Developments in Device-Independent Quantum Key Distribution

Jasmeet Singh

A dissertation submitted for the partial fulfilment of

BS-MS dual degree in Science

Indian Institute of Science Education and Research Mohali

June 2020

Dedicated to my Family

Certificate of Examination

This is to certify that the dissertation titled "**Developments in Device-Independent Quantum Key Distribution**" submitted by **Mr. Jasmeet Singh** (Reg. No. MS15064) for the partial fulfillment of BS-MS dual degree programme of the Institute, has been examined by the thesis committee duly appointed by the Institute. The committee finds the work done by the candidate satisfactory and recommends that the report be accepted.

Dr. Sandeep Goyal Dr. Kavita Dorai Prof. Arvind
(Supervisor)

Dated: June 14, 2020

Declaration

The work in this dissertation has been carried out by me under the guidance of **Prof. Arvind** at the Indian Institute of Science Education and Research Mohali.

This work has not been submitted in part or in full for a degree, a diploma, or a fellowship to any other university or institute. Whenever contributions of others are involved, every effort is made to indicate this clearly, with due acknowledgment of collaborative research and discussions. This thesis is a bonafide record of original work done by me and all sources listed within have been detailed in the bibliography.

Jasmeet Singh
(Candidate)

Dated: June 14, 2020

In my capacity as the supervisor of the candidate's project work, I certify that the above statements by the candidate are true to the best of my knowledge.

Prof. Arvind
(Supervisor)

Acknowledgment

This thesis would never have been possible without the support of many people and I feel it is my pleasant duty to thank them for the various forms of support, encouragement and help that they have provided during the time spent on it.

First and foremost, I'd like to thank my supervisor Prof. Arvind for providing me with the opportunity to work under his able guidance and for his continuous support over the past year. Without his help and counsel, this project would not have been possible. He was the one who introduced me to the topic of device-independent quantum key distribution, and provided me with valuable insights through regular discussions throughout the thesis. The door to his office was always open whenever I ran into a trouble spot or was skeptical about my research or writing.

I'd also like to thank the rest of my thesis committee members, Dr. Kavita Dorai and Dr. Sandeep Goyal, who kept pushing me forward via their insightful comments and encouragement during the process of evaluation.

I also extend my gratitude towards the members of Quantum Computation and Quantum Information (QCQI) Group at IISER Mohali, Jaskaran Singh, Rajendra Singh Bhati, Soumyakanti Bose and Jorawar Singh for providing me all the necessary help whenever I needed it. Continuous discussions with them kept me motivated and hepled me gain an in-depth knowledge of the topic. I would also like to thank Jagmeet Singh Bains, who helped me in overcoming the technical difficulties that I faced while writing the thesis.

I'd like to acknowledge IISER Mohali for providing me with the best infrastructure and environment for carrying out this project. I am also thankful to the "Department of Science and Technology", Government of India, for providing me the financial support, through DST-INSPIRE fellowship during the past five years.

Finally, I'd like to thank my family, who stood beside me all these years, strongly supporting and guiding me.

Jasmeet Singh

List of Figures

2.1 Relation of information theory to other fields [Cover 06] 5

2.2 Binary entropy H_{binary} *vs* p 7

2.3 Relationship between different types of entropies [Nielsen 11] 10

3.1 The BB84 quantum key distribution protocol [Hänggi 10] 26

3.2 Ekert's E91 quantum key distribution protocol [Hänggi 10] 28

4.1 Quantum apparatuses as *black boxes* used by Alice and Bob in DI-QKD [Scarani 13] 35

7.1 Key rate (K_N) *versus* noise (p) for different values of N 64

List of Tables

5.1 Conditional probability distribution $P(xy|ab)$ 42

7.1 Extremal strategies available to Eve for measurement inputs $x = 0$ and $y = 0$ (used to generate a key) [Acín 06b]. 60

8.1 Violation of Bell inequality for state $|\psi_d^+\rangle$ [Acín 02]. 75

Notations and Abbreviations

$\|\rangle$	A ket state
$\langle\|$	A bra state
QKD	Quantum key distribution
DI-QKD	Device-independent quantum key distribution
CHSH	Clauser-Horne-Shimony-Holt
$M^{\otimes n}$	n-tensor product of M
$\|0\rangle$	$\begin{pmatrix} 1 \\ 0 \end{pmatrix}$
$\|1\rangle$	$\begin{pmatrix} 0 \\ 1 \end{pmatrix}$
$\|+\rangle$	$\begin{pmatrix} 1 \\ 1 \end{pmatrix}$
$\|-\rangle$	$\begin{pmatrix} 1 \\ -1 \end{pmatrix}$
σ_x or $\mathbb{X}$	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
σ_y or $\mathbb{Y}$	$\begin{pmatrix} 0 & -\iota \\ \iota & 0 \end{pmatrix}$
σ_z or $\mathbb{Z}$	$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

Contents

List of Figures i

List of Tables iii

Notations and Abbreviations v

Abstract xi

1 Introduction 1

1.1 Organization of the thesis 3

2 Information theory and entropy 5

2.1 Shannon's entropy 6

2.2 Properties of entropy 7

2.2.1 Binary entropy 7

2.2.2 Joint entropy 7

2.2.3 Relative entropy 8

2.2.4 Conditional entropy 9

2.2.5 Mutual information 10

2.3 Data-processing inequality 13

2.4 Von Neumann entropy 15

2.4.1 Entropy of a mixture 16

2.5 Accessible information 18

2.6 Holevo bound 18

3 Quantum key distribution 23

3.1 Introduction 23

3.2 Protocols for quantum key distribution 24
3.2.1 BB84 Protocol 25
3.2.2 The EPR Protocol 27
3.3 Eavesdropping strategies 28
3.4 Key-rate analysis 29
3.5 Loopholes and drawbacks of device-dependent quantum key distribution: The need for device-independence 32

4 Device-independent quantum key distribution 35
4.1 Motivation for device-independence 36
4.2 Assumptions in DI-QKD 37
4.3 Advantages of DI-QKD 38
4.4 Security of DI-QKD 39

5 Bell violation and unpredictability 41
5.1 Defining Bell's Inequality 43
5.2 Violation of CHSH Inequality: An example of state $|\phi^+\rangle$ 44
5.3 Implications of P_ε: Linking non-locality and randomness 46

6 Spot-checking CHSH QKD protocol 49
6.1 The Spot-Checking CHSH QKD Protocol 50
6.2 Remarks 52

7 DI-QKD against no signalling eavesdropper 55
7.1 Protocol 56
7.2 Eavesdropping strategies: Individual attacks 58
7.3 Security analysis and key rate 59
7.4 Generalization of the protocol 62
7.5 Analysis of key rate 64

8 DI-QKD using 3-level systems 65
8.1 Introduction 65
8.2 Bell violation for qutrits 66
8.3 Device-independent protocol for qutrits 69

8.4 Eavesdropping strategy and key rate 70
8.5 Conclusion and furthur discussion 74

9 Drawbacks and loopholes of DI-QKD **77**

10 Summary & Conclusions **81**

A Basic probability theory **85**

B BB84: not secure in the device-independent scenario **89**

C Derivation of CHSH inequality **91**

Bibliography **95**

Index **101**

Abstract

Quantum cryptography, also known as quantum encryption, exploits the principles of quantum mechanics to encrypt messages in a way such that it is not possible to be read by anyone except the recipient to which it is sent. It utilizes the advantage of quantum's multiple states, coupled with its "no change theory", to achieve secure encryption, which means it cannot be unknowingly interrupted. The fundamental idea behind the security of quantum cryptography comes from the no-cloning theorem. Whenever an eavesdropper tries to gain information by attacking the quantum channel, she would end up disturbing the state.

