, Volume 6, 30959 (2016) as Optimal Device Independent Quantum Key Distribution, with the citation: (2016) doi: 10.1038/srep30959. The authors for the publication are (in order as appears in the publication) Suhaili Kamaruddin and Jesni Shamsul Shaari.

2.2 INTRODUCTION

As briefed in the first chapter, communications in a generic QKD protocol can be divided into two phases. The first phase involves communication between the legitimate parties that is, Alice and Bob, over a quantum channel in which the transmission of quantum signals (commonly photons) and measurements take place. On the other hand, the second phase would require the distribution of classical information between the parties over a classical channel. The classical channel is not required to be private in the sense that it does not need to be able to send private bits; it does however need to be free of any manipulation by a malicious attacker. This can be achieved by authentication of the channel. Alternatively, the classical information can be broadcasted, again with the intent of ensuring that the information sent/ received is free from tampering. With the help of classical communication phase, Alice and Bob are able to perform basis revelation, error correction and remove Eve's information in privacy amplification procedure. Interestingly enough, a protocol can be different with only a change in the feature of classical information distribution. For example, if we simply change the classical communication phase of BB84 protocol such that Alice would not reveal her bases, rather a set containing a pair of nonorthogonal state (with one of it being the state sent) then we will obtain the SARG04 protocol proposed by Scarani, Acin, Ribordy, & Gisin (2004). In fact, according to Scarani et al. (2004), the SARG04 protocol actually performs better than BB84 protocol. Hence, it will be intriguing to observe how variants of classical information distribution would influence the performance of a QKD protocol.

In this chapter, we shall consider in detail a binary measurement QKD for two parties, Alice and Bob, in which each party would commit to either one of two measurement bases and each yields only binary results. We will describe the protocol using quantum formalism i.e. we assume that the legitimate parties believe that they actually perform measurements on quantum states in a well-defined Hilbert space. However, the most pessimistic view would suggest that the protocol be seen as black boxes and Alice and Bob may not have any prior knowledge of their internal processes. We will then consider two different scenarios depending on the variation in the subsequent classical distribution of information between the legitimate parties, thus defining the protocol to allow for different secure key rates with the aim of achieving the highest possible.

2.3 BINARY MEASUREMENT QKD

We begin with a description of the protocol, which we define within a framework as described by quantum physics. Alice submits to Bob a quantum state of which each party would measure subsystems thereof available to them. In an ideal setup, we assume that this would result in Alice and Bob sharing the following maximally entangled states:

$$\left|\Psi\right\rangle = \frac{1}{\sqrt{2}}\left(\left|10\right\rangle - \left|01\right\rangle\right). \tag{2.1}$$

In each run, Alice and Bob can independently choose to apply one of two measurements with each choice resulting in binary outcomes. For definiteness, we describe Alice's and Bob's measurements as x and y with $x, y \in \{0,1\}$ and the binary results for their measurement choices are $a, b \in \{0,1\}$, respectively.

Restricting measurements to projecting states on the $X - Z$ plane of the Bloch sphere, any measurement can be described as projecting onto the following states;

$$\left|\theta^{+}\right\rangle = \cos(\theta)\left|0\right\rangle + \sin(\theta)\left|1\right\rangle, \tag{2.2}$$

$$\left|\theta^{-}\right\rangle = \sin(\theta)\left|0\right\rangle - \cos(\theta)\left|1\right\rangle, \tag{2.3}$$

and we set $x = 0$ to be in the Z basis i.e. $\theta = 0$ and $x = 1$ indicates the measurement made in angle $\theta = \alpha$. Meanwhile, Bob's setting is described such that $y = 0$ and $y = 1$ correspond to measurement angles $\theta = \beta$ and $\theta = \gamma$, respectively. We note that the measurement resulting in state $\left|\theta^{+}\right\rangle$ corresponds to the logical bit value $a = 0$ (for Alice) and $b = 0$ (for Bob) while, $\left|\theta^{-}\right\rangle$ corresponds to $a = 1$ (for Alice) and $b = 1$ (for Bob). At the end of the transmission and measuring process, Alice and Bob would exchange classical information to allow them to share a raw key.

The simplest scenario is where only Alice would reveal her measurement bases over a public channel (we refer to this as Version I). Another scenario, which we refer to as Version II, would be for both Alice and Bob to disclose their bases. In both cases, the parties will determine the security of the protocol by means of checking for violation of Bell-type inequality on a subset of the measurement results.

In this work we will consider the case where Alice and Bob would compute the amount of the following CHSH correlations (Clauser et al., 1969):

$$CHSH = \left\langle x=0, y=0 \right\rangle + \left\langle x=0, y=1 \right\rangle + \left\langle x=1, y=0 \right\rangle - \left\langle x=1, y=1 \right\rangle, \tag{2.4}$$

in which local correlations is bounded by inequality $-2 \le CHSH \le 2$. However, in modeling a noisy setting, we shall assume a depolarizing channel between the legitimate parties and thus, eq. (2.1) is transformed to a Werner state (Werner, 1989), ρ given as:

$$\rho = F\left|\Psi\right\rangle\left\langle\Psi\right| + (1-F)\frac{I}{4}, \tag{2.5}$$

where $0 \le F \le 1$ with the fidelity, $F = 1$ represents the noise-free condition.

From the results obtained when measuring state ρ (see Table 2.1), it is not difficult to show that the estimation of CHSH violation of eq. (2.4), $\left\langle CHSH \right\rangle$ can be written as

$$\left\langle CHSH \right\rangle = -F\left[\cos(2(\alpha-\beta)) + 2\sin(\alpha)\sin(\alpha-2\gamma) + \cos(2\beta)\right]. \tag{2.6}$$

Depending on the results, Alice and Bob may choose to abort the protocol or proceed to error correction and privacy amplification.

Table 2.1 The correlations table as a result of measuring state ρ with $\eta = \frac{1}{4}\left(1 - F\right)$.

	$y=0, b=0$	$y=0, b=1$	$y=1, b=0$	$y=1, b=1$
$x=0,$ $a=0$	$\frac{F}{2}\sin^2(\beta)+\eta$	$\frac{F}{2}\cos^2(\beta)+\eta$	$\frac{F}{2}\sin^2(\gamma)+\eta$	$\frac{F}{2}\cos^2(\gamma)+\eta$
$x=0,$ $a=1$	$\frac{F}{2}\cos^2(\beta)+\eta$	$\frac{F}{2}\sin^2(\beta)+\eta$	$\frac{F}{2}\cos^2(\gamma)+\eta$	$\frac{F}{2}\sin^2(\gamma)+\eta$
$x=1,$ $a=0$	$\frac{F}{2}\sin^2(\alpha-\beta)+\eta$	$\frac{F}{2}\cos^2(\alpha-\beta)+\eta$	$\frac{F}{2}\sin^2(\alpha-\gamma)+\eta$	$\frac{F}{2}\cos^2(\alpha-\gamma)+\eta$
$x=1,$ $a=1$	$\frac{F}{2}\cos^2(\alpha-\beta)+\eta$	$\frac{F}{2}\sin^2(\alpha-\beta)+\eta$	$\frac{F}{2}\cos^2(\alpha-\gamma)+\eta$	$\frac{F}{2}\sin^2(\alpha-\gamma)+\eta$

2.4 SECURITY ANALYSIS: SUPRA-QUANTUM EVE

We consider the pessimistic view where Eve has control of the degrees of freedom of Alice's and Bob's observables. We could imagine that the eavesdropper, Eve fabricated the devices and she is in fact controlling the source. The legitimate parties are essentially ignorant of the internal process of the protocol and their devices may be regarded as black boxes with binary inputs and outputs. We define Eve's strategy as being constrained by the no-signaling principle while requiring observations made by both Alice and Bob to be consistent with quantum predictions. Similar to the CHSH protocol (Acín, Gisin, et al., 2006; Scarani et al., 2006), Eve’s strategy is to submit to Alice and Bob a convex combination of probabilistic distributions of deterministic and nonlocal strategies.

A deterministic strategy is a strategy for which results obtained for any given set of Alice's and Bob's measurement would be fully determined i.e no uncertainty and conforms completely to a local theory (Scarani, 2009). On the other hand, a nonlocal strategy is one in which a PR box (Popescu & Rohrlich, 1994) is distributed and measurement results are not only probabilistic, but also violates the CHSH inequality up to its algebraic maximum (Scarani, 2009). However, since our protocol is described in terms of an anti-correlated state of eq. (2.1), it would be appropriate to use the anti-PR (aPR) box (Skrzypczyk & Brunner, 2009) for which all measurement settings (except for $x = y = 1$) result in anti-correlations rather than the PR box that provides for correlations. The aPR box, which is equivalent to the PR box up to a trivial local processing (Scarani, 2009), violates the lower bound of CHSH (as opposed to the PR box violating on the positive side) is given by the probability function,

$$\Pr_{aPR}(ab\,|\,xy) = \begin{cases} \tfrac{1}{2}, & a+b = xy \oplus 1 \\ 0, & \text{otherwise} \end{cases}, \tag{2.7}$$

where $\oplus$ is addition modulo 2. The deterministic strategies are described by four deterministic functions $G : [4] \times \{0,1\} \to \{0,1\}$ for $r = 1,2,3,4$ defined by

$$G(r,x) = \begin{cases} 0, & r=1 \\ 1, & r=2 \\ x, & r=3 \\ x+1, & r=4 \end{cases}. \tag{2.8}$$

Thus, the sixteen deterministic strategies, $\mathbf{D}_{rs}$ are given by

$$\mathbf{D}_{rs} = \left\{ D_{rs}^{xy}(a,b) = \delta_{G(r,x)=a}\delta_{G(s,y)=b} \mid a,b,x,y \in \{0,1\} \right\}, \tag{2.9}$$

where $D_{rs}^{xy}(a,b)$ gives the probability of having input x, y resulting in output a,b for strategy rs (Scarani, 2009).

However, we are only interested in the following eight deterministic strategies, $\mathbf{D}_{12}, \mathbf{D}_{14}, \mathbf{D}_{21}, \mathbf{D}_{23}, \mathbf{D}_{32}, \mathbf{D}_{33}, \mathbf{D}_{41}, \mathbf{D}_{44}$ which would saturate the local bound on the negative side of the CHSH range. Eve's strategy and her information on Alice-Bob distribution can be summarized in Table 2.2 which is a 'complimentary' table to that in Scarani et al. (2006) where Eve would use a PR box instead. Note that the symbol p_{rs} represents the probability of sending strategy $\mathbf{D}_{rs}$ and p_{NL} is the probability of sending aPR box. With aPR box violating the CHSH inequality up to its algebraic minimum value of -4, the estimation of local correlation, $\langle CHSH \rangle$ that Alice and Bob may find would be

$$\langle CHSH \rangle \geq (-4)(1 - p_L) + (-2)p_L \tag{2.10}$$

in which the probability of sending local correlation, $p_L = 1 - p_{NL}$ with $p_L = p_{12} + p_{14} + p_{21} + p_{23} + p_{32} + p_{33} + p_{41} + p_{44}$.

In the ensuing sections, the security analysis, given Eve's attack is constructed within the framework of an eavesdropper who may be supra-quantum but would emulate Alice and Bob's expectations; i.e. the statistics of their measurement results must be consistent with the expectation of quantum physics. We thus assume a one-to-one correspondence rule from the set of Eve's probabilities of strategies sent, E_{ijkl}, where i,k and j,l are Alice and Bob's measurement settings and results respectively to the set of probabilities of Alice-Bob's measurements, $\Pr(a=i,b=j\,|\,x=k,y=l)$.

Table 2.2 Table showing probability distribution of Eve sending the corresponding strategy (as shown in the parentheses) to Alice and Bob. This is 'complimentary' table to that in Scarani et al. (2006) where Eve would use a PR box instead.

	$y=0,b=0$	$y=0,b=1$	$y=1,b=0$	$y=1,b=1$
$x=0,a=0$	$p_{33}(\mathbf{D}_{33})$	$p_{NL}/2(P_{aPR})$ $p_{12}(\mathbf{D}_{12})$ $p_{14}(\mathbf{D}_{14})$ $p_{32}(\mathbf{D}_{32})$	$p_{14}(\mathbf{D}_{14})$	$p_{NL}/2(P_{aPR})$ $p_{12}(\mathbf{D}_{12})$ $p_{32}(\mathbf{D}_{32})$ $p_{33}(\mathbf{D}_{33})$
$x=0,a=1$	$p_{NL}/2(P_{aPR})$ $p_{21}(\mathbf{D}_{21})$ $p_{23}(\mathbf{D}_{23})$ $p_{41}(\mathbf{D}_{41})$	$p_{44}(\mathbf{D}_{44})$	$p_{NL}/2(P_{aPR})$ $p_{21}(\mathbf{D}_{21})$ $p_{41}(\mathbf{D}_{41})$ $p_{44}(\mathbf{D}_{44})$	$p_{23}(\mathbf{D}_{23})$
$x=1,a=0$	$p_{41}(\mathbf{D}_{41})$	$p_{NL}/2(P_{aPR})$ $p_{12}(\mathbf{D}_{12})$ $p_{14}(\mathbf{D}_{14})$ $p_{44}(\mathbf{D}_{44})$	$p_{NL}/2(P_{aPR})$ $p_{14}(\mathbf{D}_{14})$ $p_{41}(\mathbf{D}_{41})$ $p_{44}(\mathbf{D}_{44})$	$p_{12}(\mathbf{D}_{12})$
$x=1,a=1$	$p_{NL}/2(P_{aPR})$ $p_{21}(\mathbf{D}_{21})$ $p_{23}(\mathbf{D}_{23})$ $p_{33}(\mathbf{D}_{33})$	$p_{32}(\mathbf{D}_{32})$	$p_{21}(\mathbf{D}_{21})$	$p_{NL}/2(P_{aPR})$ $p_{23}(\mathbf{D}_{23})$ $p_{32}(\mathbf{D}_{32})$ $p_{33}(\mathbf{D}_{33})$

2.4.1 Version I

We consider the simplest case, that is, when only one party, say Alice, would publicly disclose her measurement bases. The error rate for Alice and Bob, e_{AB} which originates from Eve's sending strategies, is given by the probability, $\sum_{k,l,i} E_{i(i\oplus1)kl}$. In terms of the angles $\alpha,\beta,$ and $\gamma,$ we refer to the one-to-one correspondence between the legitimate parties' measurement settings and the probabilities of Eve's strategies (Table 2.1 and Table 2.2 respectively) and the error rate, e_{AB} is then given by

$$e_{AB} = \frac{1}{4}\left(2-2F+F\left[\sin^2(\alpha-\gamma)+\sin^2(\alpha-\beta)+\sin^2(\beta)+\sin^2(\gamma)\right]\right). \qquad (2.11)$$

Since Bob's bases are not revealed to public, we can view Eve's information on Alice-Bob distribution as represented in Table 2.3.

The readings of Table 2.3 are as follows. Suppose that Eve sends strategy $\mathbf{D}_{12}$ to the legitimate parties and Alice has publicly disclosed that she chose $x=0$. Then, Eve would know for sure that Alice's and Bob's outcome is $a=0$ and $b=1$. However, if Eve sends strategy $\mathbf{D}_{14}$ while Alice declares her choice to be $x=0$, then Eve would be uncertain of Bob's outcome as half of the time it could result in $b=0$ or $b=1$. It is obvious from Table 2.3 that Eve's information on Bob's outcome, I_{BE}, would comes from sending strategy $\mathbf{D}_{12},\mathbf{D}_{21},\mathbf{D}_{32},$ and $\mathbf{D}_{41}$, in which can be rewritten in terms of the angles (α,β,γ) as follows

$$I_{BE} = F\cos^2(\alpha-\gamma)+F\sin^2(\alpha-\beta)+1-F. \qquad (2.12)$$

Hence, with respect to eq. (2.11) and eq. (2.12), the formula for the key rate, K, is given by (Csiszár & Körner, 1978):

$$K = 1 - I_{BE} - h(e_{AB}), \qquad (2.13)$$

with $h(p) \equiv -p\log_2 p - (1-p)\log_2(1-p)$ being the binary entropic function.

Table 2.3 Table showing Eve's information on Alice-Bob distribution when Alice's basis is known.