One of the best-known examples of quantum cryptography is *quantum key distribution*. Quantum key distribution (QKD) is a cryptographic task that allows two distant parties, Alice and Bob, to exchange secret keys and communicate securely over an untrusted quantum channel (which can be affected by an eavesdropper, Eve), provided they have access to an authenticated classical channel. The basic idea is that, Eve cannot gain any information from the states transmitted from Alice to Bob. Any attempt by her to try and learn information about the key being established, causes discrepancies, leading to Alice and Bob to notice. Once the key is established, it is then typically used for encrypted communication using classical techniques.

The security of the traditional device-dependent quantum key distribution (DD-QKD) protocols is based on several assumptions, the most prominent being that honest users are able to control their devices completely and accurately. Most of these protocols do not consider the fact that the measuring devices cannot be trusted, which causes hidden danger resulting in unsafe quantum communication.

The goal of device-independent quantum key distribution (DI-QKD) is to provide a relaxation, even to the fundamental assumption of devices being truthful. In fact, in this case, no assumption is made on the internal working of the devices. The security is based only on the *observable* behaviour of the devices, i.e. the probabilities of the measurement results given the choice of measurement.

This thesis is an attempt to explore the realm quantum key distribution in the context of device-independence.

Chapter 1

Introduction

Cryptography is the method of securing information and communications such that it can only be accessed by the person for whom it is intended, thus preventing any unauthorized access to information. It involves construction of techniques such as algorithms and protocols based on a set of rules and calculations, which are used to encode messages (or information), in a way that they are hard to decode. This encoded information is difficult to be interpreted by an unwanted party. It is then used to exchange secret messages between two users. Say, a person wishes to buy something online, and therefore provides his credit card number to the selling merchant in exchange of the goods. But, it is possible that the network over which the information flows is insecure, i.e. a third party (known as an adversary or an eavesdropper) can intercept the message and can have access the information related to the credit card that has been sent by the owner. But, if this information is encrypted, it is of no use to the adversary. That's why, cryptography is necessary.

Cryptography has various applications; it can be utilized to ensure the integrity of data (i.e. the received or retrieved information is identical to the information originally sent or stored), to authenticate specific parties (i.e., that the purported sender or author of a message is indeed its real sender or author), to facilitate non-repudiation, and to preserve the confidentiality of information that may have come into the possession of some unauthorized parties.

A principle on which most of the modern day cryptographic schemes are based is

known as *private key cryptography*. In a private key cryptosystem, two parties, commonly known as Alice and Bob, can communicate with each other by sharing a common private key known only to both of them. Alice encrypts her message which she wishes to send to Bob using the key. After encryption, she sends the encrypted information to Bob. Bob then uses the pre-shared key to decrypt Alice's message to recover the information. Therefore, in order to privately share the information among themselves, both Alice and Bob must be able to share a secret key before hand, which would be further used for encryption and decryption.

Unfortunately, classical private key cryptosystem has a major problem: the secure distribution of keys. In a way, the distribution of the key is as difficult as the original problem of secure communication. They have to be delivered in advance via meetings, secure private communication channels, trusted couriers etc. and have to be securely guarded. But, the risk of it being intercepted is still there.

The solution to the problem lies in quantum mechanics. Quantum computing and quantum information is an area which has grown tremendously over the past two decades. It comprises the study and implementation of the information processing tasks that can be efficiently performed using a quantum mechanical system. Quantum computers are able to accomplish computational tasks which are not possible to carry out on classical computers.

One of the most remarkable discoveries in quantum computation and quantum information was that key distribution could be done using the principles of quantum mechanics, in such a way that Alice's and Bob's security is not compromised. This procedure is known as *quantum cryptography*. One of the best-known example of quantum cryptography is *quantum key distribution*. It is based on the framework of private key cryptosystem. It exploits the quantum mechanical principle that an observation in general, disturbs the system being observed. Thus, if an eavesdropper Eve is listening in, as Alice and Bob attempt to transmit their key, the presence of the eavesdropper will be visible as a disturbance over the communication channel being used to establish the key, which can be detected during the key sharing process.

We elaborate this idea of quantum key distribution over the next chapters of this thesis.

1.1 Organization of the thesis

This thesis deals with the analysis of quantum key distribution in the context of device-independence. The organization of the thesis is described as follows:

Chapter 2 provides an introduction to basic information theory. It includes the fundamental algebraic relationships of entropy, relative entropy and mutual information from a classical as well as a quantum point of view. Various properties and applications of entropy are also discussed. We also review the concept of accessible information, and analyze an upper bound for it, which is strongly used in the security analysis of various QKD protocols.

Chapter 3 emphasizes on a detailed analysis of standard device-dependent quantum key distribution (DD-QKD) and some of its protocols. We also give a brief outline of some strategies that could be used by an eavesdropper, to attack the quantum channel to acquire the information shared between Alice and Bob. Some loopholes and drawbacks of these QKD techniques are pointed out, which makes it necessary to develop device-independent quantum key distribution schemes.

Chapter 4 provides an introduction to device-independent quantum key distribution, and describes the necessary assumptions required to allow secure quantum key distribution in device-independent context. It also provides an overview of some of its advantages over DD-QKD.

Chapter 5 defines the Bell's inequality and provides an interpretation of the relation between its violation and unpredictability.

In Chapter 6, the basic spot-checking device-independent protocol based on the Clauser-Horne-Shimony-Holt (CHSH) inequality is discussed.

In Chapter 7, we analyze a device-independent quantum key distribution scheme secure against eavesdropping attacks limited by only the no-signalling principle.

We extend our study of the concept of device-independence to qutrits (3-level systems) and qudits (d-level systems) in Chapter 8. We analyze the security of such schemes, and provide a relation between noise resistance and dimension of quantum systems used in the protocol.

Chapter 9 emphasizes on some drawbacks and loopholes in the physical implementations of DI-QKD techniques, and provides some possible strategies to overcome those shortcomings.

Chapter 10 presents a summary of the thesis with conclusions, and suggests some possible future directions in the field of device-independence.

Appendix A provides a brief outline of basic probability theory. Appendix B and C contain some derivations and proofs of some concepts used in the thesis.

Chapter 2

Information theory and entropy

Information theory deals with the analysis and mathematical modelling of a communication system. It is a branch of applied mathematics, computer science and electrical engineering, and is widely used in many fields (see Figure 2.1). It was developed by Claude E. Shannon in 1948, in his paper "*A mathematical theory of communication*" [Shannon 01]. He formulated the laws of data compression and transmission, which formed the basis of information theory. This chapter provides an overview of various concepts of information theory such as entropy and mutual information, which are very well utilized in quantum information.