	$b=0$	$b=1$
$x=0, a=0$	$\frac{1}{2}p_{14}\left(\mathbf{D}_{14}\right)$ $\frac{1}{2}p_{33}\left(\mathbf{D}_{33}\right)$	$\frac{1}{2}p_{NL}\left(P_{aPR}\right)$ $\frac{1}{2}p_{14}\left(\mathbf{D}_{14}\right)$ $\frac{1}{2}p_{33}\left(\mathbf{D}_{33}\right)$ $p_{12}\left(\mathbf{D}_{12}\right)$ $p_{32}\left(\mathbf{D}_{32}\right)$
$x=0, a=1$	$\frac{1}{2}p_{NL}\left(P_{aPR}\right)$ $\frac{1}{2}p_{23}\left(\mathbf{D}_{23}\right)$ $\frac{1}{2}p_{44}\left(\mathbf{D}_{44}\right)$ $p_{21}\left(\mathbf{D}_{21}\right)$ $p_{41}\left(\mathbf{D}_{41}\right)$	$\frac{1}{2}p_{23}\left(\mathbf{D}_{23}\right)$ $\frac{1}{2}p_{44}\left(\mathbf{D}_{44}\right)$
$x=1, a=0$	$\frac{1}{4}p_{NL}\left(P_{aPR}\right)$ $\frac{1}{2}p_{14}\left(\mathbf{D}_{14}\right)$ $\frac{1}{2}p_{44}\left(\mathbf{D}_{44}\right)$ $p_{41}\left(\mathbf{D}_{41}\right)$	$\frac{1}{4}p_{NL}\left(P_{aPR}\right)$ $\frac{1}{2}p_{14}\left(\mathbf{D}_{14}\right)$ $\frac{1}{2}p_{44}\left(\mathbf{D}_{44}\right)$ $p_{12}\left(\mathbf{D}_{12}\right)$
$x=1, a=1$	$\frac{1}{4}p_{NL}\left(P_{aPR}\right)$ $\frac{1}{2}p_{23}\left(\mathbf{D}_{23}\right)$ $\frac{1}{2}p_{33}\left(\mathbf{D}_{33}\right)$ $p_{21}\left(\mathbf{D}_{21}\right)$	$\frac{1}{4}p_{NL}\left(P_{aPR}\right)$ $\frac{1}{2}p_{23}\left(\mathbf{D}_{23}\right)$ $\frac{1}{2}p_{33}\left(\mathbf{D}_{33}\right)$ $p_{32}\left(\mathbf{D}_{32}\right)$

By numerically optimizing eq. (2.13) in a noiseless condition, we would find that there are no useful key rate that can be extracted. This finding is not at all surprising as it is apparent from Table 2.2 that the bit strings derived from $x = y = 1$

does not come from correlations that include the nonlocal strategies. Hence, a large amount of bits has to be thrown away in the privacy amplification procedure due to the fact that in the cases of $x = y = 1$ the bits that contribute for the key string would be known to Eve.

2.4.1.1 Pseudosifting

In order to ensure that Eve would be at a disadvantage in regards to the correlations between Alice and Bob, i.e. to ensure the correlations are derived from strategies that should include the nonlocal box, referring to Table 2.2, we consider the stipulation where Bob would flip all his bits except in the event where Alice declares $x = 1$ and Bob measure $y = 1$. This step is equivalent to the pseudosifting procedure introduced by Scarani et al. (2006) (the main concern there was to maximize the correlations between Alice and Bob).

Hence, the error rate between Alice and Bob, e_{AB}^{I} with regards to the triplet angles (α, β, γ) would be

$$\begin{aligned} e_{AB}^{I} &= \frac{1}{4}\left(2 - 2F + F\left[\sin^2(\alpha - \gamma) + \cos^2(\alpha - \beta) + \cos^2(\beta) + \cos^2(\gamma)\right]\right) \\ &= -\frac{\langle CHSH \rangle}{8} + \frac{1}{2}. \end{aligned} \tag{2.14}$$

Based on Table 2.4, we can see that for each deterministic strategy, Eve would only learns about one of Alice's setting, while being totally ignorant about the other. For example, let us assume that Eve submit strategy $\mathbf{D}_{32}$ to the legitimate parties. With regards to Table 2.4, Eve would know for sure of Bob's outcome provided that

Alice’s choice is $x=0$, however the same strategy would result in Eve being uncertain of the outcome when Alice’s setting is $x=1$.

Table 2.4 Table representing Eve’s knowledge on Alice-Bob probability distribution in the event where Bob flip all his bits except for $x=y=1$.

	$b=0$	$b=1$
$x=0,a=0$	$\frac{1}{2}p_{14}(\mathbf{D}_{14})$ $\frac{1}{2}p_{33}(\mathbf{D}_{33})$	$\frac{1}{2}p_{NL}(P_{aPR})$ $\frac{1}{2}p_{14}(\mathbf{D}_{14})$ $\frac{1}{2}p_{33}(\mathbf{D}_{33})$ $p_{12}(\mathbf{D}_{12})$ $p_{32}(\mathbf{D}_{32})$
$x=0,a=1$	$\frac{1}{2}p_{NL}(P_{aPR})$ $\frac{1}{2}p_{23}(\mathbf{D}_{23})$ $\frac{1}{2}p_{44}(\mathbf{D}_{44})$ $p_{21}(\mathbf{D}_{21})$ $p_{41}(\mathbf{D}_{41})$	$\frac{1}{2}p_{23}(\mathbf{D}_{23})$ $\frac{1}{2}p_{44}(\mathbf{D}_{44})$
$x=1,a=0$	$\frac{1}{2}p_{12}(\mathbf{D}_{12})$ $\frac{1}{2}p_{41}(\mathbf{D}_{41})$	$\frac{1}{2}p_{NL}(P_{aPR})$ $\frac{1}{2}p_{12}(\mathbf{D}_{12})$ $\frac{1}{2}p_{41}(\mathbf{D}_{41})$ $p_{14}(\mathbf{D}_{14})$ $p_{44}(\mathbf{D}_{44})$
$x=1,a=1$	$\frac{1}{2}p_{NL}(P_{aPR})$ $\frac{1}{2}p_{21}(\mathbf{D}_{21})$ $\frac{1}{2}p_{32}(\mathbf{D}_{32})$ $p_{23}(\mathbf{D}_{23})$ $p_{33}(\mathbf{D}_{33})$	$\frac{1}{2}p_{21}(\mathbf{D}_{21})$ $\frac{1}{2}p_{32}(\mathbf{D}_{32})$

Assuming the choice of measurement basis is equiprobable, Eve’s information gain on Bob, I_{BE}^{I} would then be

$$
\begin{aligned}
I_{BE}^{I} &= \frac{p_L}{2} \\
&= \frac{\left\langle CHSH \right\rangle + 4}{4}.
\end{aligned}
\tag{2.15}
$$

From eq. (2.14) and eq. (2.15), the key rate, K_I is then given by

$$
\begin{aligned}
K_I &= 1 - I_{BE}^{I} - h(e_{AB}^{I}) \\
&\geq 1 - \left(\frac{\left\langle CHSH \right\rangle + 4}{4} \right) - h(e_{AB}^{I}).
\end{aligned}
\tag{2.16}
$$

It is obvious that the secret key rate is a monotonically increasing function of the CHSH violation (it is clear from eq. (2.14) that an increase in $\left\langle CHSH \right\rangle$ would decrease the uncertainty between Alice and Bob) and thus maximized for angles (α,β,γ) maximizing the CHSH violation and the protocol would be the CHSH protocol (Acín, Gisin, et al., 2006; Scarani et al., 2006). This could be actually derived from eq. (25) in Scarani et al. (2006) where in a quantum setup, Alice and Bob prescribe measurements that would maximize the Bell violation. Thus we can conclude that generalizing the angles of measurements, in a case where only Alice reveals her measurement bases, the most optimal protocol would necessarily reduce to that of CHSH protocol (Acín, Gisin, et al., 2006; Scarani et al., 2006).

Therefore, from now onwards we will be referring version I to the event where Bob would perform the pseudosifting procedure as of the CHSH protocol.

2.4.2 Version II

In this version, we require that both Alice and Bob reveal their measurement bases. With Eve's strategy given by $\sum_{k,l,i} E_{i(i\oplus 1)kl}$, the uncertainty between Alice and Bob, $\omega(\alpha,\beta,\gamma)$ is given by

$$\begin{aligned}\omega(\alpha,\beta,\gamma)=\frac{1}{4}\Bigg[& h\left(F\sin^2(\alpha-\beta)+\frac{1-F}{2}\right)+h\left(F\sin^2(\alpha-\gamma)+\frac{1-F}{2}\right) \\ & +h\left(F\sin^2(\beta)+\frac{1-F}{2}\right)+h\left(F\sin^2(\gamma)+\frac{1-F}{2}\right)\Bigg]. \end{aligned} \tag{2.17}$$

As Alice's and Bob's measurements' settings are eventually made known, any measurement coinciding with the receipt of Eve's deterministic strategies would provide the latter with complete information. Given that Eve's information gain, $I_{BE}^{'}=p_L$ and along with eq. (2.10), the key rate, $K^{'}$ can be shown to be

$$\begin{aligned} K^{'} &= 1-I_{BE}^{'}-\omega(\alpha,\beta,\gamma) \\ &\geq 1-\left(\frac{\langle CHSH\rangle+4}{2}\right)-\omega(\alpha,\beta,\gamma). \end{aligned} \tag{2.18}$$

Through numerical optimization of eq. (2.18) for a perfect error-free channel, we would see that no positive key can be derived. As the $\langle CHSH\rangle$ value decreases, the error in the strings naturally increases, which implies a noisier channel. This would result in a large number of bits being thrown away for privacy amplification. The only way to avoid throwing a lot of bits during the privacy amplification is to reduce the error in the strings by managing the triplet angles (α,β,γ).

However, as we can see from the right hand side of eq. (2.17), minimizing error in one of the term would necessarily increase the error in another term of the equation. For example, if we managed the angle β so that the error in the third term of eq. (2.17) is being minimized, then the error of the first term will increase due to the big difference between angle α and β. Eventually, a lot of bits will be discarded due to error correction procedure. The only way to obtain a secure key is to find a balance between the decrease in the $\langle CHSH \rangle$ value and the increase in the correlations between Alice and Bob.

Nevertheless, we are not able to do this in this scenario, which may probably due to the impossibility of optimizing all the angles to have a minimal kind of error correction and at the same time privacy amplification. However, if we were to have fewer angles to work with, then we would have more control over the angles and decrease the error. Hence, in what follows, we propose a protocol in which the bits for key purposes would be extracted only from one correlation so that we could manage the error in the bit strings and finally obtain a positive key rates.

2.4.2.1 An Optimized Protocol

As mentioned previously, we consider that the bit strings involved for key purposes would only comes from one correlation, specifically from the case $x = y = 0$. Then, the error in the strings that Alice and Bob would have to correct, e_{AB}^{II} (corresponding to Eve's strategy $\sum_i E_{i(i\oplus 1)00}$) is given by,

$$e_{AB}^{II} = \frac{1}{2}\left[1 - F\cos(2\beta)\right]. \tag{2.19}$$

As Eve's information gain, $I_{BE}^{II} = p_L$ and along with eq. (2.10) the key rate, K_{II} can be shown to be,

$$\begin{aligned} K_{II} &= 1 - I_{BE}^{II} - h(e_{AB}^{II}) \\ &\geq 1 - \left(\frac{\langle CHSH \rangle + 4}{2} \right) - h(e_{AB}^{II}), \end{aligned} \tag{2.20}$$

in which

$$h(e_{AB}^{II}) = \frac{1}{2}\left[2 + F\cos(2\beta)\log_2\left(\frac{1 - F\cos(2\beta)}{F\cos(2\beta) + 1} \right) - \log_2\left(1 - (F\cos(2\beta))^2\right) \right]. \tag{2.21}$$

It should be noted that, as Alice's and Bob's measurement bases are randomly chosen, the actual fraction of bits that go into K_{II} from the total number of runs would be less than 1 (in fact if the choices were equiprobable, then the case $x = y = 0$ would occur only $1/4$ of the time). However, given that the cases when $x, y = 1$ are not used for raw key purposes, i.e. only for checking a CHSH violation (along with a sample for when $x, y = 0$), similar to Acín, Massar, et al. (2006), one can imagine having a bias in bases' choice, and so long as sufficient statistics is achieved towards determining CHSH violation, one can have the probability for $x = y = 0$ approaching 1.

In maximizing the key rate, K_{II} we consider the following partial derivatives;

$$\frac{\partial K_{II}}{\partial \alpha} = 2F\sin(\beta - \gamma)\cos(2\alpha - \beta - \gamma), \tag{2.22}$$

$$\frac{\partial K_{II}}{\partial \gamma} = -2F\sin(\alpha)\cos(\alpha - 2\gamma), \tag{2.23}$$

$$\frac{\partial K_{II}}{\partial \beta} = 2F\cos(\alpha)\sin(\alpha - 2\beta) - \frac{\partial h(e_{AB}^{II})}{\partial \beta}, \tag{2.24}$$

where

$$\frac{\partial h(e_{AB}^{II})}{\partial \beta} = -F\sin(2\beta)\log_2\left[\frac{1 - F\cos(2\beta)}{1 + F\cos(2\beta)}\right]. \tag{2.25}$$

Considering eq. (2.4), it is obvious that measurement choices such $\{x = 0\} = \{x = 1\}$ or $\{y = 0\} = \{y = 1\}$ would result in no violation of the CHSH inequality no matter the given bipartite state. Thus, $\alpha \neq 0$ and $\beta \neq \gamma$ and equating the partial derivatives of K_{II} to zero, we find

$$\alpha - 2\gamma = \pi/2 + I_1\pi; \quad 2\alpha - \beta - \gamma = \pi/2 + I_2\pi, \tag{2.26}$$

where I_1 and I_2 are integers. Solving eq. (2.26) gives us

$$3\gamma - \beta = -\pi/2 + I_3\pi; \quad I_3 = I_2 - 2I_1. \tag{2.27}$$

Thus a choice of one variable, say β determines all other angles. By defining the fidelity, $F = 1 - 2D$ (Scarani et al., 2006), such that the disturbance, D represent the probability that the measurement results from the same basis agree, we can see from Figure 2.1, a plot of the secure key rate for varying β (for simplicity we choose $I_1 = I_2 = 0$).

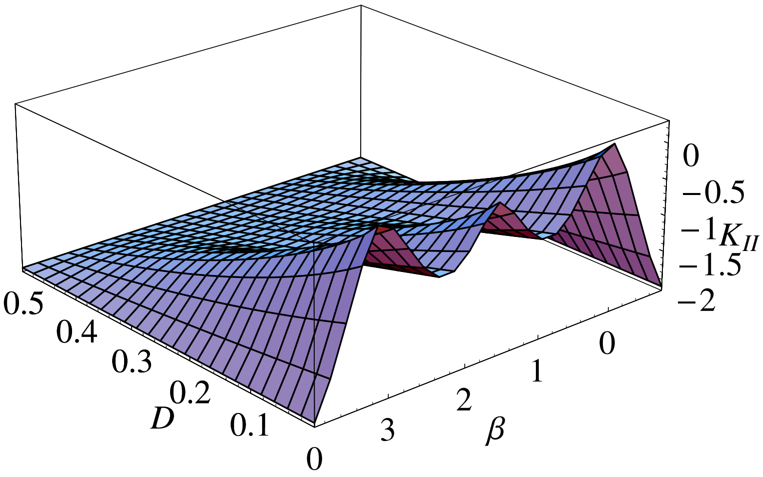

Figure 2.1 Key rate, K_{II} for varying β and D.

It is possible to consider a choice of values for I_1 and I_2 differently from 0. However, this would only force the value of the angles used by Alice and Bob to include some phase factor and affect Eve's information gain (which contains trigonometric functions of the angles). A maximal key rate then needs to be searched and identified for a possibly different value for β. We have in fact done a number of numerical search for a maximal key rate for such a scenario and found no advantage over the simpler choice of choose $I_1 = I_2 = 0$.

This can possibly be understood as follows: referring to eq. (2.26), we can absorb $I_1\pi$ into γ by introducing $\gamma' = \gamma + I_1\frac{\pi}{2}$. Then we consider using $\beta' = \beta - I_1\frac{\pi}{2} + I_2\pi$ resulting in a set of equations identical to eq. (2.26) and eq. (2.27) except for the substitution of γ and β with γ' and β' respectively and the terms related to I_1 and I_2 disappear (effectively eq. (2.26) and eq. (2.27) with $I_1 = I_2 = 0$). We can then imagine that Alice and Bob use the angles α, β' and γ' instead. The key rate formula thus is retained with no modification to the possible values of key rates achievable.

An analytical solution is unfortunately not immediate; and we plot a numerically optimized secure key rate in Figure 2.2. While it is the case that a different value for disturbance, D, would require a different set of angles used, this may be not too practical as one must commit to determining D prior to choosing the angles. It is possibly simpler to decide on one fixed value of β (thus the other angles as well) and derive a secure key for every possible D. We could simplify matters greatly by considering $\beta = 0$, and letting $I_1 = I_2 = 0$. We then have $\gamma = -\pi/6$ and $\alpha = \pi/6$.

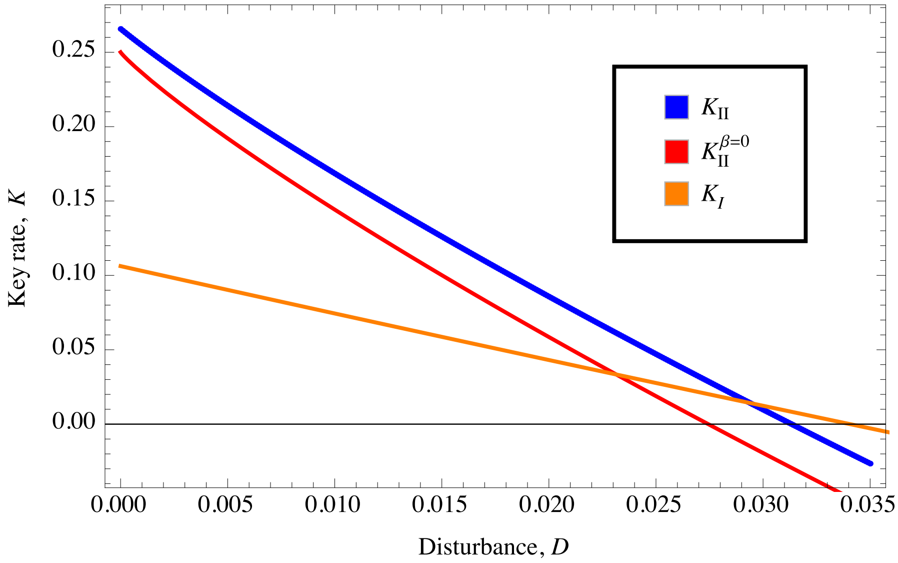

Figure 2.2 Key rate as a function of disturbance, D. (a) K_{II} represent numerically optimized key rate. (b) $K_{II}^{\beta=0}$ denote the extracted key rate given that $\beta = 0$. (c) K_I indicate the key rate achievable by CHSH protocol without postprocessing.