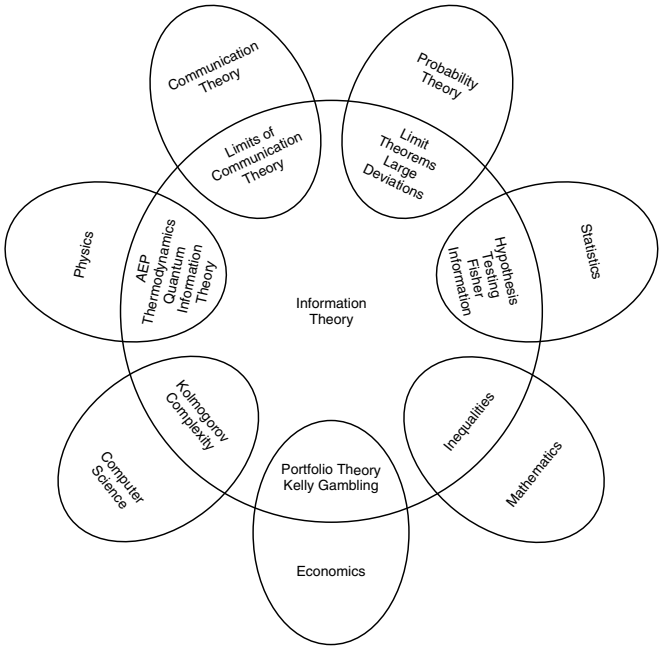

Figure 2.1: Relation of information theory to other fields [Cover 06]

2.1 Shannon's entropy

Entropy refers to the measure of uncertainty in the state of a particular physical system. Suppose, a discrete random variable X in a set $\mathcal{X}$ has probability mass function $p_X(x) = \Pr\{X = \mathrm{x}\}$ with $x \in \mathcal{X}$. The Shannon entropy for X is defined as follows.

Definition 2.1.1. [Cover 06] The *Shannon's entropy* $H(X)$ of a discrete random variable X, associated with a probability distribution $p_X(x)$ is defined by

$$H(X) = H(p_1(x), p_2(x), ..., p_n(x)) = -\sum_{x\in\mathcal{X}} p_X(x)\log_2\, p_X(x). \tag{2.1}$$

The entropy is expressed in *bits*. For example, for a fair coin, $p(\text{Head}) = p(\text{Tail}) = \frac{1}{2}$. Therefore, the entropy for a fair coin toss is given by $H(X) = -[p_{Head}\, \log_2\, p_{Head} + p_{Tail}\, \log_2\, p_{Tail}] = -[\frac{1}{2}\log_2\frac{1}{2} + \frac{1}{2}\log_2\frac{1}{2}] = 1$ bit. Also, the convention $0\log_2 0 = 0$ is used, as $\lim_{x\to 0} x\log_2 x = 0$. This is because, an event with $p_X(x) = 0$ (*this event can never occur*) should not have a contribution in the calculation of entropy.

If the probability distribution associated with a random variable X is $p_X(x)$, then the expectation value E of another random variable $f(X)$ is given by:

$$E(f(X)) = \sum_{x\in\mathcal{X}} f(x)p_X(x). \tag{2.2}$$

The entropy of X can also be represented in terms of the expectation value of a random variable $f(X) = \log_2 \frac{1}{p(X)}$ as:

$$H(X) = E\, \log_2 \frac{1}{p(X)}. \tag{2.3}$$

Lemma 2.1.1. *The entropy for a discrete random variable X is non-negative, i.e. $H(X) \geq 0$.*

Proof. Since probability $p_X(x)$ lies between 0 and 1, so $\frac{1}{p_X(x)} \geq 1$. This implies, $\log_2 \frac{1}{p_X(x)} \geq 0$. Therefore by equation (2.3), $H(X) \geq 0$. □

Some of the basic properties of entropy are discussed in the following section.

2.2 Properties of entropy

2.2.1 Binary entropy

The *binary entropy* is defined for random variables, for which only two outcomes are possible. Say, the probability of one of the outcome of a random variable is p. So, the other outcome occurs with a probability $(1-p)$, and therefore the binary entropy is defined as:

$$H_{binary}(p) = -p\log_2(p) - (1-p)\log_2(1-p). \tag{2.4}$$

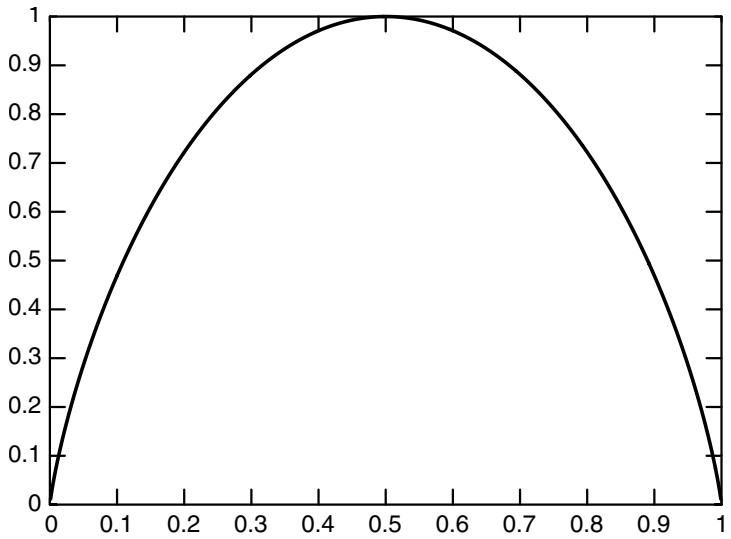

Figure 2.2: Binary entropy H_{binary} *vs* p

From Figure 2.2, we see that the binary entropy is a *concave* function, with $H_{binary}(p) = 0$ for $p = 0$ or 1. The maximum value for $H_{binary}(p)$ is 1 which occurs at $p = 0.5$. Also, $H_{binary}(p) = H_{binary}(1-p)$.

2.2.2 Joint entropy

The entropy for a single discrete random variable X has been defined in the previous section. Now, we extend the concept of entropy to two variables.

Definition 2.2.1. For a pair of random variables (X, Y), with joint probability dis-

tribution $p(x, y)$, the *joint entropy* $H(X, Y)$ is defined as:

$$H(X, Y) = -\sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log_2 p(x, y). \tag{2.5}$$

The joint entropy is the measure of total uncertainty of the pair (X, Y). The above definition can now be extended to any number of random variables. Also, we note that $H(X, Y) = H(Y, X)$.

2.2.3 Relative entropy

Definition 2.2.2. The *relative entropy* is a measure that provides us with the distance between two probability distributions. Say, there are two probability distributions, $p(x)$ and $q(x)$. The relative entropy of $p(x)$ to $q(x)$ is given by:

$$H(p(x)||q(x)) \equiv \sum_{x \in \mathcal{X}} p(x) \log_2 \frac{p(x)}{q(x)}. \tag{2.6}$$

In terms of the Shannon entropy, relative entropy can be written as follows:

$$\begin{aligned} H(p(x)||q(x)) &= \sum_{x \in \mathcal{X}} p(x) \log_2 p(x) - \sum_{x \in \mathcal{X}} p(x) \log_2 q(x) \\ &= -H(X) - \sum_{x \in \mathcal{X}} p(x) \log_2 q(x). \end{aligned} \tag{2.7}$$

The relative entropy is also referred as *Kullback–Leibler distance* between the probability distributions $p(x)$ and $q(x)$.