In order to show that a maximal key rate is in fact achievable with such angles for $\beta = 0$, we consider the Hessian matrix, $\mathcal{H}$ (Gradshteyn & Ryzhik, 2007) which is given by

$$\mathcal{H} = \begin{bmatrix} -2F & F \\ F & -2F \end{bmatrix}. \tag{2.28}$$

From eq. (2.28), the upper left element of the matrix, $\mathcal{H}$ gives $\frac{\partial^2 K_{II}}{\partial \alpha^2} = -2F$. We can then calculate the determinant of the Hessian matrix, $|\mathcal{H}|$ as

$$|\mathcal{H}| = (-2F)(-2F) - (F)(F) = 3F^2. \tag{2.29}$$

Since F does not take on a negative value and F^2 will always be positive then we can deduce that

$$\frac{\partial^2 K_{II}}{\partial \alpha^2} < 0; \quad |\mathcal{H}| > 0, \tag{2.30}$$

thus implying that a maximal key rate is achievable when $\gamma = -\pi/6$ and $\alpha = \pi/6$ given $\beta = 0$.

2.5 DISCUSSION

We compare the performance of the protocols of Version I and II in Figure 2.2. We can immediately observe that the protocol of Version II (for varying β and $\beta = 0$)

outperforms Version I for D up to about 3% and 2.4% respectively when the terms related to error correction (in terms of Alice-Bob mutual information) play a more prominent role in determining the maximal achievable key rate as opposed to privacy amplification. In general, this can be understood in the context of the legitimate parties making measurements to maximize correlations between them at the expense of determining the actual amount of local violation their bits are derived from.

On the other hand, for larger values of D, the information that Eve gleans from Bob becomes more pronounced for Version II; where Alice and Bob have little information on the type of correlation they actually share. We can in fact, in this vein, write an inequality to denote when the secure key rate of one protocol, K_{II} would exceed another, K_I in terms of the difference of mutual information between the protocols as follows

$$K_{II} > K_I \Rightarrow I_{AB}^{II} - I_{AB}^{I} > I_{BE}^{II} - I_{BE}^{I}, \tag{2.31}$$

where I_{AB}^{I} and I_{AB}^{II} are the mutual information between Alice-Bob for protocols I and II respectively while, I_{BE}^{I} and I_{BE}^{II} are Eve's information gain for protocols I and II respectively.

We see from Figure 2.3 in fact such an inequality holds only up to $D \approx 0.03$ where errors between the two legitimate parties become less important in determining the key rate as the difference between the two versions decrease while the difference in Eve's gain increases. The case for the protocol of Version II with $\beta = 0$ against Version I is similar and applying inequality of eq. (2.31) gives

$$1-\left(\frac{5+2\sqrt{2}}{4}\right)F < h\left(\frac{1-F}{2}\right)-h\left(\frac{2-\sqrt{2}F}{4}\right), \tag{2.32}$$

so long as $D < 2.4\%$ (this can be checked through simple numeric for eq. (2.32)). The fact that the protocol of Version II for varying β exceeds that of $\beta = 0$ is rather obvious from the fact that the former is based on the optimal choice for β.

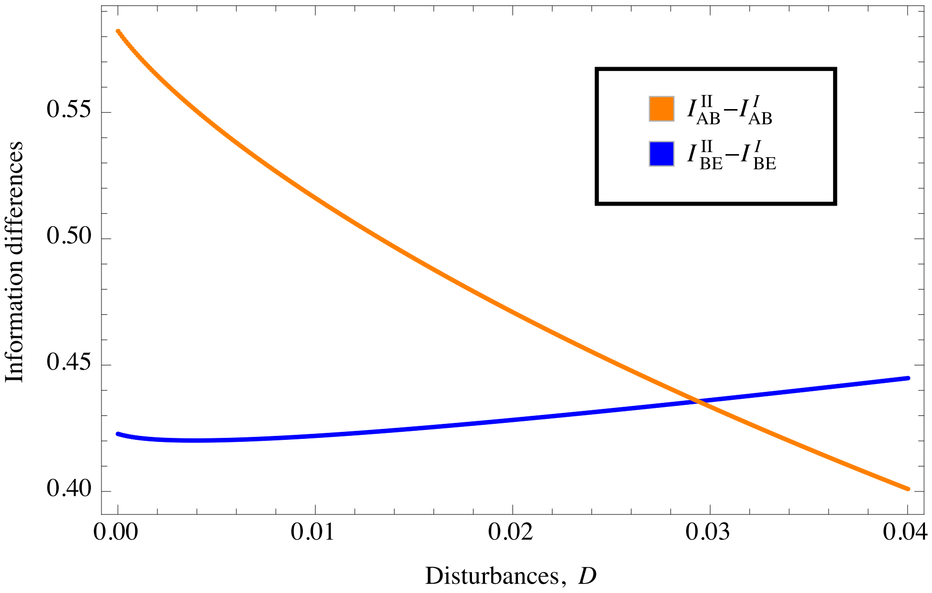

Figure 2.3 Differences of Alice-Bob mutual information (orange curve) and Eve information gain (blue curve) between the protocols of Version I and Version II (with varying β) versus D.

2.6 CONCLUSION

In the search for an ultimately secure key distribution procedure with the most pessimistic assumptions, protocols based on violating Bell inequalities were conceived. Limiting an adversary, Eve, with only the no-signaling principle while being supra-quantum still nevertheless allows for secure key distribution to be established. However, in this work we have noted that deriving a secure key and determining a Bell violation are clearly two incompatible processes; one can only be achieved maximally at the expense of the other and thus generating the most optimal secure key rate must necessarily capitalize on a possible trade-off.

In this work, we have considered two variants of a QKD protocol where the basic building block would really be two parties committing to measurements, each chosen from a set of two bases and each yielding binary results. Version I, which allows for the legitimate parties to make measurements with non overlapping bases and minimal disclosure of bases (by Alice only) provides for maximal determination of a Bell violation. This naturally results in the CHSH protocol (Scarani et al., 2006). It however, evidently sacrifices the actual correlation between the resulting shared raw key. Version II on the other hand allows for higher correlation between the shared raw key though at the expense of ascertaining a Bell violation; hence decreasing the legitimate parties' ability to determine how secure their key is from Eve and effectively resulting in more bits to be discarded in privacy amplification.

We have also used a simpler form of Version II by having a maximal correlation between Alice and Bob in one set of bases' choice (setting $\beta = 0$). On the whole, we note that Version II exceeds Version I for disturbance on the channel for up to about 3% and 2.4%, the latter is for the case $\beta = 0$. The latter may provide for ease for practical implementation due to having a fixed set of measurement bases for any disturbance on the channel while Version II on the whole is better suited for the low channel disturbance.

We should like to note that about a year after the completion and publication of this particular work we came upon a work by Hänggi, Renner, & Wolf (2010) that bears some semblance to ours considering a binary input-output device independent cryptosystem in which its security relies on nonlocal correlations and the assumption that the eavesdropper Eve is only restricted by the no-signaling postulate. However, we should note the difference nevertheless in our approach where we started off with measurement angles (α, β, γ) within a quantum scenario and then proceed to determine the measurement angles that would maximize Bell violation and those that maximize the bit correlation between the parties.

Moreover, we limit our study to the case where Eve distributes only two-party no-signaling correlation instead of a possible three-party scenario as in Hänggi et al. (2010). Our motivation comes from the fact that nonlocal three-party correlations result in outcomes for which two out of three parties are totally uncorrelated, resulting in the irreducibility of nonlocal three-party correlations to a two-party scenario using local operations (Barrett, Linden, et al., 2005).

CHAPTER THREE

DEVICE INDEPENDENT QUANTUM KEY DISTRIBUTION USING SINGLE PHOTON ENTANGLEMENT

3.1 PUBLICATION

The main findings reported in this chapter have been published in the journal Europhysics Letters, Volume 110, 20003 (2015) as Device-independent quantum key distribution using single-photon entanglement, with the citation: (2015) doi: 10.1209/0295-5075/110/20003. The authors for the publication are (in order as appears in the publication) Suhaili Kamaruddin and Jesni Shamsul Shaari.

3.2 INTRODUCTION

In the aforementioned device independent schemes, entanglement of at least two particles is used as the resource for nonlocality. However, the counterfactual phenomena is described within the context of a single photon entanglement, which can be demonstrated from a single photon incident on a beam splitter. In order to talk about counterfactual protocol in a device independent scenario, it is instructive to consider the use of single photon entanglement as a nonlocal resource. The possibility of utilizing the entanglement between a photon and a vacuum as a means for nonlocality was first proposed by Tan, Walls, & Collett (1991), which initially has been controversial at best. This issue, at any rate, seems to be settled following the discussion made by Van Enk (2005) and Dunningham & Vedral (2007) as pointed out by Wildfeuer & Dowling (2008) and later on shown experimentally in Pramanik, Adhikari, Majumdar, & Home (2012).

In this chapter, we will consider a QKD protocol based on nonlocality of a single particle originally proposed by Lee, Lee, Chung, Lee, & Kim (2003), where Alice and Bob, each can randomly choose to perform one of the two projective measurements on the entangled state of a single photon and the vacuum. Indeed, it is worth stressing that the entanglement is really between the particle number degrees of freedom in two spatial modes. The expectation value obtain from the measurements is then used to test for violation of a particular version of Bell inequality as in Peres (1995).

The general features of the protocol itself follows closely that of the previous chapter's where the legitimate parties would commit to a measurement that would maximize the correlation of the shared raw key. More specifically, it is the protocol of Version II of chapter 2 (the case where Alice and Bob use overlapping basis in one set of bases' choice). The measurement probes that we consider would be based on displacement operators as described in Banaszek & Wódkiewicz (1999) and in Wildfeuer & Dowling (2008) where the Clauser-Horne (CH) inequality (Clauser & Horne, 1974) is used to check for locality violation. Again, the protocol has the very interesting feature according to which no assumptions are made regarding the nature of measurements by Alice and Bob which can be seen as black boxes. We then present our analysis of security against individual attack within a device-independent scenario where Eve is constrained only by the no-signaling principle. Given the similarity in structure of the protocol to that of Version II of the previous chapter, the security analysis follows where Eve distributes a combination of deterministic as well as nonlocal strategies to the legitimate parties.

Before we proceed with the protocol, we will first review the quantum mechanical description of the beam splitters.

3.3 BEAM SPLITTER

We consider a beam splitter with two input and output ports as depicted in Figure 3.1. The two annihilation operators, $\hat{a}_2$ and $\hat{a}_3$ of the output fields are linearly related to the operators of the input field, $\hat{a}_0$ and $\hat{a}_1$ by

$$\begin{pmatrix} \hat{a}_2 \\ \hat{a}_3 \end{pmatrix} = U \begin{pmatrix} \hat{a}_0 \\ \hat{a}_1 \end{pmatrix}, \tag{3.1}$$

where we define the beam splitter transformation matrix, U as

$$U = \begin{pmatrix} t & r' \\ r & t' \end{pmatrix}, \tag{3.2}$$

with the element of the matrix, r and t being the respective reflectance and transmittance of the beam splitter. In order to determine the elements of U, we would assume that the beam splitter is lossless, which implies that the transformation matrix U is unitary. Hence, we would find that

$$|r'| = |r|, |t'| = |t|; \quad |r|^2 + |t|^2 = 1; \quad t^* r' + r^* t' = 0. \tag{3.3}$$

As long as eq. (3.3) holds, it can be seen that the operators of both the input and output fields satisfied the following commutation relations

$$\left[\hat{a}_i, \hat{a}_j^\dagger\right] = \delta_{ij}, \quad \left[\hat{a}_i, \hat{a}_j\right] = 0 = \left[\hat{a}_i^\dagger, \hat{a}_j^\dagger\right]. \tag{3.4}$$

Thus, the unitary matrix, U can be written as

$$U = \begin{pmatrix} \cos\theta & e^{i\varphi}\sin\theta \\ -e^{i\varphi}\sin\theta & \cos\theta \end{pmatrix}. \tag{3.5}$$

For $50:50$ beam splitter (i.e $\theta = \pi/4$) and phase shift, $\varphi = 0$, the beam splitter transformation matrix U can be represented as the Hadamard transformation matrix,

$$U = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}. \tag{3.6}$$

Indeed, it is worth noting that, other forms of U which correspond to different phase values are also used in the literature.

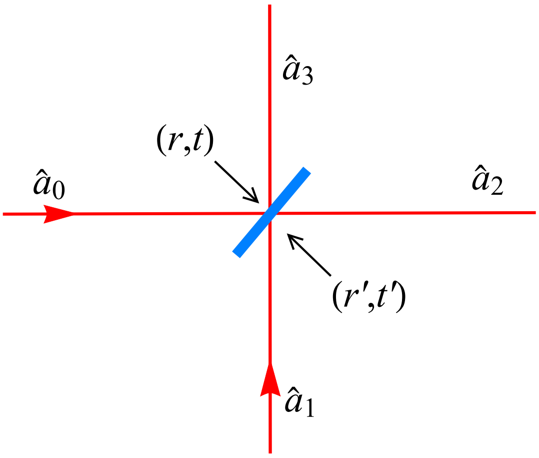

Figure 3.1 A representation of the input and output fields on a beam splitter in quantum mechanics.

Now, let us consider the case where a single photon incident in one of the input ports (say, mode 0) on the beam splitter. The single photon input state $|1\rangle_0 |0\rangle_1$, can be rewritten (in terms of the annihilation and creation operator) as $\hat{a}_0^\dagger |0\rangle_0 |0\rangle_1$. For the beam splitter described by eq. (3.6), we find that

$$\hat{a}_0^\dagger = \frac{1}{\sqrt{2}}\left(\hat{a}_2^\dagger - \hat{a}_3^\dagger\right), \tag{3.7}$$

$$\hat{a}_1^\dagger = \frac{1}{\sqrt{2}}\left(\hat{a}_2^\dagger + \hat{a}_3^\dagger\right). \tag{3.8}$$

Thus, using $|0\rangle_0 |0\rangle_1 \xrightarrow{BS} |0\rangle_2 |0\rangle_3$ we may write

$$\begin{aligned} |0\rangle_0 |0\rangle_1 &\xrightarrow{BS} \frac{1}{\sqrt{2}}\left(\hat{a}_2^\dagger - \hat{a}_3^\dagger\right)|0\rangle_2 |0\rangle_3 \\ &= \frac{1}{\sqrt{2}}\left(|1\rangle_2 |0\rangle_3 - |0\rangle_2 |1\rangle_3\right). \end{aligned} \tag{3.9}$$

3.3.1 Homodyne Detection

Let us consider a homodyne detection scheme as depicted in Figure 3.2. The method involves combining a signal field to be measured with a beam of strong coherent light $|\gamma\rangle$, also called local oscillator, using a beam splitter. The superimposed light can be described by the beam splitter transformation of eq. (3.6). Basically, a homodyne detection scheme can be divided into two types, that is, balanced and unbalanced homodyne detection scheme.

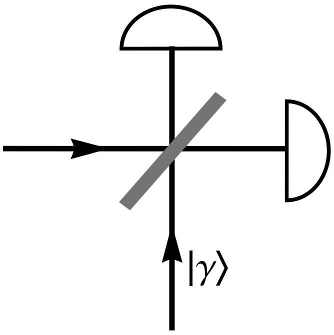

Figure 3.2 A representation of a homodyne detection scheme.

A balanced homodyne detection scheme is such that the signal interferes with local oscillator at a well-balanced 50:50 beam splitter which results in all four ports being used. Meanwhile, the beam splitter of an unbalanced homodyning is characterized such that $|r| << |t|$, which leads to only three out of four ports being used. In the limit $t \to 1$ and $\gamma \to \infty$, the effect of the beam splitter is described by the coherent displacement operator

$$\hat{D}(\alpha) = \mathrm{e}^{-\frac{1}{2}|\alpha|^2} \mathrm{e}^{\alpha \hat{a}^\dagger} \mathrm{e}^{-\alpha^* \hat{a}}, \tag{3.10}$$

expressed in terms of the photon creation and annihilation operator, $\hat{a}^\dagger$ and $\hat{a}$ as well as the coherent displacement $\alpha = \gamma\sqrt{1-T}$ where T denotes the transmissivity of the beam splitter.

3.4 THE PROTOCOL

We consider a single photon entanglement protocol and denote it as SDI protocol. In the protocol, we suppose that Alice and Bob share a quantum channel consisting of a light source (LS) that emits a single photon. The single photon passes through a 50:50 beam splitter (BS), which may be represented by a Hadamard transformation of the input modes, consisting of a single photon and a vacuum state (Agarwal, 2013), resulting in a state given by

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|1\rangle_A|0\rangle_B - |0\rangle_A|1\rangle_B\right), \tag{3.11}$$

where the path accessible to Alice and Bob are represented by mode A and B, respectively. We require both parties to commit to measurements where the measurement setting in each of the mode consists of a BS and a photon detector where a strong coherent state $|\gamma\rangle$ is injected into the second input port of the BS (see Figure 3.3).