Theorem 2.2.1. ***(Information inequality)*** *Let $p(x)$ and $q(x)$ be two probability distributions, with $x \in \mathcal{X}$, then the relative entropy $H(p(x)||p(y)) \geq 0$, with equality iff $p(x)$ and $q(x)$ are equal $\forall$ x.*

Proof. Using the definition of relative entropy from equation (2.6),

$$H(p(x)||q(x)) = \sum_{x \in \mathcal{X}} p(x) \log_2 \frac{p(x)}{q(x)} = -\sum_{x \in \mathcal{X}} p(x) \log_2 \frac{q(x)}{p(x)}.$$

Since, $\log_2 x \ \ln 2 = \ln x \leq x-1$, therefore,

$$H(p(x)||q(x)) = -\sum_{x\in\mathcal{X}} p(x)\log_2\frac{q(x)}{p(x)} \geq \frac{1}{\ln 2}\sum_{x\in\mathcal{X}} p(x)\Big(1-\frac{q(x)}{p(x)}\Big) \tag{2.8}$$

$$= \frac{1}{\ln 2}\sum_{x\in\mathcal{X}}(p(x)-q(x))$$

$$= \frac{1}{\ln 2}\Big(\sum_{x\in\mathcal{X}} p(x) - \sum_{x\in\mathcal{X}} q(x)\Big)$$

$$= \frac{1}{\ln 2}(1-1) = 0. \tag{2.9}$$

Therefore, $H(p(x)||q(x)) \geq 0$, and the equality holds iff $\frac{q(x)}{p(x)} = 1$ in equation (2.8), implying that $p(x) = q(x)\ \forall\ x$. □

2.2.4 Conditional entropy

Suppose, we are given a pair of discrete random variables X and Y. The measure of the total uncertainty about the pair (X,Y) is given by the joint entropy (refer Subsection 2.2.2). But, say we know the value of X; therefore we have $H(X)$ bits of information about (X,Y), and therefore the pair (X,Y) loses some uncertainty. The remaining uncertainty about the pair (X,Y), provided that we know X, is given by the *conditional entropy* $H(X|Y)$. It is defined as :

$$H(Y|X) = H(X,Y) - H(X). \tag{2.10}$$

It is the measure of uncertainty in Y, given that we know X.

Corollary. *For three discrete random variables X, Y and Z,*

$$H(X,Y|Z) = H(X|Z) + H(Y|X,Z). \tag{2.11}$$

Proof. Using equation (2.10), we have

$$H(X,Y|Z) = H(X,Y,Z) - H(Z). \tag{2.12}$$

Adding and subtracting $H(X, Z)$ to the right hand side of the above equation gives

$$H(X, Y|Z) = H(X, Y, Z) - H(X, Z) + H(X, Z) - H(Z).$$

Again, by equation (2.10), we get,

$$H(X, Y|Z) = H(X, Y|Z) + H(X|Z).$$

□

2.2.5 Mutual information

Definition 2.2.3. Suppose, we have two discrete random variables X and Y, with probability mass functions $p(x)$ and $p(y)$ respectively, and a joint probability distribution $p(x, y)$. The *mutual information* $I(X : Y)$ is defined as the relative entropy between the joint distribution $p(x, y)$ and the product of individual probability distributions $p(x)p(y)$:

$$I(X : Y) = \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} p(x, y) \log_2 \frac{p(x, y)}{p(x)p(y)} \tag{2.13}$$

$$= H(p(x, y)||p(x)p(y)). \tag{2.14}$$

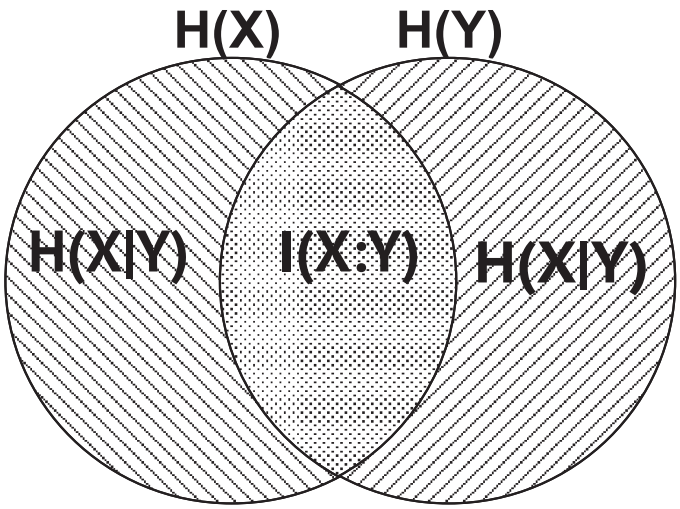

Figure 2.3: Relationship between different types of entropies [Nielsen 11]

The mutual information $I(X : Y)$ is the measure of the information that is common

to both X and Y. It could be re-written as follows:

$$\begin{aligned} I(X:Y) &= \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log_2\frac{p(x,y)}{p(x)p(y)} \\ &= \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log_2\frac{p(x|y)}{p(x)} \\ &= \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log_2 p(x|y) - \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log_2 p(x) \end{aligned} \tag{2.15}$$

$$I(X:Y) = H(X) - H(X|Y). \tag{2.16}$$

Now, using the definition of conditional entropy from equation (2.10), we get

$$I(X:Y) = H(X) + H(Y) - H(X,Y). \tag{2.17}$$

Replacing Y with X in equation (2.16), we get the mutual information of a random variable with itself (also referred as *self-information*) as:

$$I(X:X) = H(X) - H(X|X) = H(X), \tag{2.18}$$

since $H(X|X) = 0$. Therefore, entropy is also called as self-information. From equation (2.17), it is also clear that $I(X:Y) = I(Y:X)$.

Corollary. *(**Non-negativity of Mutual Information**) For any two discrete random variables X and Y, the mutual information $I(X:Y) \geq 0$, with equality iff X and Y are independent.*

Proof. From equations (2.13) and (2.14),

$$I(X:Y) = H(p(x,y)||p(x)p(y)) = \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\log_2\frac{p(x,y)}{p(x)p(y)}.$$

We have already proved in Theorem 2.2.1, that relative entropy $H(p(x)p(y)) \geq 0$. Therefore, $I(X:Y) \geq 0$. If X and Y are independent, then $p(x,y) = p(x)p(y)$, and since $\log_2 1 = 0$, the equality holds. □

Another property commonly used in information theory is the *conditional mutual*

information, which is defined as the reduction in uncertainty in X due to knowledge of Y, when Z is given.

Definition 2.2.4. The conditional mutual information of random variables X and Y, given another random variable Z, is given by

$$I(X:Y|Z) = H(X|Z) - H(X|Y,Z). \tag{2.19}$$

We also define chain rule for entropy and mutual information.

Theorem 2.2.2. *(**Chain rule for entropy**) Let $X_1, X_2, ..., X_n$ be a set of random variables. Then the combined entropy of the collection is given by*

$$H(X_1, X_2, ..., X_n) = \sum_{j=1}^{n} H(X_j|X_{j-1}, ..., X_1). \tag{2.20}$$

Proof. The repeated application of the relation between joint entropy and conditional entropy, defined by equation (2.10), gives

$$H(X_1, X_2) = H(X_1) + H(X_2|X_1) \tag{2.21}$$

$$H(X_1, X_2, X_3) = H(X_1) + H(X_2, X_3|X_1) \tag{2.22}$$

$$= H(X_1) + H(X_2|X_1) + H(X_3|X_2, X_1). \tag{2.23}$$

This generalizes for n random variables as

$$H(X_1, X_2, ..., X_n) = H(X_1) + H(X_2|X_1) + ... + H(X_n|X_{n-1}, ..., X_1) \tag{2.24}$$

$$= \sum_{j=1}^{n} H(X_j|X_{j-1}, ..., X_1). \tag{2.25}$$

□

Theorem 2.2.3. *(**Chain rule for mutual information**) For a set of random variables, $X_1, X_2, ..., X_n$ and Y,*

$$I(X_1, X_2, ..., X_n : Y) = \sum_{j=1}^{n} I(X_j : Y|X_{j-1}, X_{j-2}, ..., X_1). \tag{2.26}$$

Proof. Using the definition of mutual information given in equation (2.16), we have

$$I(X_1, X_2, ..., X_n : Y) = H(X_1, X_2, ..., X_n) - H(X_1, X_2, ..., X_n|Y). \tag{2.27}$$

Now, using the chain rule of entropy defined by equation (2.20), we get

$$I(X_1, X_2, ..., X_n : Y) = \sum_{j=1}^{n} H(X_j|X_{j-1}, ..., X_1) - \sum_{j=1}^{n} H(X_j|X_{j-1}, ..., X_1, Y) \tag{2.28}$$

$$= \sum_{j=1}^{n} I(X_j : Y|X_{j-1}, X_{j-2}, ..., X_1). \tag{2.29}$$

□

2.3 Data-processing inequality

The notion of data-processing inequality comes from the idea of *Markov chain* of random variables. Suppose there are three random variables X, Y and Z. They are said to form a Markov Chain $X \to Y \to Z$, in that order, if the conditional distribution of Z depends only on X, and is independent of Y. More formally, the joint probability distribution function of X, Y and Z can be written as

$$p(x, y, z) = p(x)p(y|z)p(z|y). \tag{2.30}$$

Also, $X \to Y \to Z$, iff X and Z are conditionally independent. This is because,

$$p(x, z|y) = \frac{p(x, y, z)}{p(y)} = \frac{p(x, y)p(z, y)}{p(y)} = p(x|y)p(z|y). \tag{2.31}$$

Theorem 2.3.1. *(**Data-processing inequality**) Say, $X \to Y \to Z$, then*

$$H(X) \geq I(X : Y) \geq I(X : Z). \tag{2.32}$$

This states that if a random variable X is subject to some noise, producing an output Y, then any data-processing by us on Y cannot be used to increase the information that Y contains about the original information X.

Proof. By equation (2.5),

$$H(X,Y) = -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\ \log_2 p(x,y) \tag{2.33}$$

$$= -\sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\ \log_2 p(y)p(x|y) \tag{2.34}$$

$$= -\sum_{y\in\mathcal{Y}} p(y)\ \log_2 p(y) - \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\ \log_2 p(x|y) \tag{2.35}$$

$$H(X,Y) = H(Y) - \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} p(x,y)\ \log_2 p(x|y). \tag{2.36}$$

Since, $0 \leq p(y|x) \leq 1$, $\log_2\ p(x|y)) \leq 0$. This implies,

$$H(X,Y) - H(Y) \geq 0. \tag{2.37}$$

Adding $-H(X)$ to both sides of the above equation and using equation (2.17), we get:

$$H(X) \geq I(X:Y). \tag{2.38}$$

To prove the second part of the inequality, we use the chain rule of mutual information given by equation (2.26),

$$I(X:Y,Z) = I(X:Z) + I(X:Y|Z). \tag{2.39}$$

Also,

$$I(X:Y,Z) = I(X:Y) + I(X:Z|Y). \tag{2.40}$$

Since $X \to Y \to Z$ forms a Markov chain, X and Z are conditionally independent of Y. Therefore, $I(X:Z|Y) = 0$. And mutual information is non-negative, so $I(X:Y|Z) \geq 0$. Thus, by comparing equations (2.39) and (2.40), we have

$$I(X:Y) \geq I(X:Z).$$

□

2.4 Von Neumann entropy

Similar to the Shannon entropy as a measure of uncertainty for classical probability distributions, entropy is also defined for quantum systems.

Definition 2.4.1. For a quantum state, represented by a density operator ρ, *von Neumann entropy* is defined as:

$$S(\rho) \equiv -Tr(\rho \log_2 \rho). \tag{2.41}$$

Lemma 2.4.1. *Given a state ρ, with eigenvalues λ_x, the von Neumann entropy could be expressed as:*

$$S(\rho) = -\sum_x \lambda_x log_2 \lambda_x. \tag{2.42}$$

Proof. Let the set $\{|x\rangle\}$ be the basis vectors of the state ρ. Then, its spectral decomposition ρ is given as:

$$\rho = \sum_x \lambda_x |x\rangle\langle x|, \tag{2.43}$$

where λ_x are the eigenvalues of ρ. Then,

$$\log_2\rho = \log_2 \big(\sum_x \lambda_x |x\rangle\langle x| \big) \tag{2.44}$$

$$= \big(\sum_x \log_2\lambda_x |x\rangle\langle x| \big) \tag{2.45}$$

$$-\rho\log_2\rho = -\sum_x \log_2\lambda_x \big(\rho|x\rangle\langle x|\big). \tag{2.46}$$

From equation (2.41),

$$S(\rho) = -Tr(\rho \log_2 \rho) = -Tr\big\{ \sum_x \log_2\lambda_x \big(\rho|x\rangle\langle x|\big)\big\} \tag{2.47}$$

$$= -Tr\big\{ \sum_x \log_2\lambda_x \big(\sum_y \lambda_y |y\rangle\langle y|x\rangle\langle x|\big)\big\} \tag{2.48}$$

$$= -\sum_x \log_2\lambda_x \Big[\lambda_x \big\{Tr|x\rangle\langle x|\big\}\Big]. \tag{2.49}$$

Since $\{|x\rangle\}$ are the set of basis vectors of the state ρ, therefore $\sum_x Tr(|x\rangle\langle x|) = 1$.

So,

$$S(\rho) = -\sum_x \lambda_x \log_2 \lambda_x. \tag{2.50}$$

□

Similar to the Shannon entropy (refer Section 2.1), the von Neumann entropy for any density operator ρ is non-negative:

$$S(\rho) \geq 0. \tag{2.51}$$

The joint entropy for a composite quantum system with two components A and B is defined as $S(A, B) \equiv -Tr(\rho_{AB} \log_2 \rho_{AB})$, where ρ_{AB} is the density matrix of the joint system AB. Also, the conditional information and mutual information for quantum systems are defined in a similar way, as was defined for the Shannon entropy (refer Section 2.2):

$$S(A|B) \equiv S(A, B) - S(B), \tag{2.52}$$

$$S(A : B) \equiv S(A) + S(B) - S(A, B). \tag{2.53}$$

2.4.1 Entropy of a mixture

Theorem 2.4.2. *[Nielsen 11] Suppose a mixture of quantum states is given by $\rho = \sum_j p_j \rho_j$, with probabilities p_j and density operators ρ_j. The entropy of the mixture ρ is bounded as follows:*

$$S(\rho) \leq \sum_j p_j S(\rho_j) + H(p_j). \tag{2.54}$$

The equality holds iff the states ρ_j have orthogonal subspaces.