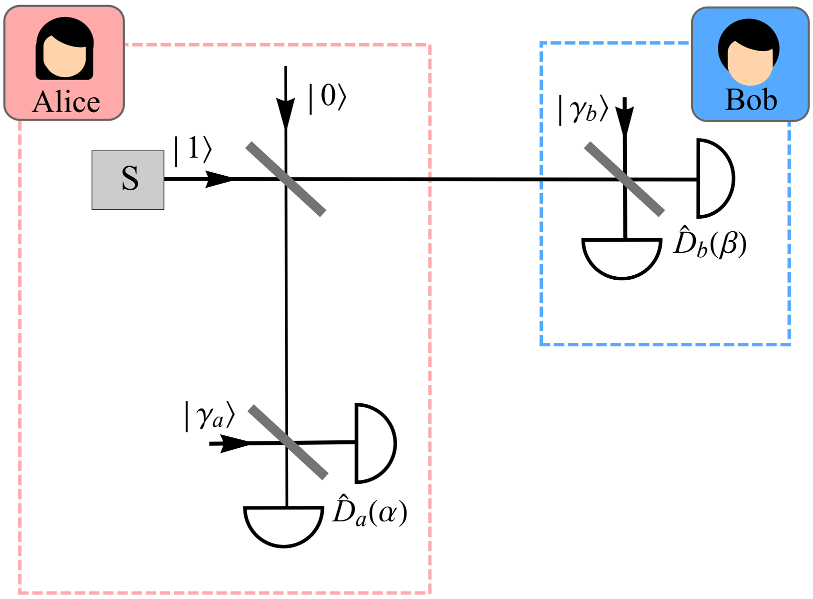

Figure 3.3 A schematic diagram of the proposed protocol where the single photon entanglement source is under Alice's control and measurement apparatuses are trusted.

The measurement operators depending on the coherent displacement α are described by

$$\hat{Q}(\alpha) = \hat{D}(\alpha)\left|0\right\rangle\left\langle 0\right|\hat{D}^{\dagger}(\alpha), \tag{3.12}$$

$$\hat{P}(\alpha) = \hat{D}(\alpha)\sum_{n=1}^{\infty}\left|n\right\rangle\left\langle n\right|\hat{D}^{\dagger}(\alpha). \tag{3.13}$$

Here, the operators $\hat{Q}(\alpha)$ and $\hat{P}(\alpha)$ would give the probabilities for the absence and presence of photon(s), respectively, with $\hat{Q}(\alpha)+\hat{P}(\alpha)=\hat{\mathbf{1}}$ where $\hat{\mathbf{1}}$ is the identity operator. In what follows, we shall identify the measurement operators on Alice's side with $\hat{Q}_A(\alpha)$ and $\hat{P}_A(\alpha)$ while Bob's with $\hat{Q}_B(\beta)$ and $\hat{P}_B(\beta)$ in which α and β are the coherent displacements correspond to Alice's and Bob's measurement operator, respectively.

Given a quantum state, say ρ, we can calculate the expectation values of the measurement operators to determine the probability of each events happening. As in this case where $\rho=\left|\Psi\right\rangle\left\langle\Psi\right|$, the probability of Alice's detector clicking when Bob's detector does not click, $Q_A P_B(\alpha,\beta,\rho)$ can be obtain from

$$\begin{aligned} Q_A P_B(\alpha,\beta,\rho) &= \mathrm{tr}\left(\hat{Q}_A(\alpha)\otimes\hat{P}_B(\beta)\,\rho\right), \\ &= \frac{1}{2}\mathrm{e}^{-|\alpha|^2}\left(|\alpha|^2+1-|\alpha-\beta|^2\,\mathrm{e}^{-|\beta|^2}\right), \end{aligned} \tag{3.14}$$

while the probability of Bob's detector clicking when Alice's detector does not click, $P_A Q_B(\alpha,\beta,\rho)$ is

$$\begin{aligned} P_A Q_B(\alpha,\beta,\rho) &= \mathrm{tr}\left(\hat{P}_A(\alpha)\otimes\hat{Q}_B(\beta)\,\rho\right), \\ &= \frac{1}{2}\mathrm{e}^{-|\beta|^2}\left(|\beta|^2+1-|\alpha-\beta|^2\,\mathrm{e}^{-|\alpha|^2}\right), \end{aligned} \tag{3.15}$$

in which α and β are the coherent displacements for mode A and B, respectively. In the instances where no photon registration in detectors of both sides, the joint probability distribution, $Q_{AB}(\alpha,\beta,\rho)$ is given by

$$\begin{aligned} Q_{AB}(\alpha,\beta,\rho) &= \mathrm{tr}\left(\hat{Q}_A(\alpha)\otimes\hat{Q}_B(\beta)\,\rho\right), \\ &= \frac{1}{2}\mathrm{e}^{-|\alpha|^2-|\beta|^2}\,|\alpha-\beta|^2, \end{aligned} \tag{3.16}$$

with the marginal probabilities of no photon count in each modes are

$$\begin{aligned} Q_A(\alpha,\rho) &= \mathrm{tr}\left(\hat{Q}_A(\alpha)\otimes\hat{\mathbf{1}}_B\,\rho\right), \\ &= \frac{1}{2}\left(|\alpha|^2+1\right)\mathrm{e}^{-|\alpha|^2}, \end{aligned} \tag{3.17}$$

$$\begin{aligned} Q_B(\beta,\rho) &= \mathrm{tr}\left(\hat{\mathbf{1}}_A\otimes\hat{Q}_B(\beta)\rho\right), \\ &= \frac{1}{2}\left(|\beta|^2+1\right)\mathrm{e}^{-|\beta|^2}. \end{aligned} \tag{3.18}$$

The measurements taking place in both settings are performed when Alice randomly chooses between two possible values of $\alpha\in\{0,s\}$, and Bob between two possible values of $\beta\in\{0,-s\}$ denoting their measurement 'bases'. In the events where Alice and Bob happen to choose $\alpha = 0$ and $\beta = 0$, respectively, it can be easily shown that for the state $\rho = |\Psi\rangle\langle\Psi|$, eq. (3.14) and eq. (3.15) thus amount to

$$Q_A P_B(0,0,\rho) = P_A Q_B(0,0,\rho) = \frac{1}{2}. \tag{3.19}$$

Assigning the logical value '0' ('1') to the event only Alice's (Bob's) detector clicks, it is clear that Alice and Bob can share a string of bits. To determine its secrecy, they need to assure themselves that the results of their measurements are in fact derived from the measurements on the state $|\Psi\rangle$ rather than some predetermined states. Thus they can resort to checking for a particular Bell violation, i.e. the Clauser-Horne (CH) inequality (Clauser & Horne, 1974), by determining the expectation value, $\langle CH \rangle$ given as:

$$\begin{aligned}\langle CH \rangle = {} & Q_{AB}(0,0,\rho) + Q_{AB}(s,0,\rho) + Q_{AB}(0,-s,\rho) \\ & - Q_{AB}(s,-s,\rho) - Q_A(0,\rho) - Q_B(0,\rho).\end{aligned} \tag{3.20}$$

Note that the nonlocality is satisfied if eq. (3.20) violates inequality $-1 \le \langle CH \rangle \le 0$. It has been shown in Banaszek & Wódkiewicz (1999) that a maximal violation happens for $\alpha = -\beta \approx 0.5$, a value that can be obtained by minimizing eq. (3.20).

The protocol can now be summarized as follows:

1. Alice and Bob measure states by choosing $\alpha \in \{0, s\}$ and $\beta \in \{0, -s\}$ (s is optimal value for maximal CH violation).

2. At the end of transmission and measurement of all quantum states, Alice and Bob would reveal over a public channel their measurement bases.
3. A subset for the measurement results where Alice and Bob both chose $\alpha = \beta = 0$ along with the other measurement settings (each randomly selected) would be revealed for bit error and $\langle CH \rangle$ value estimation.
4. The remaining subset for $\alpha = \beta = 0$ would be used as a raw key.
5. Based on step 3. above, Alice and Bob may execute error correction and privacy amplification to distill a secret key.

3.5 INDIVIDUAL ATTACK FROM SUPRA QUANTUM ADVERSARY

We assume the worst case scenario as depicted in Figure 3.4, in which Alice and Bob are each given access to a black box and the source is controlled by Eve instead of carrying out the illustrated operation in Figure 3.4.

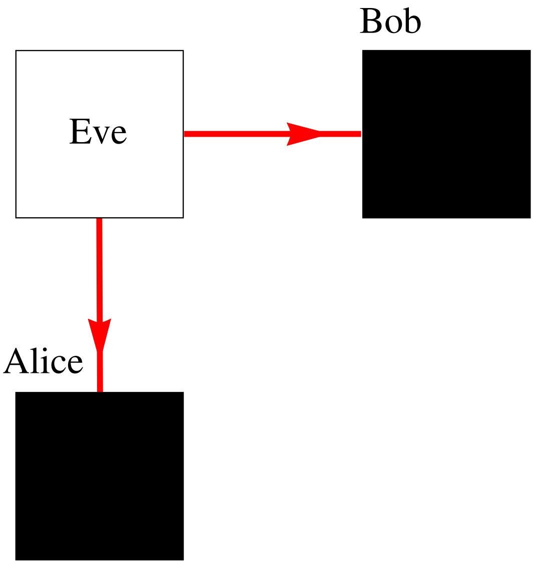

Figure 3.4 A schematic representation of Figure 3.3 in the device-independent scenario where Alice's and Bob's measurement apparatuses are deemed as black boxes and the source is controlled by Eve.

In ascertaining the secrecy of the protocol, we shall consider the case where Eve is supra-quantum, i.e. she is not limited by quantum physics though constrained by the no-signaling principle. While the protocol described above makes use of nontraceless measurement operators and results in a different range of values for a CH violation compared to the standard Werner state scenario with a standard spin correlation measurement (Wildfeuer & Dowling, 2008), the measurements nevertheless do yield binary outcomes. Hence, the protocol is effectively a case in which Alice and Bob both make binary measurements with each measurement resulting in binary outcomes. This allows for the consideration of an individual attack scenario where Eve can be seen as sending to the legitimate parties a mixture of deterministic strategies plus a nonlocal box. The nonlocal box itself can be chosen to violate the inequality at its algebraic maximum such that even a fraction used may nevertheless give Alice and Bob the impression that they are actually measuring maximally entangled states.

As in Chapter 2, we shall resort to the use of the aPR box (Skrzypczyk & Brunner, 2009), which would violate the CH inequality up to its maximal algebraic on the negative side of the $\langle CH \rangle$ range (as opposed to the PR box which violates the inequalities on the positive side). We referred to the aPR box of eq. (2.7), where $\Pr_{aPR}(ab\,|\,xy) = \frac{1}{2}$ for $a + b = xy \oplus 1$ and $\Pr_{aPR}(ab\,|\,xy) = 0$, otherwise. In consideration of the protocol described in the previous section, the binary inputs $x = 0,1$ and $y = 0,1$ would correspond to the coherent displacements of the measurement operators $\alpha = 0,s$ and $\beta = 0,-s$, respectively. The binary outputs for a,b each as 0 or 1 would correspond to ``no photons” or ``photon present”, respectively. Here, we again use the four deterministic function $G:\left[4\right]\times\left\{0,1\right\}\rightarrow\left\{0,1\right\}$ for $r = 1,2,3,4$ as defined by eq. (2.8). Of the sixteen possible strategies described by eq. (2.9), the eight that are of interest would be the $\mathbf{D}_{12},\mathbf{D}_{14},\mathbf{D}_{21},\mathbf{D}_{23},\mathbf{D}_{32},\mathbf{D}_{33},\mathbf{D}_{41},\mathbf{D}_{44}$, which saturate the local bound on the negative side of the $\langle CH\rangle$ range. We denote p_{ij} as the probability of Eve sending strategy $\mathbf{D}_{ij}$ and p_{NL} the probability of sending the aPR box.

We can see from Table 3.1 that Alice and Bob would share a raw key for $x=y=0$ (more specifically $\alpha=\beta=0$) with probability $p_{NL}+p_D$, where $p_D = p_{12}+p_{14}+p_{32}+p_{21}+p_{23}+p_{41}$ and the fraction of error in the key, p_e is given by $p_e = p_{33}+p_{44}$. With the aPR box violating the CH inequality up to a value of -1.5, the value Alice and Bob may find for their estimation of local violation, $\langle CH\rangle$ would be

$$\langle CH\rangle \geq -1.5\left[1-(p_D+p_e)\right]+(-1)(p_D+p_e). \tag{3.21}$$

Table 3.1 Table showing probability distribution of Eve sending the corresponding strategy (as shown in the parentheses) to Alice and Bob for $x=y=0$. Note that this table is a part of Table 2.2 in previous chapter.

	$y=0,b=0$	$y=0,b=1$
$x=0,a=0$	$p_{33}(\mathbf{D}_{33})$	$p_{NL}/2(P_{aPR})$ $p_{12}(\mathbf{D}_{12})$ $p_{14}(\mathbf{D}_{14})$ $p_{32}(\mathbf{D}_{32})$
$x=0,a=1$	$p_{NL}/2(P_{aPR})$ $p_{21}(\mathbf{D}_{21})$ $p_{23}(\mathbf{D}_{23})$ $p_{41}(\mathbf{D}_{41})$	$p_{44}(\mathbf{D}_{44})$

In what follows, we would consider the case where Eve provides for a scenario that Alice and Bob would expect from quantum theory. Hence, they would imagine that the shared quantum channel is noisy and the single-photon entangled state of eq. (3.11) is transformed into a Werner-like state, ρ (Wildfeuer & Dowling, 2008):

$$\rho = F\left|\Psi\right\rangle\left\langle\Psi\right| + (1-F)\frac{I}{4}, \tag{3.22}$$

with fidelity, $F=1$ represent the noise-free condition in which $0 \le F \le 1$. The joint probability distribution of no photon registration events in both detectors, $Q_{AB}(\alpha,\beta,\rho)$ is now given as

$$\begin{aligned} Q_{AB}(\alpha,\beta,\rho) = {} & \frac{F}{2}\mathrm{e}^{-|\alpha|^2-|\beta|^2}\left|\alpha-\beta\right|^2 \\ & + \frac{1-F}{4}\mathrm{e}^{-|\alpha|^2-|\beta|^2}\left(1+|\alpha|^2+|\beta|^2+|\alpha|^2|\beta|^2\right), \end{aligned} \tag{3.23}$$

where α and β are the coherent displacements for mode A and B, respectively.

The probability of Alice's detector clicking when Bob's detector does not click and vice versa with $\alpha = \beta = 0$ is given by

$$Q_A P_B(0,0,\rho) = P_A Q_B(0,0,\rho) = \frac{1}{2} - \frac{1-F}{4}. \tag{3.24}$$

Thus error, p_e should be given by

$$p_e = 1 - Q_A P_B(0,0,\rho) - P_A Q_B(0,0,\rho) = \frac{1-F}{2}. \tag{3.25}$$

With $\alpha = -\beta = s$, an estimation of CH, $\langle CH \rangle$ can be shown to be

$$\begin{aligned}\langle CH \rangle = \frac{1}{4}\mathrm{e}^{-2s^2}(-\mathrm{e}^{2s^2}(3+F) - (1+s^2)^2 + F(1-6s^2+s^4) \\ +2\mathrm{e}^{s^2}(1+s^2+F(-1+s^2))).\end{aligned} \tag{3.26}$$

Rearranging eq. (3.26) gives us F in terms of $\langle CH \rangle$ as follows

$$F = \frac{-4\langle CH \rangle \mathrm{e}^{2s^2} - s^4 + 2\mathrm{e}^{s^2}s^2 - 2s^2 + 2\mathrm{e}^{s^2} - 3\mathrm{e}^{2s^2} - 1}{-s^4 - 2\mathrm{e}^{s^2}s^2 + 6s^2 + 2\mathrm{e}^{s^2} + \mathrm{e}^{2s^2} - 1}. \tag{3.27}$$

To ensure that the error p_e in the key would correspond to the CH violation (or lack of it), Eve needs to decide the amount of information she would want to gain, $I_{AE} = p_D + p_e$. This defines the value of $\langle CH \rangle$ Alice and Bob would measure. Writing p_e in terms of $\langle CH \rangle$, Eve can easily determine the amount of p_e and p_D she should commit to subject to the constraint

$$p_D + p_e \leq 2\left(\langle CH \rangle_{\max} + 1.5\right), \tag{3.28}$$

where $\langle CH \rangle_{\max}$ represent the maximal CH violation. However, care must be taken with respect to the value for p_D, as a strategy which sets $p_D = 1$ would result in no

Bell violation without errors, and would not meet Alice's and Bob's expectation for an error free channel.