Proof. Let's suppose that ρ_j are density operators for pure states, i.e. $\rho_j = |\phi_j\rangle\langle\phi_j|$ for a system J. An auxiliary system K is introduced, with orthonormal basis $|j\rangle$, corresponding to the index j of the probabilities p_j. We define a joint system JK, with a state $|JK\rangle$ given by

$$|JK\rangle = \sum_j \sqrt{p_j} |\phi_j\rangle |j\rangle. \tag{2.55}$$

$|JK\rangle$ is a pure state, therefore by Schmidt decomposition, the eigenvalues of the density operators of system J and K are the same. This implies

$$S(K) = S(J) = S\Big(\sum_j p_j |\phi_j\rangle\langle\phi_j|\Big) = S\Big(\sum_j p_j \rho_j\Big) = S(\rho). \tag{2.56}$$

Suppose α_j^i are the eigenvalues and $|\alpha_j^i\rangle$ are the eigenvectors of ρ_j. For $\sum_j p_j\rho_j$, the eigenvectors remain the same, but eigenvalues equal $p_j\alpha_j^i$. Therefore, by equation (2.42),

$$S\Big(\sum_j p_j\rho_j\Big) = -\sum_{ij} p_j\alpha_j^i \log_2 p_j\alpha_j^i, \tag{2.57}$$

$$= -\sum_j p_j \log_2 p_j - \sum_j p_j \sum_i \alpha_j^i \log_2 \alpha_j^i, \tag{2.58}$$

$$= H(p_j) + \sum_j p_j S(\rho_j). \tag{2.59}$$

On performing a projective measurement on system K in $|j\rangle$ basis, the state (of system K) becomes $\rho^{\tilde{K}}$, where

$$\rho^{\tilde{K}} = \sum_j p_j |j\rangle\langle j|. \tag{2.60}$$

The entropy for this state is equal to $S(\rho^{\tilde{K}}) = H(p_j)$. The entropy does not decrease on a projective measurement (refer [Nielsen 11]), therefore $S(\rho) = S(K) \leq S(\rho^{\tilde{K}}) = H(p_j)$. Since ρ_j are pure, $S(\rho_j) = 0$. Combining this result with equation (2.59) provides the required bound for pure states ρ_j,

$$S(\rho) \leq \sum_j p_j S(\rho_j) + H(p_j). \tag{2.61}$$

We now prove the case for the mixed states. Let $\rho_j = \sum_k p_k^j |e_k^j\rangle\langle e_k^j|$ be an orthonormal decomposition for the states ρ_j. So $\rho = \sum_{jk} p_j p_k^j |e_k^j\rangle\langle e_k^j|$. Now, using $\sum_k p_k^j$=1 and

equation (2.61), we get,

$$S(\rho) \leq -\sum_{jk} p_j p_k^i \log_2(p_j p_k^j) \tag{2.62}$$

$$= -\sum_j p_j \log_2 p_j - \sum_j p_j \sum_j p_j \log_2 p_j \tag{2.63}$$

$$= H(p_j) + \sum_j S(\rho_j). \tag{2.64}$$

In both pure and mixed state cases, the equality holds iff $K = \tilde{K}$, which happens only when $|\phi_j\rangle$ are orthogonal. □

2.5 Accessible information

We consider here two parties, Alice and Bob. Say, Alice prepares a quantum state according to a random variable $X = 0, 1, ..., n$, represented by the ensemble $\mathcal{E} \equiv \{p_X(x), \rho_x\}$. Bob wants to determine the value of X, so he performs a POVM $\{M_y\}$ on the state given to him and gets a result Y. The measure of information that he can gain about X, knowing the measurement result Y is the mutual information $I(X : Y)$. Here, Bob can choose the measurement that he wants to perform, and he would like to perform a measurement that maximizes the mutual information $I(X : Y)$, which in result maximizes his information about X. Therefore, Bob's *accessible information* is the *maxima* of the mutual information $I(X : Y)$ over all possible measurements that can be performed by Bob [Nielsen 11]:

$$I_{acc}(\mathcal{E}) = \max I(X : Y). \tag{2.65}$$

The next section provides a natural bound on the accessible information of Bob.

2.6 Holevo bound

Holevo bound establishes an upper bound on the amount of information than can be retrieved about a quantum state. Thus, it bounds the accessible information. It is defined by the following theorem:

Theorem 2.6.1. *[Cover 06] (**The Holevo bound**) Suppose Alice prepares a state from an ensemble* $\mathcal{E} \equiv \{p_X(x), \rho_X(x)\}$, *where* $X = 0,1,...,n$, *and* $p_i(x)$ *is the probability with which state* $\rho_i(x)$ *is prepared. Bob performs a POVM described by* $\{M_y\} = \{M_0,M_1,...,M_m\}$ *on the state prepared by Alice, and gets a measurement outcome* Y. *The Holevo bound states that for any of the possible measurements that could be performed by Bob:*

$$I(X:Y) \leq \chi. \tag{2.66}$$

Here $\chi = S(\rho) - \sum_x p_x S(\rho_x)$ *is the Holevo quantity, where* $\rho = \sum_x p_x \rho_x$.

Proof. Suppose there are 3 quantum systems J, K and L, where J and L are auxiliary systems, and system K is given to Bob by Alice. Let J be the *preparation* system, with an orthonormal basis $|x\rangle$, where the basis elements describe the possible preparations corresponding to the labels 0,1,...,n. L is Bob's measuring device, with basis $|y\rangle$, where the basis elements describe the possible outcomes of Bob's measurement (1,2,...,n). The combined initial state of the three systems can be represented as:

$$\rho^{JKL} = \sum_x p_x |x\rangle\langle x| \otimes \rho_x \otimes |0\rangle\langle 0|. \tag{2.67}$$

A trace-preserving quantum operation $\mathcal{E}$ on system K and L, represents the POVM measurements described by $\{M_y\}$ on J, and store the measurement outcomes in K:

$$\mathcal{E}(\delta \otimes |0\rangle\langle 0|) = \sum_z \sqrt{M_y}\delta\sqrt{M_y} \otimes |y\rangle\langle y|. \tag{2.68}$$

Here, δ is a state of K, and $|0\rangle$ is the initial state of the measurement device. Suppose the states of the system JKL, before and after the quantum operation $\mathcal{E}$ are represented by $\{J, K, L\}$ and $\{\tilde{J},\tilde{K},\tilde{L}\}$ respectively. Since, applying a quantum operation $\mathcal{E}$ on KL cannot increase the mutual information between J and KL, therefore,

$$S(\tilde{J} : \tilde{K}, \tilde{L}) \leq S(J : K, L). \tag{2.69}$$

Also, removing a system cannot increase the mutual information, so,

$$S(\tilde{J} : \tilde{K}) \leq S(\tilde{J} : \tilde{K}, \tilde{L}). \tag{2.70}$$

Combing equations (2.69) and (2.70), we get:

$$S(J:K) \geq S(\tilde{J}:\tilde{K}). \tag{2.71}$$

The combined state of systems $\tilde{J}$, $\tilde{K}$ and $\tilde{L}$ is represented as:

$$\rho^{\tilde{J}\tilde{K}\tilde{L}} = \sum_{x,y} p_x |x\rangle\langle x| \otimes \sqrt{M_y}\rho_x\sqrt{M_y} \otimes |y\rangle\langle y|. \tag{2.72}$$

Tracing out system $\tilde{K}$ gives,

$$\begin{aligned}
\rho^{\tilde{J},\tilde{L}} = Tr_{\tilde{K}}(\rho^{\tilde{J}\tilde{K}\tilde{L}}) &= Tr_{\tilde{K}}(\sum_{x,y} p_x |x\rangle\langle x| \otimes \sqrt{M_y}\rho_x\sqrt{M_y} \otimes |y\rangle\langle y|) \qquad (2.73)\\
&= \sum_{x,y} |x\rangle\langle x| \otimes p_x Tr\big(\sqrt{M_y}\rho_x\sqrt{M_y}\big) \otimes |y\rangle\langle y| \\
&= \sum_{x,y} |x\rangle\langle x| \otimes p_x Tr\big(\rho_x M_y\big) \otimes |y\rangle\langle y| \\
&= \sum_{x,y} p_x p(y|x) |x\rangle\langle x| \otimes |y\rangle\langle y| \\
\rho^{\tilde{J},\tilde{L}} &= \sum_{x,y} p(x,y) |x\rangle\langle x| \otimes |y\rangle\langle y|. \qquad (2.74)
\end{aligned}$$

Therefore,

$$S(\tilde{J}:\tilde{L}) = H(X:Y). \tag{2.75}$$

The combined state of systems J and K is represented as:

$$\rho^{JK} = \sum_x p_x |x\rangle\langle x| \otimes \rho_x. \tag{2.76}$$

Using the results from Theorem 2.4.2, we get $S(J) = H(p_x)$, $S(K) = S(\rho)$, and $S(J,K) = H(p_x) + \sum_x p_x S(\rho_x)$. So,

$$S(J:K) = S(J) + S(K) - S(J,K) = S(\rho) - \sum_x p_x S(\rho_x) = \chi. \tag{2.77}$$

Comparing equations (2.71), (2.75) and (2.77) gives us the required Holevo bound. □

The Holevo bound is a crucial result which is used in the proof of various arguments

and calculations in quantum information. One of the its fundamental applications is its use in the calculation of the key rates for various QKD protocols, as discussed in the upcoming chapters.

Chapter 3

Quantum key distribution

3.1 Introduction

Quantum key distribution (QKD) protocols allows two separated parties (say Alice and Bob) to share secure private keys over a public channel. The security of the key is guaranteed by the laws of quantum mechanics, given that the error rate is below a certain threshold. The basic idea behind QKD is that an eavesdropper (Eve) cannot gain any information from the quantum state transmitted by Alice to Bob without causing a disturbance in their state. By no-cloning principle, it is impossible for Eve to make a perfect copy of Alice's qubit. Therefore, any attempt by Eve to obtain information from the quantum channel between Alice and Bob will cause some disturbance, which can be detected by the users.

Proposition 3.1.1. *[Nielsen 11] (**Information gain implies disturbance**) In order to distinguish between 2 non-orthogonal states, any information gain is possible only at the cost of introducing disturbance to the state.*

Proof. Suppose $|\phi_1\rangle$ and $|\phi_2\rangle$ are two non-orthogonal quantum states, and an eavesdropper Eve is trying to obtain information about the states. Without any loss of generality, we can assume that while obtaining the information, Eve unitarily interacts its own system with the states $|\phi_1\rangle$ or $|\phi_2\rangle$ by introducing an ancilla ($|u\rangle$). It is

assumed that this process does not disturb the states. We get:

$$|\phi_1\rangle|u\rangle \rightarrow |\phi_1\rangle|v'\rangle \tag{3.1}$$

$$|\phi_2\rangle|u\rangle \rightarrow |\phi_2\rangle|v'\rangle \tag{3.2}$$

In order to obtain some information about the states, Eve would want $|v\rangle$ and $|v'\rangle$ to be non-identical. Now since the unitary transformation preserves norm, we can write

$$\begin{aligned} \langle\phi_2|\phi_1\rangle\langle v|v'\rangle &= \langle\phi_2|\phi_1\rangle\langle u|u\rangle \\ \langle v|v'\rangle &= \langle u|u\rangle \\ &= 1 \end{aligned} \tag{3.3}$$

and therefore, $|v\rangle$ and $|v'\rangle$ must be identical. Thus, distinguishing between two non-orthogonal will surely disturb at least one of the two states. □

This idea of transmitting non-orthogonal states from Alice to Bob is used further as the basic underlining principle for quantum key distribution. By checking the disturbance caused in the transmitted states, an upper bound can be established on the noise (or eavesdropping) that's being occurring in the channel, such that, if the noise is below a certain threshold, they perform information reconciliation and privacy amplification to obtain a shared secret key; and if it's above the threshold, they abort the protocol and start it over again. The threshold for the maximum amount of tolerable error depend upon the efficacy of the information reconciliation and privacy amplification protocols.

Having developed the intuition behind quantum key distribution, we discuss some of its protocols in the following section.

3.2 Protocols for quantum key distribution

Although, quantum key distribution came into light after the formulation of BB84 protocol by Charles Bennet and Gilles Brassard in 1984, the use of quantum techniques in context of security can be found since 1970's. Since then, many quantum key distribution protocols have been formulated till date, with rigorous security proofs.

Generally, quantum key distribution protocols are of two types:

- **Prepare and Measure**: Here, the transmitting user Alice encodes the optical signals using a discrete random variable, such as a bit. The encoded optical signals are then sent to the receiving user, Bob. Bob then performs a measurement on the received bits in order to retrieve the information sent by Alice.

- **Entanglement-based**: In this case, entanglement is used as the basis for performing quantum key distribution. Here, a single source emits a pair of entangled particles (such as polarized photons), which are then separated and sent to both Alice and Bob, who then perform measurements by choosing a random basis, to generate a key.

We discuss here two most conventional QKD protocols: BB84 protocol and EPR protocol. The BB84 protocol is based on the prepare and measure scheme, whereas the EPR protocol is based on the entanglement-based scheme.

3.2.1 BB84 Protocol

The first quantum cryptographic protocol was the BB84 protocol, developed by Bennett and Brassard [Bennett 84] in 1984, as the name suggests. In this protocol, photon polarization states are utilized to transmit the information between the two users. The protocol [Nielsen 11] is as follows:

- Alice creates two strings a and b, each of $4n$-random classical bits. She encodes the strings as a block of $4n$ qubits.

$$\psi = \bigotimes_{i=1}^{4n} |\psi_{a_i b_i}\rangle \tag{3.4}$$

  where $a_i(b_i)$ is the i^{th} bit of $a(b)$, and each qubit is one of the following four

states:

$$|\psi_{00}\rangle = |0\rangle \tag{3.5}$$

$$|\psi_{10}\rangle = |1\rangle \tag{3.6}$$

$$|\psi_{01}\rangle = |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \tag{3.7}$$

$$|\psi_{11}\rangle = |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \tag{3.8}$$

The above process simply effects in encoding a in $\mathbb{Z}$ or $\mathbb{X}$ basis, which is determined by b.

- After encoding the bits into qubits, she sends the resulting state to Bob.