From eq. (3.25) and eq. (3.27), we can rewrite the error, p_e in term of the CH violation, $\langle CH \rangle$ as

$$p_e = \frac{2\left((\langle CH \rangle + 1)\mathrm{e}^{2s^2} - \mathrm{e}^{s^2}s^2 + 2s^2\right)}{-s^4 + 6s^2 + \mathrm{e}^{2s^2} - 2\mathrm{e}^{s^2}(s^2 - 1) - 1}. \tag{3.29}$$

Applying the Csiszár-Körner theorem, the key rate formula, K can be written as

$$K = 1 - I_{AE} - h(p_e). \tag{3.30}$$

Given that Eve's information gain, $I_{AE} = p_D + p_e$ and inequality (3.21), we can then rewrite the key rate formula of eq. (3.30) as

$$K \geq 1 - 2\left(\langle CH \rangle + 1.5\right) - h(p_e). \tag{3.31}$$

Inserting eq. (3.29) into eq. (3.31), we can have the achievable key rate shown as the solid curve in Figure 3.5 Figure with the maximum key rate obtained being approximately 0.22 for zero error rate ($F = 1$) and greater than zero for a CH violation up to about -1.08. This is greater than CHSH protocol (Acín, Gisin, et al., 2006; Scarani et al., 2006) for error free scenario (given isotropic distribution) of only about 0.12 though lesser than Acín, Massar, et al. (2006) at about 0.414.

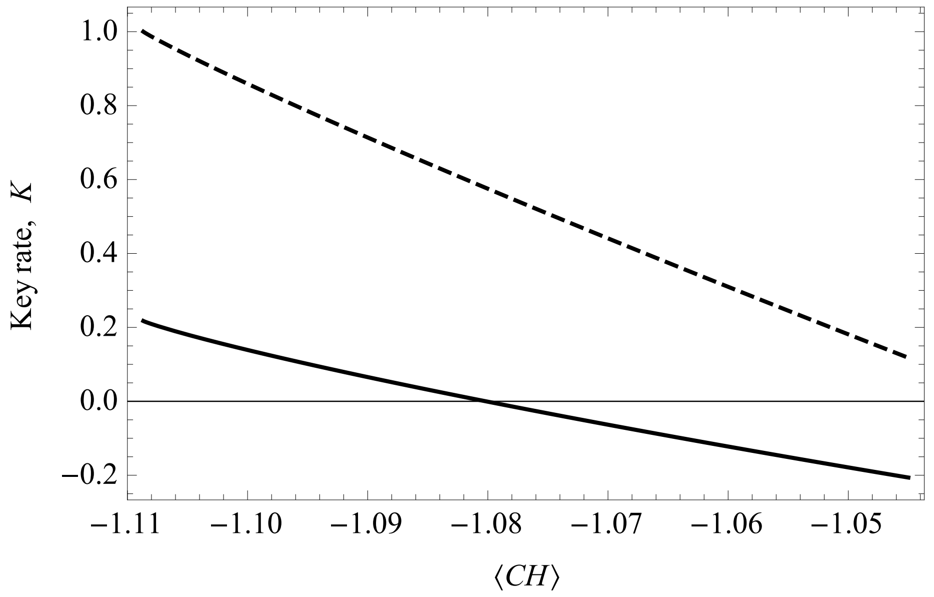

Figure 3.5 Key rate as a function of CH violation. The solid curve represents the achievable key rate in what would be expected by Alice and Bob in a quantum scenario provided by the no-signaling Eve, while the dashed line corresponds to the case of a quantum Eve and trusted devices.

We could consider a more optimistic scenario, where Eve is in fact constrained to quantum physics while the legitimate parties trust their devices. Hence, Eve would be seen distributing maximally entangled states instead of aPR boxes and separable ones for deterministic strategies. The measurement on the maximally entangled states, with regard to overlapping measurement basis used in key extraction, violates the CH inequality up to $\xi_q \approx -1.108$. Thus, the estimation of local violation $\langle CH \rangle$ that the legitimate parties would find is

$$\langle CH \rangle \geq \xi_q \left[1-(p_D+p_e)\right]+(-1)(p_D+p_e). \tag{3.32}$$

With Eve's information gain, $I_{AE}=p_D+p_e$ and eq. (3.32), the key rate formula of eq. (3.30) gives the dashed curve in Figure 3.5 for distillable secret key.

Even here, at least for a noiseless channel, the achievable key rate of unity is better when compared to the CHSH protocol (about 0.4) under trusted conditions. This is mainly due to the fact that unlike the CHSH protocol, the SDI protocol does not suffer from issues of non overlapping measurement basis for key extraction purpose. It is possible to consider the statistics of the individual terms of eq. (3.20) for a Werner-like state and let Eve's attack to be further constrained so as these would be true. However, without doing so, we would thus limit ourselves to the minimal consideration to ensure a secret key could be derived.

3.5.1 Decoupling; a non quantum picture

In this short subsection, we consider relaxing the requirement, that is, Eve is not required to provide a scenario that is expected by Alice and Bob from a quantum theory.

It is worth noting that, with respect to Table 3.1, strategies inducing errors are essentially decoupled from error-free strategies; i.e. Eve can choose *not to* induce any error by simply not sending the $\mathbf{D}_{33}$ and $\mathbf{D}_{44}$ strategies. On the other hand, should she choose to introduce errors, she would very well decrease the correlation in Alice's and Bob's strings which need to be subjected to error correction without penalizing her own information gain, which is maximal whenever she sends deterministic strategies. The key rate given in eq. (3.30) is necessarily a function of both the estimation of local violation, $\langle CH \rangle$ and error rate, p_e (refer to Figure 3.6). The former is to ensure that the legitimate parties have some correlations derived from nonlocal resources while the latter is necessary for error correction purposes. Such a feature is actually not at all surprising and is ultimately the result of using overlapping basis measurements for key generation purposes.

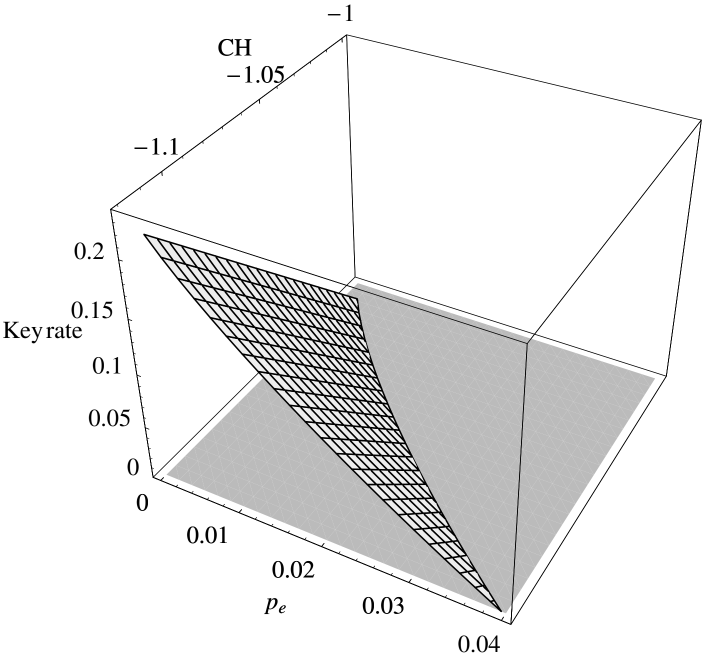

Figure 3.6 Key rate as a function of error rate, p_e and estimation of local violation, CH.

As an example, if we imagine a protocol where Alice and Bob commit to measurements in the bases A_i and B_i respectively for $i = 1,...,n$. With measurements on a maximally entangled state and $\Pr(a_k = b_k \mid A_k B_k) = 1$ for a particular k, while the other $n-1$ measurements are used for estimating some Bell violation, an eavesdropper could always send deterministic strategies corresponding to eigenstates of the measurement operators of A_k and B_k to ensure Alice and Bob would always get correlated results. The case for overlapping bases measurements that result in anti-correlations between Alice and Bob instead would be completely equivalent.

In such a noise free scenario, the key derived is completely insecure. This is why the 'Ekert' like protocol in Acín, Massar, et al. (2006) using only one overlapping measurement basis between Alice and Bob to derive a key requires a combination of sufficient statistics to ensure a Bell violation along with the key rate given. On its own, the key rate formula (which can be effectively written only as a function of errors) does not provide for a secure key. Such freedom on Eve's side however may not spell for a very useful scenario. A quick example is if we assume that Eve makes use of an isotropic distribution in describing her strategies; with $p_e = (1 - p_{NL})/4$, it can be shown that no positive key rate may be gained despite a maximal CH violation. This would be counterintuitive to Alice and Bob who would imagine that a maximal violation can only be the result of a noiseless channel.

3.6 CONCLUSION

In this chapter, we have analyzed a QKD protocol relying on the nonlocality features of a single particle to demonstrate its security within a device independent context. Regardless of how the protocol is illustrated, the security analysis assumes that the legitimate parties are up against an individual attack strategy prepared by an eavesdropper limited only by the no signaling principle. We have shown that a secret key can be extracted from a mixture of deterministic strategies and a nonlocal one i.e anti-PR box distributed by Eve.

In presenting a reference for realistic settings where errors in the key should imply a decrease in the CH violation (as would be true if dealing with a Werner like state), we considered the case where Eve prepared a scenario that would be expected by Alice and Bob from quantum theory. In this scenario, Eve has the freedom to determine the amount of her information gain, I_{AE} which must always satisfy the constraint $p_D + p_e \le 2\left(\langle CH \rangle_{\max} + 1.5\right)$. As long as this holds, it represents the minimal consideration for parameters to be estimated by the legitimate parties in a realistic scenario for sufficiency to assume access to a Werner like state without compromising security. We show that a positive key rate may be obtained for a CH violation up to -1.08.

Given the overlapping measurement basis, we also note how Eve's strategy decouples the error induced from meaningful information gain on her side. It thus becomes essential for the key rate to be described in terms of both local violation and error rate; while the latter is essential in determining the amount of correlation between Alice's and Bob's raw keys, without the former, there is no guarantee for the secrecy of the key.

CHAPTER FOUR

DEVICE INDEPENDENT COUNTERFACTUAL QUANTUM KEY DISTRIBUTION

4.1 INTRODUCTION

While CQKD gives the picture of a secure protocol where no signal is effectively sent between the legitimate parties, the basis for the protocol is really the quantum phenomena of entanglement, in this case, between a polarized photon and the vacuum. Entanglement which can be viewed as the source of the nonlocal nature of quantum theory is however not verified in the protocol and this begs the question if the entire protocol can be simulated by a setup which does not require the use of entanglement. This is our starting point for understanding the possible security that can be achieved within a device independent framework.

Stressing the fact that such a framework represents an extremely pessimistic stand where the very apparatus used by the legitimate parties could in principle be constructed by Eve (for her benefit), like the earlier chapters, we consider an eavesdropper who would be supra-quantum in the sense that she has access to nonlocal correlations that go beyond afforded by quantum physics, limited only by the no-signaling principle.

In the following, we will show that given the device independent framework for secrecy, the CQKD as proposed by Noh (2009) is in fact completely insecure. Though actually this is the case even if Eve is limited only by quantum physics. We propose a setup for which would be considered as black boxes for Alice and Bob to completely simulate the expected statistics of the CQKD while allowing Eve to have full knowledge of the shared key. The setup would consist of only separable systems as signals and we further show that protocol fails even in the case of entangled sources. Given that, we identify the essential source of insecurity and propose a modification and subsequently a proper CQKD, which would be secure within a device independent framework.

4.2 COUNTERFACTUAL PROTOCOL

Let us begin with a description of the counterfactual protocol in reference to the protocol of Li (2014). It must be noted that this description is completely equivalent to the one proposed by Noh (2009); though it has, to a certain extent, some simplicity in its description. We imagine that two parties, say Alice and Bob, share a setup as depicted in Figure 4.1.

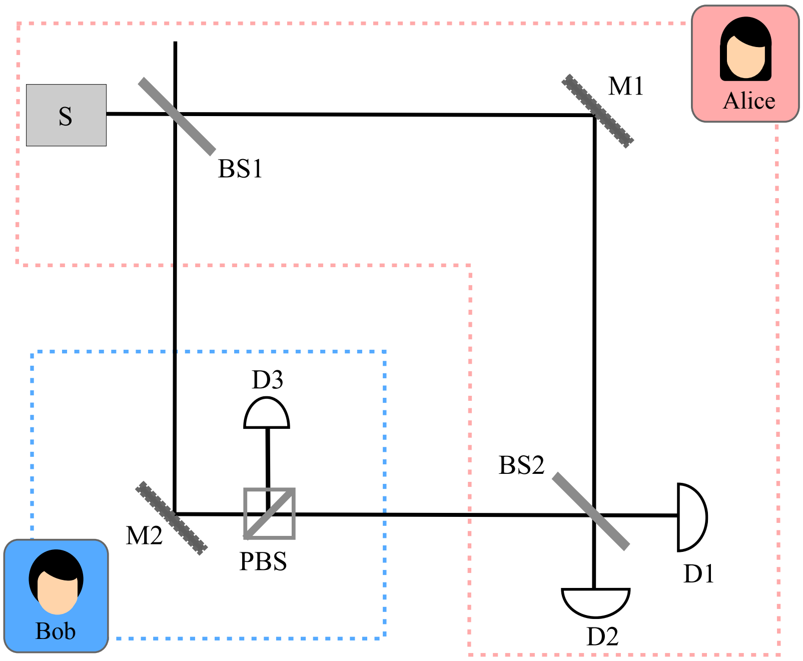

Figure 4.1 A diagram of counterfactual protocol proposed by Li (2014). BS1 and BS2 are beam splitters, D1, D2 and D3 are detectors, M1 and M2 are mirrors and PBS is a polarizing beam splitter.

The protocol starts when Alice triggers the photon source (S) that emits a pulse containing a single-photon. Depending on Alice's random choices, the single-photon could be in either horizontally polarized state $|H\rangle$, which represent Alice's bit ‘0’ or vertically polarized state $|V\rangle$ as bit ‘1’. The single-photon pulse passes through a 50:50 beam splitter (BS1) in which the output results in either one of the following states (in accordance with Alice’s choice of polarization state):

$$|\Psi\rangle_H = \frac{1}{\sqrt{2}}\left(|H\rangle_A|0\rangle_B - |0\rangle_A|H\rangle_B\right), \tag{4.1}$$

$$|\Psi\rangle_V = \frac{1}{\sqrt{2}}\left(|V\rangle_A|0\rangle_B - |0\rangle_A|V\rangle_B\right), \tag{4.2}$$

where $|0\rangle_i$ denotes the vacuum state with $i \in A, B$ represent the path towards Alice’s mirror M1 and Bob’s site, respectively. We further denote the paths A, B_1 and B_2 for the paths from the source towards M1, from the beam splitter BS1 to the mirror M2 and from M2 to BS2 respectively.

The pulse that travels through path B is reflected by M2 before entering the input port of the polarizing beam splitter (PBS) on Bob’s site. Bob will randomly choose between horizontal and vertical polarization to represent his bit. The PBS is configured such that, if Bob’s choice of polarization is not equal to Alice, the PBS will transmit the pulse towards BS2 and the split pulse that travels in the two modes are recombined at beam splitter, BS2. In an ideal setting, the interference effect will cause the photon to be detected at D1 with certainty. However, if the incoming polarization is the same with Bob’s choice, the pulse will be reflected towards Bob’s measurement setting, which consists of photon detector, D3. The measurement process will cause the state $\left|\Psi\right\rangle_H$ to collapse to either $\left|H\right\rangle_A\left|0\right\rangle_B$ or $\left|0\right\rangle_A\left|H\right\rangle_B$; or state $\left|\Psi\right\rangle_V$ to either $\left|V\right\rangle_A\left|0\right\rangle_B$ or $\left|0\right\rangle_A\left|V\right\rangle_B$, which eventually destroys the interference.

In the event that the state collapses to either $\left|H\right\rangle_A\left|0\right\rangle_B$ or $\left|V\right\rangle_A\left|0\right\rangle_B$ the detector D1 and D2 in Alice's site will click with equal probability. On the other hand, if the state collapses to either $\left|0\right\rangle_A\left|H\right\rangle_B$ or $\left|0\right\rangle_A\left|V\right\rangle_B$, the detector D3 will click with certainty. At the end of transmission, Alice and Bob will reveal which of their detectors click. The case of detector D3 clicking implies that Alice gets nothing, while a click of either D1 or D2 implies that Bob effectively did not receive a photon. As D1 also clicks in the case of an interference, only the click at D2 provides Alice with a conclusive guess of Bob's choice of polarization. Thus the raw key will be extracted from the event in which detector D2 clicks.

4.2.1 Security Analysis and Black Boxes

In this section, we will describe the counterfactual protocol within a device independent scenario in which Alice and Bob are provided with untrusted devices and they have no knowledge of the internal function of the QKD devices. The adversary may configure the devices such that they will simulate the results that would be obtained from executing a counterfactual QKD protocol as described above.

In what follows, we can view these devices as black boxes (`A' for Alice and `B' for Bob) each provided with binary input, say a `H' and a `V' button as potrayed in Figure 4.2. For definiteness, we define `H' as bit `0' and `V' as bit `1'. We further consider two different strategies by Eve in determining how the black boxes should behave. In either case, Eve would be distributing tripartite states to Alice and Bob, though in the first strategy, the states between Alice and Bob are completely separable and the second, an entangled bipartite state is separable from a (relevant) third polarized state.

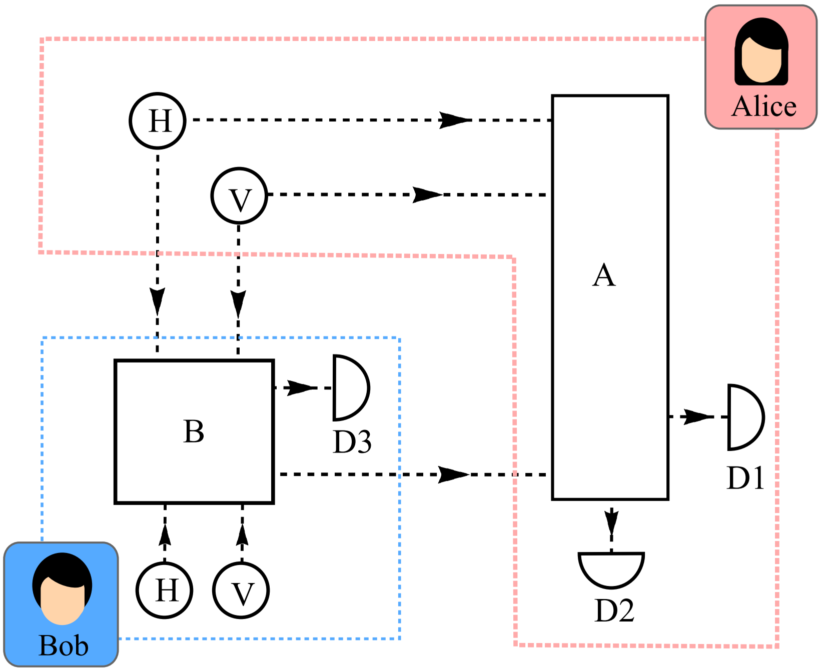

Figure 4.2 A schematic diagram of the proposed protocol.

4.2.1.1 CQKD with separable states

Let us now propose a protocol by prescribing requirements of how the boxes should behave in order to replicate the effects of the counterfactual QKD.

Suppose Alice chooses to click one of the buttons; instead of sending a polarized state to a beam splitter as in the actual counterfactual QKD, the state that is really being distributed is a three-qubit state, either:

$$|0\rangle_A|1\rangle_B|m\rangle_B \quad \text{or} \quad |1\rangle_A|0\rangle_B|m\rangle_B, \tag{4.3}$$

where $m \in \{H,V\}$ depends on Alice's choice of a button and the subscript A and B represent the qubit that is being distributed to Alice and Bob, respectively. While we do not make any requirement on state $|m\rangle_B$ to be a polarized state we nevertheless assume so in what follows for the sake of simplicity. The two-qubit state (either $|1\rangle_B|m\rangle_B$ or $|0\rangle_B|m\rangle_B$) would then be sent to Bob's box, B. Bob will also randomly choose between his `H' or `V' button.

At first glance, it may seem as if information is leaked out of Alice's site by sending the state $|m\rangle_B$ over to Bob. However, in a counterfactual perspective, it is crucial that the state $|m\rangle_B$ i.e the polarization degree of freedom to be accessible to Bob otherwise the PBS cannot work. Eve would eventually know the values of m as she can make a measurement to distinguish the two polarization states perfectly. Based on the choices made by Alice and Bob, we will consider the following two cases.

Case 1: Alice's and Bob's bit do not match. Bob's device will resend the second qubit to Alice's site. This qubit along with her qubit would be inputs to box A in which would result in D1 clicking. This replicates the interference effect of the counterfactual QKD. We note that while this may seemingly 'violate' a requirement of device-independence where no information is leaked from Bob's station, we argue this to be exceptional given the necessary channel (path B_2) from Bob to Alice in a counterfactual setup.

Case 2: Alice's and Bob's bit coincide. Bob's box will not send anything towards Alice's site. This action is similar to the path-blocking procedure as in Noh (2009) and Li (2014). We then consider the following scenarios:

1. In the event where Eve had distributed $\left|1\right\rangle_A \left|0\right\rangle_B \left|m\right\rangle_B$, Alice's qubit $\left|1\right\rangle_A$ will be submitted to box A to result in either detector D1 or D2 clicking with equal probability.
2. On the other hand, had Eve distributed $\left|0\right\rangle_A \left|1\right\rangle_B \left|m\right\rangle_B$, then Bob's detector D3 will click. When box A detects Alice's qubit as $\left|0\right\rangle_A$, neither D1 nor D2 click.

The above can in fact be achieved by first equipping box B with a measurement device to distinguish between the polarization states of the third incoming qubit; whether it is horizontally or vertically polarized. Since it is orthogonal, then it can be done perfectly. We further require box B to act as follows: when Bob inputs a choice for polarization (using either the H or V button), his choice would be compared to the polarization of the incoming qubit. If they are the same, a further measurement is made to distinguish between states $\left|0\right\rangle_B$ and $\left|1\right\rangle_B$ of the second qubit. In the case of the latter, the detector D3 is fired. Either way the process for box B ends and no qubit is sent out of Bob's site. On the other hand, if the polarization of the incoming qubit is different from Bob's button choice, the second qubit is sent to Alice.

In order to simulate the counterfactual protocol we propose the following ansatz. For Case 1, we require that box A to behave as such that the probability of detector Dj clicking given $\left|i \oplus 1\right\rangle_B \left|i\right\rangle_A$ is written as

$$P(\mathrm{D}j \,|\, \left|i \oplus 1\right\rangle_B \left|i\right\rangle_A) = \frac{1+(-1)^{(j+1)}}{2}, \tag{4.4}$$

in which $j = 1,2$ and $i = 0,1$. Meanwhile, in Case 2 we need box A to behave as such that the probability of detector Dj clicking given $\left|\text{no input}\right\rangle_B \left|i\right\rangle_A$ is

$$P(Dj \,|\left|\text{no input}\right\rangle_B \left|i\right\rangle_A) = \begin{cases} \frac{1}{2}, & i = 1 \\ 0, & i = 0 \end{cases}, \tag{4.5}$$

for $j = 1,2$ with $\left|\text{no input}\right\rangle_B$ represents the event when there is no incoming qubit from Bob. This box can be done by virtue of having the $CNOT$ function in which $CNOT : \left|b,a\right\rangle \to \left|b,a \oplus b\right\rangle$. Hence, let us reconsider both cases.

In Case 1, box A will receive the second qubit from Bob as well as Alice's qubit as inputs. Box A will then perform the $CNOT$ function on either one of the following:

$$CNOT\left|0\right\rangle_B \left|1\right\rangle_A, \tag{4.6}$$

$$CNOT\left|1\right\rangle_B \left|0\right\rangle_A, \tag{4.7}$$

with Alice's resulting state would eventually be detected by either detector D1 or D2. Assuming that detector D1 will detect state $\left|0\right\rangle_A$ and D2 will detect state $\left|1\right\rangle_A$, the above $CNOT$ function will eventually result in D2 only clicking.

When Alice's and Bob's bit are the same, no qubit from Bob will be sent out to box A. In the event where box A detects Alice's qubit as $\left|1\right\rangle_A$, it will perform a $CNOT$ function on state $\left|x+\right\rangle = \left(\left|0\right\rangle + \left|1\right\rangle\right) / \sqrt{2}$ along with Alice's state written as

$$CNOT\left|x+\right\rangle\left|1\right\rangle_{A}. \tag{4.8}$$

We can assume that the state $\left|x+\right\rangle$ is supplied by the box A. As a result, with equiprobability detector D1 and D2 will click. On the other hand, if state $\left|0\right\rangle_{A}$ is being detected, then box A will end its process.

As demonstrated above, Eve can perfectly simulate the protocol by distributing a system that is made up of entirely separable states. As she knows the values of m, as well as when Alice and Bob accepts or rejects a run, Eve basically has complete knowledge of the key. It is then obvious that the protocol presented by Noh (2009) and Li (2014) are not secure in a device independent context.

4.2.1.2 CQKD with entangled states

The requirement made in Noh (2009) and Li (2014) to disclose 'which detector clicked' in public channel was intended to allow for Alice and Bob to know when a bit is accepted for key purposes. This however actually provides Eve with information on the bit string regardless of whether the qubits are entangled or not. Let us suppose that the state, $\left|\Psi\right\rangle_{m}$ being distributed are as follows:

$$\left|\Psi\right\rangle_{m} = \frac{\left(\left|1\right\rangle_{A}\left|0\right\rangle_{B} - \left|0\right\rangle_{A}\left|1\right\rangle_{B}\right)}{\sqrt{2}} \otimes \left|m\right\rangle_{B}, \tag{4.9}$$

in which $m \in \{H,V\}$ depends on Alice's choice of a button. Since the state $\left|H\right\rangle_{B}$ and $\left|V\right\rangle_{B}$ can be measured perfectly without disturbing the entangled state, then knowing ‘which detector clicked’ will allow Eve to know with certainty which bit is accepted as a key. As a matter of fact, this strategy is much more straightforward than the case for the separable states as Eve does not need to prescribe the various ways the boxes behave as described in the earlier subsection. It is only more demanding in the context of Eve having perfect control of some entangled state.

We note clearly that the main loophole in the protocol comes from the revelation of ‘which detector clicked’ as in either strategy, Eve knows fully well on the values of m which she can determine. One way of closing this loophole while still allowing for the legitimate parties to share a key is by having Alice to only declare when detector D2 clicks. In this way, whenever Bob does not measure a photon (D3), he would know when D2 clicks thus not use those for key sharing and when D1 clicks for key bits.

The second less obvious loophole is the case for Bob’s resending of a qubit in the path B_2 as in the separable state strategy. Hence, if Alice and Bob were to drop this requirement i.e. they do not reveal which detector clicked in the public channel, or at most mention only when D2 clicks, and assure themselves that their first two qubits are in fact a maximally entangled states (which can violate a Bell inequality) then it is possible for them to extract a secure key.

By not revealing the information on ‘which detector clicked’, Eve would not have known which bit is going to be accepted even if the strings for raw key is publicly broadcasted. It would seem that both scenarios can be viewed as a separate system. In what follows, we are going to propose a framework for device independent counterfactual QKD (DI CQKD) based on these conditions.

4.3 THE PROPOSED COUNTERFACTUAL PROTOCOL

In this protocol, we suppose that Alice and Bob would share two setups as shown in Figure 4.3. For definiteness, we named the setup that consists of source S_1 as Setup 1 while the other as Setup 2.

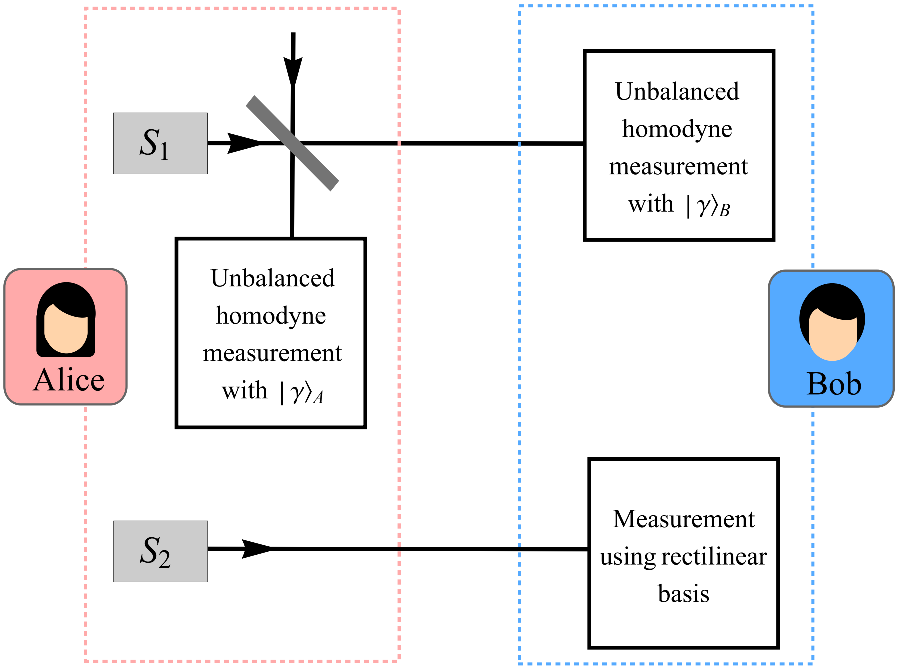
S_1
Unbalanced homodyne measurement with $|\gamma\rangle_B$
Alice
Unbalanced homodyne measurement with $|\gamma\rangle_A$
Bob
S_2
Measurement using rectilinear basis

Figure 4.3 A schematic diagram of the proposed counterfactual protocol.

In Setup 1, we will consider the SDI protocol of Chapter 3 in which Setup 1 starts as Alice triggers the single photon source S_1. The resulting state, $|\Psi\rangle$ from single photon incident on the 50:50 beam splitter (BS) is given by

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|1\rangle_A|0\rangle_B - |0\rangle_A|1\rangle_B\right), \tag{4.10}$$

where A and B are the path towards Alice and Bob, respectively. Both parties then commit to an unbalanced homodyne measurement with a strong coherent state $\left|\gamma\right\rangle_j$ where $j \in \{A, B\}$ represent the coherent state used in Alice's and Bob's measurement setting, respectively. The event of either Alice's or Bob's detector click corresponds to the binary value for the bit strings. A certain amount of secrecy (i.e. non zero value for Eve's uncertainty) is assured by having Alice and Bob testing for a CH inequality on the measurement that they should make. For detailed description of the protocol, we referred to Chapter 3 of this thesis.

Meanwhile, in Setup 2, Alice would prepare the qubit to be in either horizontally polarized state $\left|H\right\rangle$ or vertically polarized state $\left|V\right\rangle$. She would then submit this qubit to Bob where he will measure it in the rectilinear basis (this can be achieved by a polarizing beam splitter with two detectors) and the measurements would distinguish between the polarization states perfectly. For the sake of simplicity, we shall assume that the channel for Setup 2 is completely error free. This is not unreasonable as given the fact that the states can be distinguished perfectly, even by Eve, one can imagine that there is no reason for them to be transmitted as single photons subject to a depolarising channel; rather these states can be essentially 'broadcast' and the only real critical issue is to have it authenticated. Note that, we also do not put the requirement that both setups need to be performed simultaneously. Now, using the results from both setups we can establish the key as follows. We discard the result for all runs in Setup 2 that correspond to bit 1 in Setup 1. The remaining bits from Setup 2 will then serve as key strings for Alice and Bob. As an example, imagine a sample of the strings resulting each from Setup 1 and Setup 2, as shown from Table 4.1.

Table 4.1 Sample of strings resulting from Setup 1 and Setup 2.

Setup 1 results	0	1	0	0	1	0	1	1	0
Setup 2 results	H	H	V	H	V	V	H	V	H

After discard	H		V	H		V			H
Raw key	0		1	0		1			0

Alice and Bob, without disclosing publicly could discard the results of Setup 2 corresponding to bit 1 of Setup 1 to result in the following string: 'H V H V H'. Representing H as 0 and V as 1, we can see how the binary string now shared between Alice and Bob derived from Setup 2 can be used as a raw key which contains some uncertainty for Eve due to her ignorance of exactly which results are to be discarded and which to retain. As the bits between Alice and Bob in Setup 1 must be necessarily correlated (perfectly) it is obvious to note that an error correction procedure needs to be done for the results of Setup 1 prior to the establishing of the key based on Setup 2 as just described.

The protocol can now be outlined as follows.

1. Alice submits a photon to the 50:50 beam splitter, resulting in an entangled states of single photon and vacuum that is accessible to both Alice (in path A) and Bob (in path B).
2. Both of them would make a homodyne measurement, identical to the ones presented in Chapter 3.

3. After completing the transmission and measurement process, Alice and Bob would estimate the CH value on the measurement results and perform error correction procedure.
4. Note that steps 1 to 3 are identical to the protocol described in Chapter 3, with the exception of privacy amplification, which we do not execute.
5. Alice sends to Bob a string of polarized photon.
6. Bob measures the states using rectilinear basis.
7. Based on the results of step 2 and 5, the legitimate parties will discard the rounds in both setups, which corresponds to bit 1 of Setup 1.
8. The remaining bits would then be used as a raw key.

It is worth noting that we are proposing an equivalent protocol to CQKD within a device independent scenario. By equivalence we mean that the protocol actually capitalizes on the nature of single photon entanglement while the bits used for key is derive from the case where photons have not travelled to Bob but only to Alice. This is in fact the working principle for the CQKD. In what follows we will provide an analysis of the proposed protocol's security.

4.3.1 Security Analysis

Supposedly, Alice and Bob share N bit strings in which we consider that on average, there would be an equal number between bit 0 and bit 1. Within these N bits, there are U bits that are unknown to Eve in which half of them will eventually be discarded. Hence, the possible ways for the parties to throw out the bits, W can be determine as follows

$$W = \begin{pmatrix} U \\ \frac{U}{2} \end{pmatrix}$$

$$= \frac{U!}{\frac{U}{2}!\left(U - \frac{U}{2}\right)!}. \tag{4.11}$$

Eve's uncertainty, U_E related to the unknown bits is given by the Shannon entropy of eq. (1.17) as

$$U_E = -\sum \frac{1}{W} \log_2\left(\frac{1}{W}\right)$$

$$= \log_2 W. \tag{4.12}$$

Now, let us apply the above scenario in which Alice and Bob would initially share N bits string to the SDI protocol of Chapter 3. Similarly, we imagine that Eve would not have any knowledge on U bits out of these N bits. Then, Eve's uncertainty per bit for this protocol is given by

$$\frac{U}{N} \approx p_{NL}, \tag{4.13}$$

which is approximately equal to the probability of Eve sending a nonlocal box, p_{NL}.

Let us consider a scenario where Alice and Bob discard an equal fraction of bits in the SDI protocol i.e. the bits that correspond to Eve sending nonlocal boxes is halved. Therefore, the uncertainty that she has in that scenario, U_{SDI} would be

$$U_{SDI} = -\sum \frac{1}{2^{\frac{U}{2}}} \log_2 \left(\frac{1}{2^{\frac{U}{2}}} \right)$$
$$= \log_2 2^{\frac{U}{2}}$$
$$= \frac{U}{2}. \quad (4.14)$$

We define R as the ratio of the uncertainty of this protocol to Eve's uncertainty when half of SDI protocol bits are discarded in which can be written as

$$R = \frac{\log_2 W}{\frac{U}{2}}. \quad (4.15)$$

In the limit of long keys i.e. as U approaching infinite, we obtain

$$\lim_{U \to \infty} R = 2, \quad (4.16)$$

as shown in Figure 4.4. This is of course the result that we would attain considering that the number of the two bits are equal.

With Eve's uncertainty, $\mathcal{E}_u = p_{NL} \cdot R$ and Eve's information $I_{AE} = 1 - \mathcal{E}_u$, the key rate, K is given by the following formula

$$K = 1 - I_{AE} - h(e_{AB}), \quad (4.17)$$

in which the $h(\cdot)$ is the binary entropic function. Note that e_{AB} is the error between Alice and Bob, which corresponds to Setup 1.

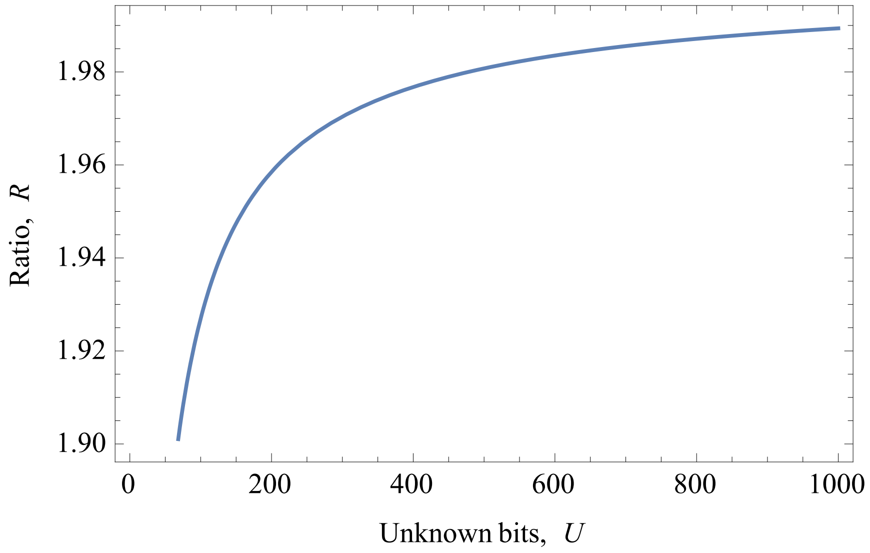

Figure 4.4 The ratio of this protocol to SDI protocol versus Eve's unknown bits, U .

Hence, it is instructive to compare the performance of DI CQKD with SDI protocol of Chapter 3. We note that the key rate that is described in eq. (4.17) should be divided by 2 when comparing the protocols. This is due to our assumption that the number of bit '0' and '1' in the string are necessarily the same. As we can see from Figure 4.5, the maximum key rate achievable for the DI CQKD protocol (represented as the solid curve) being approximately 0.22, which is the same as the SDI protocol described by the dashed curve. However, it is obvious from the graph that the key rate of DI CQKD is non zero for a CH violation up to about -1.06 whereas the SDI protocol obtain a non zero key rate only up till -1.08 of the CH violation. The DI CQKD perform better than the SDI protocol, as the key rate of DI CQKD remains greater than the key rate of SDI protocol throughout the graph. This obvious increment is the result of Eve's information being suppress in the DI CQKD making her uncertainty per bit is twice than that of SDI protocol.

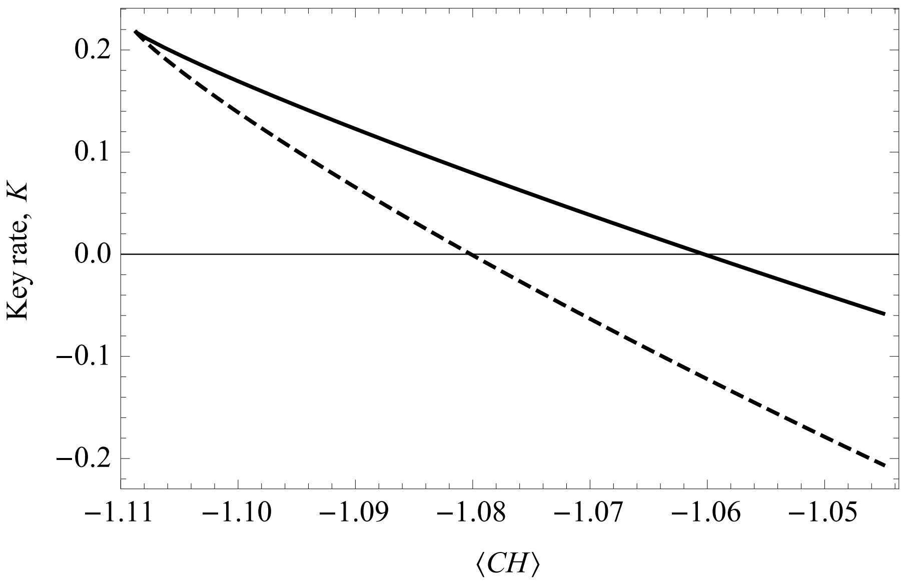

Figure 4.5 Key rate versus estimation of local violation, $\langle CH \rangle$. The dashed line represent the achievable key rate of SDI protocol, while the solid curve corresponds to the DI CQKD protocol.

The case for Eve's increased uncertainty may not be as surprising if one considers the simple case of using a 'partially' secret key to encrypt a message, say by a simple XOR procedure. Assuming both the key and the message are strings of bits such that there are no correlations between the bits, then the encrypted message cannot provide any more information to Eve than the key does. As an example, if we imagine the case where Eve knows parts of the key while being ignorant of the rest; an XOR of a known bit with a completely unknown one would result in a bit with the equal probability of being one or the other; thus maximum uncertainty for that bit. An analogous argument holds for the compromised parts of the bit to Eve's benefit. Although admittedly this example is different from what we are currently dealing with, it exemplifies the possible fact that using a partially known key to encrypt (in the simple manner above) should not decrease Eve's uncertainty of the cryptogram beyond her uncertainty of the key.

In our case above, we see that the final bit value is strongly dependent on its position and whether the bits before it were accepted or otherwise, for which the latter is decided by the 'partially secret key' of Setup 1. In other words, the case we consider here is actually a mapping of the known message (of Setup 2) to a shorter string with the number of possible mapping determined by the number of how many ways one can have a binary string of equal numbers of 1 and 0 from Eve's unknown subset derived from Setup 1. Admittedly, the key rate derived is an optimistic scenario as we do not consider the possibility of mappings resulting in identical strings (collisions) though the probability of such an event we believe can be made small by having longer strings. We admit that these arguments are heuristically in nature and it is desirable to have a more rigorous proof. However, we also understand that such a matter may be highly nontrivial and we would consider it as part of future work.

4.4 EXTENDING TO CQKD WITH BELL TEST: A DI CQKD

The above scenario we considered is based on the equivalence of the CQKD protocol and any QKD protocol that sees a bit being shared between Alice and Bob with no (nett) signal being sent between them. It is not difficult to imagine how we can apply the above scenario to a CQKD with a Bell test.

Let us consider the CQKD with the following addendum:

1. Bob's measurement is not simply a click of the detector when a signal reaches it (in a successfully blocked scenario), but the measurement would be a homodyne detection like that of Setup 1 (with coherent displacement of $\beta = 0, -s$).
2. Alice has a choice of either

a. making a measurement like that of CQKD where she may have D1 or D2 clicking or only D3 clicks when Bob successfully blocks (we refer to this as the Key Mode, or KM); or

b. making a CHSH measurement like that of Setup 1 in which the beam splitter, BS2 of Figure 4.1 would be removed (we refer to this as the CHSH mode, or CHSHM).

We do not specify exactly how this can be experimentally achieved except that Alice's buttons would allow her to do as above. Hence, we can imagine the protocol to run as follows:

1. Alice determines whether she wants to perform KM or CHSHM.
2. With probability $1-c$, she commits to perform KM and with probability c, she commits to CHSHM measurement.
3. Bob will randomly decide on his polarization. He will also randomly choose between the possible configurations for his homodyne detection.
4. At the end of the protocol, Alice announces when she actually used a CHSH measurement.
5. Based on item 4, Alice and Bob would determine their CHSH value.
6. For the remaining runs, Alice would only announce instances when she gets a click at D1 (which would be discarded).
7. Runs where Alice chooses KM and Bob chooses $\beta=-s$ would also be discarded (Bob would need to announce these).
8. The remaining runs would then be subjected to the sifting procedure of our equivalent protocol of the prior section.

The above protocol is in effect the CQKD with a Bell test. At first glance it would seem that Alice and Bob would have plenty buttons to choose from; i.e. Bob has 4 - a combination of two polarization and two homodyne parameters while Alice has a choice of 6 - two buttons for KM and 4 buttons for CHSHM. However, if we assume that Eve distributes the signals (strategies) to both Alice and Bob, we can assume she knows perfectly the polarization values (reducing this to the equivalent protocol where the polarization states are 'broadcasted'). Further to that, we assume the CHSH test would be done for separate choices of polarizations; thus this effectively makes Bob's choice of buttons only 2.

A similar argument would reduce Alice's to 3; where 2 of it is used for CHSH check. This effectively results in a protocol with 2 measurement basis on Bob's side and 3 on Alice's, similar to that of Acín, Massar, et al. (2006). As the key is derived in cases where Bob successfully blocks the signal, with the actual information of which detector clicked (Alice's or Bob's side) not divulged, this results in an identical scenario as the case for the equivalent protocol. Obviously there would be some differences in a detailed analysis (example, whether there would be errors related to Bob's choice of polarization when compared to Alice which we assume as non), though one can see that Eve, not knowing which button Alice (nor Bob) presses, the strategies she sends to determine which detectors actually clicked in the cases where a key is derived would also be the same type of strategies sent when a CHSH is tested; thus we conclude that the amount of nonlocal strategies resulting in a CHSH violation in a CHSHM would also be the (statistically) same amount that would allow for Alice and Bob to share a key in the KM. Thus we argue that the security of the DI CQKD reduces to that of the equivalent protocol.

4.5 CONCLUSION

In this work, we have outline the counterfactual QKD as described by Noh (2009) and Li (2014) and analyzed the security of the counterfactual protocol within a device independent context. We eventually show that the security of the protocol is compromised, as the protocol is reproducible using separable states, resulting in entirely classical correlations between the systems where the states can actually be predetermined by Eve. We further show that the need for the legitimate parties to disclose 'which detector clicked' in the public channel has given Eve access to the information of the shared key despite the state being entangled. This is because the entanglement is only between the first two qubits while the polarized state that is used to establish the key string is not. Hence, we propose our own (equivalent) version of a device independent counterfactual QKD (DI CQKD) with the basic building block being the SDI protocol of the previous chapter.

Subscribing to a heuristic analysis for an individual attack strategy by a supra-quantum Eve, we compare the performance of DI CQKD and SDI protocol. Based on our findings, both the DI CQKD protocol and SDI protocol achieve the same highest key rate of approximately 0.22. However, we note that the performance of DI CQKD protocol exceeds SDI as a positive key rate is obtained for a violation of CH up till -1.06 compared to SDI that is only up to -1.08 with the DI CQKD key rate being greater than that of SDI the entire time.

Finally we show how one can actually use this equivalent protocol to construct a DI CQKD where selected runs of a conventional CQKD (similar to Li (2014)) is randomly substituted with runs to determine a Bell violation.

CHAPTER FIVE

CONCLUSION AND FUTURE OUTLOOK

5.1 INTRODUCTION

The main objective of this thesis is to propose a device independent framework for the counterfactual QKD of Noh (2009) and Li (2014). We divided the thesis into five chapters in which Chapter 1 consists of some background on QKD and DI QKD. We opted for a concise approach to the chapter, highlighting only what we believe is the more necessary elements.

Chapter 2 sees our first contribution where we consider an optimized QKD setup in which the parties commit to measurements with binary input and output. Here, Eve is assumed to be supra-quantum, that is, she is only constrained by the no-signaling principle. We compare between two different versions of the setup in which we consider Version I as the event where only Alice disclose her measurement bases. On the other hand, Version II would refer to the event where both Alice and Bob reveal their bases over the public channel. In both versions, Alice and Bob will determine the security of the protocol against an individual attack by Eve by means of checking for violation of CHSH inequality, on a subset of the measurement results. A key can be derived by optimizing the angles of the measurements. We also consider a simpler form of Version II by having a maximal correlation between Alice and Bob in one set of bases' choice by setting $\beta = 0$. We note that Version II exceeds Version I for disturbance on the channel for up to about 3% and 2.4%, the latter is for the case $\beta = 0$. Despite being more generic in nature, we use the result of this chapter, namely, the case of $\beta = 0$ in the following chapter on single photon entanglement QKD.

In Chapter 3, we have analyzed a QKD protocol relying on the nonlocality features of a single particle to demonstrate its security within a device independent context. Regardless of how the protocol is illustrated, the security analysis assumes that the legitimate parties are up against an individual attack strategy prepared by an eavesdropper limited only by the no-signaling principle. In order to determine its secrecy, the legitimate parties resort to observe the violation of the CH inequality. We show that a positive key rate may be obtained for a CH violation up to -1.08.

We start off Chapter 4 by describing the counterfactual protocol of Noh (2009) (or more precisely as presented by Li (2014)). We then proceed to show that the protocol is insecure in a device independent scenario. The main reason for the insecurity can be attributed to two main elements. They are

1. Alice's and Bob's complete disclosure of detector clicks;
2. absence of a CHSH check (which is a necessary ingredient for all device independent QKD).

Consequently, we propose a framework for device independent counterfactual QKD and then heuristically show that it is possible to have a positive key rate; which is impossible for the original CQKD protocol. This essentially concludes the development of the device independent framework for counterfactual QKD.

In the next section, we present several suggestions for future outlook that are of interest but unable to cover in a justifiable manner.

5.2 FUTURE OUTLOOK

The current work would contain interests in both the cryptographic as well as a more fundamental nature for future research. In the ensuing subsection, we will present cryptographic concerns borne from this work first before delving into fundamental issues. It would be interesting to note that these latter issues may open up new perspectives in quantum physics.

5.2.1 Cryptographic interest: Eavesdropping strategy

In a standard QKD protocol, Eve's strategy can generally be divided into three types of attacks, namely, individual attack, collective attack and joint attack. Recall that in individual attack, Eve probes and measures Alice's and Bob's quantum systems separately and independently, using the same strategy (Gisin et al., 2002).

According to Gisin et al. (2002), a collective attack can be described as a strategy in which Eve attacks each quantum systems independently using the same strategy as in individual attack. However, in collective attack, Eve would perform collective measurement on the qubits hence the name. For one-way postprocessing under the collective attacks, the secret key rate achievable is bounded by the Devetak-Winter bound (Devetak & Winter, 2005). Assuming that Eve's information on Alice is more than Bob, the key rate, K is then given by the following

$$K = I_{AB} - I_{AE}, \tag{5.1}$$

with Eve's information on Alice, I_{AE} can be described by

$$I_{AE} = \max\ \chi(A:E), \tag{5.2}$$

in which $\chi(A:E)$ is the Holevo quantity between Eve and Alice.

Meanwhile, another class of eavesdropping attack is the joint attack. This is considered as the most general attack and it is defined as a strategy in which Eve can probe and measure all quantum systems jointly. In both collective and joint attacks, it is assumed that Eve would perform her measurement only after the legitimate parties completed all public communications about basis reconciliation, error correction, and privacy amplification (Gisin et al., 2002).

5.2.1.1 Supra-quantum Eve

In our work thus far we have only consider an attack by a supra-quantum Eve. Her attack strategy includes submitting a mixture of deterministic strategies and nonlocal boxes i.e. PR boxes, sent individually making it ultimately an individual type attack. According to Jones & Masanes (2005), PR boxes can be viewed as the basic unit of nonlocal correlation. Hence, it may be of interest to consider Eve's attack strategy that includes a more generalized nonlocal boxes. However, it may be trivial to consider a nonlocal box with arbitrary inputs and binary outputs as Jones & Masanes (2005) has shown that all bipartite no-signaling correlations with binary outputs can be simulated by PR box. For the case of binary inputs and arbitrary outputs, Barrett, Linden, et al. (2005) has characterized its corresponding distribution, $\Pr(ab\,|\,xy)$ as follows

$$\Pr(ab\,|\,xy) = \begin{cases} \frac{1}{k}, & (b-a) \bmod k = xy \\ 0, & \text{otherwise} \end{cases}, \tag{5.3}$$

where input $x, y \in \{0,1\}$ and output $a, b \in \{0, \ldots, k-1\}$ with $k \in \{2, \ldots, \min(d_a, d_b)\}$. Note that, k, d_a and d_b are integers. The case where $d_a = d_b = 2$ represents the PR box correlation.

Therefore, the most natural question to ask is: would there be strategies for a supra-quantum Eve, which are analogous to the collective and joint attack in standard QKD literature?

5.2.1.2 Quantum Eve

We have mainly considered the case for a supra-quantum Eve, the eavesdropper who is not limited by quantum mechanics, but only on the no-signaling principle. This has provided us with the most pessimistic picture and may be less realistic. It would be interesting, though possibly an academic exercise to determine the actual performance of the QKD protocols of the earlier chapters within the context of a quantum Eve, i.e. an eavesdropper who is limited in fact by quantum mechanics.

The essential picture is as follows: Eve could distribute between the legitimate parties a Bell diagonal state for which Alice and Bob are subject to perform measurement on a random subset of their particles in well-chosen bases. Based on the results, they can estimate the locality violation and decide whether it is possible to distill a secure key rate from them. While the actual calculations may not be trivial, we expect that the results would not provide much insight into the QKD problem beyond a possibly more optimistic picture and may be of interest to the more practical side of quantum cryptography. It is instructive to extend the discussion to include collective attacks and joint attacks as well.

However, it is important to note that a device independent QKD against a collective attack by a quantum Eve has already exist in literature. In the protocol proposed by Pironio et al. (2009), Alice would have three measurement bases as opposed to only two, of which one would maximally overlap with Bob's for key purposes, though the Bell violation to be estimated by the relevant parties comes from a set of measurements excluding the ones for raw key. Hence, it is interesting to see the performance of the binary measurement based QKD as in our work would result against a collective attack by a quantum Eve.

5.2.2 Cryptographic Interest: Device Independent CQKD

We have proposed in Chapter 4, a device independent framework for counterfactual QKD. We have seen how in analyzing the security of the protocol, we have made several simplistic assumptions as follows:

Assumption 1: On average, there would be an equal number between bit 0 and bit 1. Note that this assumption is reasonable given an infinitely long key scenario. This is because the probability that the bit would result in bit 0 or bit 1 would converge to an average value when the number of rounds of the protocol increases as described by the law of large numbers. However, it is compelling to consider the case where the string of bits is made up of uneven number of these two bits within the finite key perspective and then determine its performance. This may well be a possible starting point for a finite key analysis.

Assumption 2: Colliding strings at the end of the protocol happens with a very small probability. We consider that at the end of the protocol, given an infinitely long string would see collisions (identical strings) with negligible probability. However, it would be desirable to have a proper quantification of such a probability and determine the relevant quantities that would affect it. This problem lies in the details of classical information theory.

5.2.3 Fundamental interest: Correlation versus Nature of Correlation

We saw in the second chapter how, given a binary measurement based QKD setup with each party committing to two different measurement bases, a key can be derived by optimizing the angles of the measurements. This understandably is the issue of identifying the point where measurements in overlapping bases (or nearly so) between the two parties, Alice and Bob and those where they maximize the CHSH estimation. The former provides for maximal correlation between them but allows for an eavesdropper to simulate the whole picture and thus compromising on the security by allowing Eve to have more information than the latter. On the other hand, the latter creates a situation where Eve's uncertainty of the key is higher than that between Alice and Bob, which in principle allow for key extraction.

Notwithstanding the cryptographic concern above, the whole issue possibly hides a more fundamental interest. This is the issue of non-compatible measurements. Since its early days, quantum mechanics saw bounds being set on the precision for which two observables can be measured; the famous Heisenberg uncertainty principle.

Suppose we consider two quantum mechanical observables A and B, with ΔA and ΔB being the standard deviation of the measurement results of observables A and B, respectively. The Heisenberg uncertainty principle can be expressed as

$$\Delta A \Delta B \geq \frac{1}{2}\left|\left\langle\left[A, B\right]\right\rangle\right|, \tag{5.4}$$

in which $\left[A, B\right]$ being the commutator of A and B. With regard to eq. (5.4), if observables A and B are non-commutating i.e. when $\left[A, B\right] > 0$, then it follows from this $\Delta A \Delta B > 0$. We can see that by reducing the uncertainty of A would increase the uncertainty of B and vice versa. Hence, the Heisenberg uncertainty principle indicates that it is not possible to measure the two observables both simultaneously and precisely, though it is possible to measure one observable accurately at the expense of the other.

However, this is not the only way to characterize the uncertainty relations. In information-theoretic definition, uncertainty is closely related to entropy. The entropy works as a measure of the amount of uncertainty in the state of a physical system. Hence, rather than make use of eq. (5.4), it is more instructive to use the well known entropic uncertainty relation of the form (Coles, Berta, Tomamichel, & Wehner, 2017):

$$H(A)+H(B)\geq\log\frac{1}{c}, \tag{5.5}$$

in which $H(\cdot)$ is defined as Shannon's entropy with c being the maximal overlap between observables A and B. For an excellent review kindly refer to Coles et al. (2017).

Though the incompatibility discussed above is in the context of measurement (incompatibility between observables), the concept of incompatibility however has been generalized to other collections of input-output devices (Heinosaari, Miyadera, & Ziman, 2016). A quick example given in the same reference would be process measurements (Heinosaari et al., 2016).

Going back to the issue of the measurements made in the QKD protocol above, let us rewrite in terms of the following. Imagine the scenario where two parties are given each, a qubit that is part of a bipartite system (not necessarily entangled).

We allow the parties to commit to any measurement bases (two each) to determine the following:

1. The nature of the correlation between the qubits.
2. The correlations between the two qubits.

The first is really an estimation of the CHSH, while the second is the estimation of the mutual information between the two. We see that measurements that allow for the maximization of the CHSH value, i.e. determining precisely the nature of the correlation between the two parties, i.e. whether it is local or otherwise may not be compatible with establishing the amount of correlated bits between the two parties. It is worth noting that these may not be an issue with incompatibility between observables.

5.2.4 Fundamental interest: Quantum Cheshire Cat

The Quantum Cheshire Cat was first introduced by Aharonov, Popescu, Rohrlich, & Skrzypczyk (2013). In the paper, they suggested that physical properties could be separated from the objects, just like the Cheshire Cat of Alice in Wonderland and its grin. It maintains polarization as a separable degree of freedom from the (existence) photon itself. A polarized photon (e.g horizontal) state, $|\Psi\rangle$ after passing through a beam splitter can be written as

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\left(|B_1\rangle - |B_2\rangle\right)|H\rangle, \tag{5.6}$$

in which $|B_1\rangle$ and $|B_2\rangle$ correspond to the photon being in the output paths of the beam splitter. This, in principle, should open the counterfactual QKD to a natural vulnerability where the polarization degree of freedom can be measured independently of the photon. It would be interesting to design such a measurement.

However, this matter of Quantum Cheshire Cat has not been fully resolved and is currently a matter of debate and further research (Corrêa, Santos, Monken, & Saldanha, 2015).

REFERENCES

Acín, A., Gisin, N., & Masanes, L. (2006). From Bell's theorem to secure quantum key distribution. *Physical Review Letters*, *97*(12), 120405.

Acín, A., Massar, S., & Pironio, S. (2006). Efficient quantum key distribution secure against no-signalling eavesdroppers. *New Journal of Physics*, *8*(8), 126. http://doi.org/10.1088/1367-2630/8/8/126

Agarwal, G. S. (2013). *Quantum optics*. Cambridge university press.

Aharonov, Y., Popescu, S., Rohrlich, D., & Skrzypczyk, P. (2013). Quantum cheshire cats. *New Journal of Physics*, *15*(11), 113015. http://doi.org/10.1088/1367-2630/15/11/113015

Banaszek, K., & Wódkiewicz, K. (1999). Testing quantum nonlocality in phase space. *Physical Review Letters*, *82*(10), 2009.

Barrett, J., Hardy, L., & Kent, A. (2005). No signaling and quantum key distribution. *Physical Review Letters*, *95*(1), 10503.

Barrett, J., Linden, N., Massar, S., Pironio, S., Popescu, S., & Roberts, D. (2005). Nonlocal correlations as an information-theoretic resource. *Physical Review A - Atomic, Molecular, and Optical Physics*, *71*(2), 22101. http://doi.org/10.1103/PhysRevA.71.022101

Bell, J. S. (1964). On the Einstein Podolsky Rosen paradox. *Physics*, *1*, 195–200. http://doi.org/10.1002/prop.19800281202

Bennett, C., Brassard, G., & Mermin, N. (1992). Quantum cryptography without Bell's theorem. *Physical Review Letters*, *68*(5), 557–559. http://doi.org/10.1103/PhysRevLett.68.557

Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, *68*(21), 3121–3124. http://doi.org/10.1103/PhysRevLett.68.3121

Bennett, C. H., & Brassard, G. (1984). Quantum Cryprography: Public Key distribution and coin tossing. In *Int. Conf. on Computers, Systems & Signal Processing* (pp. 175–179).

Brida, G., Cavanna, A., Degiovanni, I. P., Genovese, M., & Traina, P. (2012). Experimental realization of counterfactual quantum cryptography. *Laser Physics Letters*, *9*(3), 247–252. http://doi.org/10.1002/lapl.201110120

Bruß, D. (1998). Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, *81*(14), 3018. http://doi.org/10.1103/PhysRevLett.81.3018

Cereceda, J. L. (2001). Identification of all Hardy-type correlations for two photons or particles with spin 1/2. *Foundations of Physics Letters*, *14*(5), 401–424. http://doi.org/10.1023/A:1015520603468

Cirel'son, B. S. (1980). Quantum generalizations of Bell's inequality. *Letters in Mathematical Physics*, *4*(2), 93–100. http://doi.org/10.1007/BF00417500

Clauser, J. F., & Horne, M. A. (1974). Experimental consequences of objective local theories. *Physical Review D*, *10*(2), 526.

Clauser, J. F., Horne, M. A., Shimony, A., & Holt, R. A. (1969). Proposed experiment to test local hidden-variable theories. *Physical Review Letters*, *23*(15), 880.

Coles, P. J., Berta, M., Tomamichel, M., & Wehner, S. (2017). Entropic uncertainty relations and their applications. *Reviews of Modern Physics*, *89*(1), 15002. http://doi.org/10.1103/RevModPhys.89.015002

Corrêa, R., Santos, M. F., Monken, C. H., & Saldanha, P. L. (2015). "Quantum Cheshire Cat" as simple quantum interference. *New Journal of Physics*, *17*(5), 53042. http://doi.org/10.1088/1367-2630/17/5/053042

Csiszár, I., & Körner, J. (1978). Broadcast Channels with Confidential Messages. *IEEE Transactions on Information Theory*, *24*(3), 339–348. http://doi.org/10.1109/TIT.1978.1055892

Devetak, I., & Winter, A. (2005). Distillation of secret key and entanglement from quantum states. In *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* (Vol. 461, pp. 207–235).

Diffie, W., & Hellman, M. (1976). New directions in cryptography. *IEEE Transactions on Information Theory*, *22*(6), 644–654.

Dunningham, J., & Vedral, V. (2007). Nonlocality of a single particle. *Physical Review Letters*, *99*(18), 180404.

Einstein, A., Podolsky, B., & Rosen, N. (1935). Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Physical Review*, *47*, 777.

Ekert, A. K. (1991). Quantum Cryptography Based on Bell's Theorem. *Physical Review Letters*, *67*(6), 661–663.

Freedman, S. J., & Clauser, J. F. (1972). Experimental test of local hidden-variable theories. *Physical Review Letters*, *28*(14), 938.

Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics*, *74*(1), 145.

Gradshteyn, I. S., & Ryzhik, I. M. (2007). Table of Integrals, Series and Products 7th edn, ed A Jeffrey and D. *Zwillinger (New York: Academic)*.

Hänggi, E., Renner, R., & Wolf, S. (2010). Efficient device-independent quantum key distribution. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 216–234).

Heinosaari, T., Miyadera, T., & Ziman, M. (2016). An invitation to quantum incompatibility. *Journal of Physics A: Mathematical and Theoretical*. http://doi.org/10.1088/1751-8113/49/12/123001

Jones, N. S., & Masanes, L. (2005). Interconversion of nonlocal correlations. *Physical Review A*, *72*(5), 52312.

Kamaruddin, S., & Shaari, J. S. (2015). Device-independent quantum key distribution using single-photon entanglement. *EPL (Europhysics Letters)*, *110*(2), 20003.

Kamaruddin, S., & Shaari, J. S. (2016). Optimal Device Independent Quantum Key Distribution. *Scientific Reports*, *6*.

Lee, J.-W., Lee, E. K., Chung, Y. W., Lee, H.-W., & Kim, J. (2003). Quantum cryptography using single-particle entanglement. *Physical Review A*, *68*(1), 12324.

Li, Y.-B. (2014). Analysis of counterfactual quantum key distribution using error-correcting theory. *Quantum Information Processing*, *13*(10), 2325–2342.

Mayers, D., & Yao, A. (1998). Quantum Cryptography with Imperfect Apparatus. Retrieved from http://arxiv.org/abs/quant-ph/9809039v1

Menezes, A., van Oorschot, P., & Vanstone, S. (1996). *Handbook of Applied Cryptography* (Vol. 19964964). CRC press. http://doi.org/10.1201/9781439821916

Mermin, N. D. (1995). The best version of Bell's theorem. *Annals of the New York Academy of Sciences*, *755*(1), 616–623.

Nielsen, M. A., & Chuang, I. L. (2010). *Quantum computation and quantum information*. Cambridge university press.

Noh, T.-G. (2009). Counterfactual quantum cryptography. *Physical Review Letters*, *103*(23), 230501.

Peres, A. (1995). Nonlocal effects in Fock space. *Physical Review Letters*, *74*(23), 4571.

Pironio, S., Acin, A., Brunner, N., Gisin, N., Massar, S., & Scarani, V. (2009). Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, *11*. http://doi.org/10.1088/1367-2630/11/4/045021

Popescu, S., & Rohrlich, D. (1994). Quantum nonlocality as an axiom. *Foundations of Physics*, *24*(3), 379–385.

Pramanik, T., Adhikari, S., Majumdar, A. S., & Home, D. (2012). Testing nonlocality of single photons using cavities. *Physics Letters A*, *376*(4), 344–348.

Renou, M.-O., Rosset, D., Martin, A., & Gisin, N. (2016). On the inequivalence of the CH and CHSH inequalities due to finite statistics. *arXiv Preprint arXiv:1610.01833*.

Rivest, R. L., Shamir, A., & Adleman, L. (1978). A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, *21*(2), 120–126.

Scarani, V. (2009). Quantum information: primitive notions and quantum correlations. *arXiv Preprint arXiv:0910.4222*.

Scarani, V. (2012). The device-independent outlook on quantum physics. *Acta Physica Slovaca*, *62*(4), 347–409.

Scarani, V., Acin, A., Ribordy, G., & Gisin, N. (2004). Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. *Physical Review Letters*, *92*(5), 57901.

Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics*, *81*(3), 1301–1350. http://doi.org/10.1103/RevModPhys.81.1301

Scarani, V., Gisin, N., Brunner, N., Masanes, L., Pino, S., & Ac'\in, A. (2006). Secrecy extraction from no-signaling correlations. *Physical Review A*, *74*(4), 42339.

Schneier, B. (2007). *Applied cryptography: protocols, algorithms, and source code in C*. john wiley & sons.

Sergienko, A. V. (2005). *Quantum communications and cryptography*. CRC press.

Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell Labs Technical Journal*, *28*(4), 656–715.

Shenoy, H. A., Srikanth, R., & Srinivas, T. (2013). Semi-counterfactual cryptography. *EPL (Europhysics Letters)*, *103*(6), 60008.

Shor, P. W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Foundations of Computer Science, 1994 Proceedings., 35th Annual Symposium on* (pp. 124–134).

Skrzypczyk, P., & Brunner, N. (2009). Couplers for non-locality swapping. *New Journal of Physics*, *11*(7), 73014.

Sun, Y., & Wen, Q.-Y. (2010). Counterfactual quantum key distribution with high efficiency. *Physical Review A*, *82*(5), 52318.

Tan, S. M., Walls, D. F., & Collett, M. J. (1991). Nonlocality of a single photon. *Physical Review Letters*, *66*(3), 252.

Vaidman, L. (2016). “Counterfactual” quantum protocols. Retrieved from http://arxiv.org/abs/1605.02181

Van Assche, G. (2006). *Quantum cryptography and secret-key distillation*. Cambridge University Press.

Van Enk, S. J. (2005). Single-particle entanglement. *Physical Review A*, *72*(6), 64306.

Vernam, G. S. (1926). Cipher printing telegraph systems: For secret wire and radio telegraphic communications. *Journal of the AIEE*, *45*(2), 109–115.

Werner, R. F. (1989). Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Physical Review A*, *40*(8), 4277.

Wiesner, S. (1983). Conjugate coding. *ACM Sigact News*, *15*(1), 78–88.

Wildfeuer, C. F., & Dowling, J. P. (2008). Strong violations of Bell-type inequalities for Werner-like states. *Physical Review A*, *78*(3), 32113.

Yin, Z.-Q., Li, H.-W., Chen, W., Han, Z.-F., & Guo, G.-C. (2010). Security of counterfactual quantum cryptography. *Physical Review A*, *82*(4), 42335.