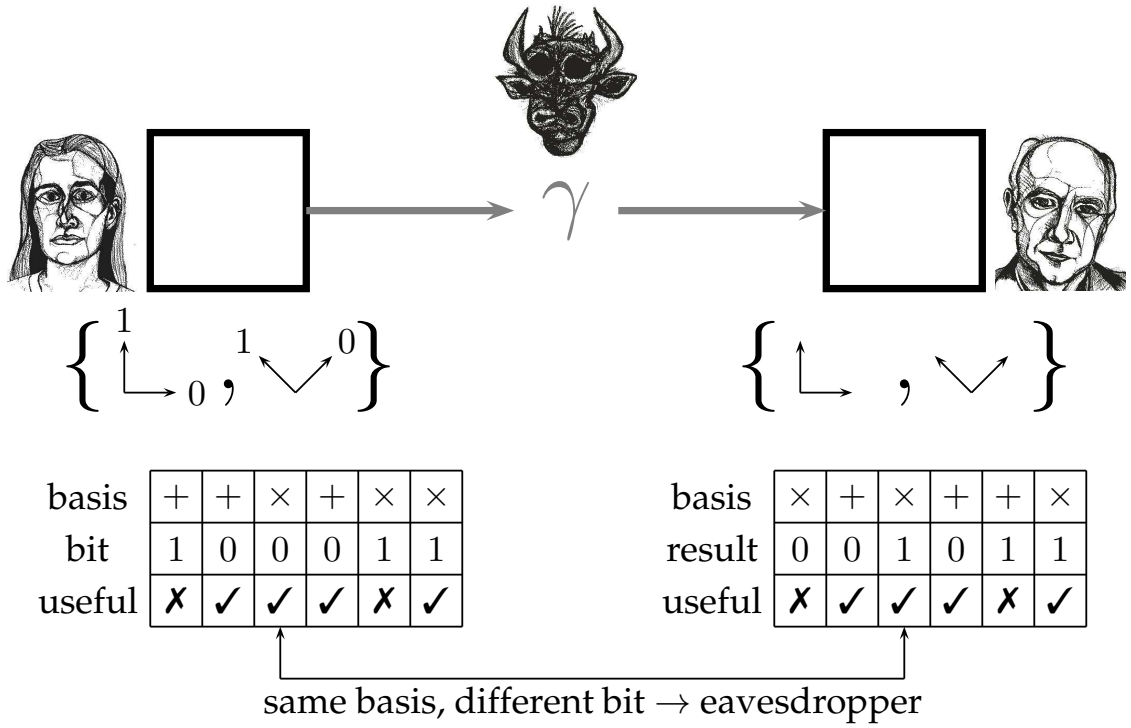

Figure 3.1: The BB84 quantum key distribution protocol [Hänggi 10]

- Upon receiving the qubits, Bob announces this fact, and measures the received qubits randomly in $\mathbb{X}$ or $\mathbb{Z}$ basis.
- Alice announces b over a public channel.
- Over the public channel, Alice and Bob check and discard the bits in which Bob made a measurement in different basis than the one in which Alice prepared. Assuming n is very large, they are left with approximately $2n$ bits.

- Now to check the noise or eavesdropping in the channel, Alice randomly selects n bits (of her $2n$ bits) that serve as check bits, and publicly announces the selection. Alice and Bob, both compare their values among the check bits (see Figure 3.1). If the error rate is above a certain threshold, then they'll abort the protocol, otherwise they'll continue.

- Alice and Bob together performs information reconciliation and privacy amplification on their remaining n bits to get an m-bit shared key.

3.2.2 The EPR Protocol

The EPR scheme [Ekert 91] was proposed by Ekert in 1991. The security of this protocol is based on a different property of quantum physics known as *entanglemnet*. It uses entangled pairs of photons, which are distributed such that one pair of photon is with Alice, and other pair with Bob. The entangled states should be perfectly correlated. The protocol is as follows:

- Alice prepares $4n$ pairs of the following EPR state,

$$|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{3.9}$$

  (This state is chosen because it's rotationally invariant, and will give perfect correlations irrespective of the basis the state is measured.)

- She sends the second pair of the qubit to Bob over a quantum channel.

- Alice and Bob measures their qubits randomly in S_z $\{|+\rangle, |-\rangle\}$ or S_x $\{|0\rangle, |1\rangle\}$ basis.

- Over the public channel, they perform basis reconciliation. Given that n is very large, they are left with $2n$ bits.

- Alice randomly selects n bits that will serve as check bits. Then, they'll check their values as well as the correlations corresponding to them. If the error rate is above a certain threshold, then they'll abort the protocol, otherwise they'll continue.

- Alice and Bob together performs information reconciliation and privacy ampli-

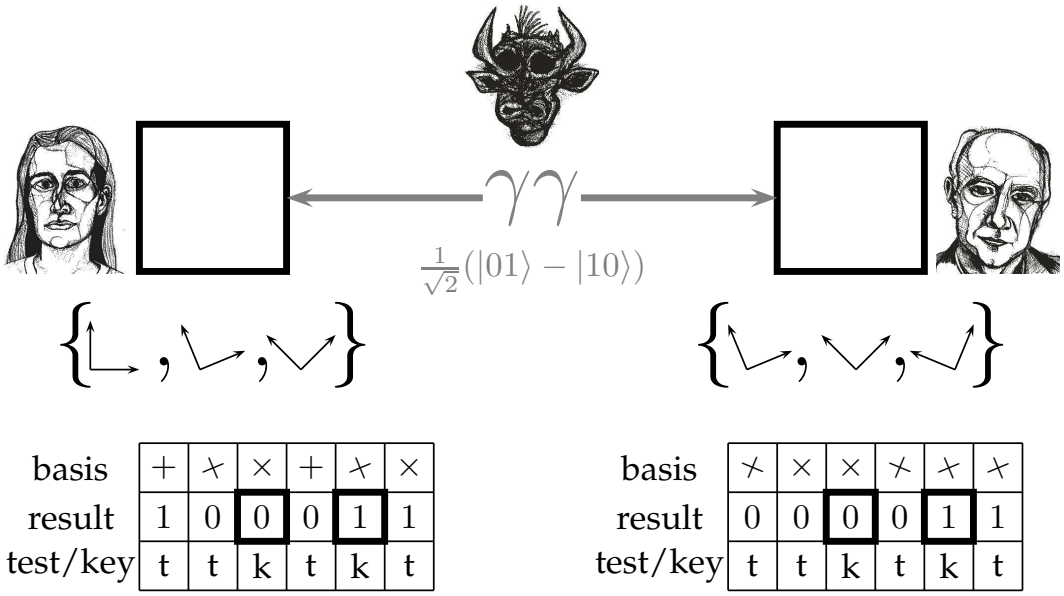

Figure 3.2: Ekert's E91 quantum key distribution protocol [Hänggi 10]

fication on their remaining n bits to get an m-bit shared key.

3.3 Eavesdropping strategies

The protocols described above are provably secure [Shor 00]. In absence of noise or any other errors due to measurement etc., a disagreement in any of the bits would indicate the presence of a eavesdropper in the quantum channel. Eve's aim is to gain information shared between Alice and Bob by inducing some noise over the quantum channel. To achieve this, she uses some strategies (also called 'attacks'), commonly known as the *eavesdropping strategies*.

Till date, many eavesdropping strategies have been defined and analyzed. A general objective of eavesdropping analysis is to develop ultimate proofs to security for quantum protocols, such that those protocols are secure against any kind of strategies that an eavesdropper might use. A particular strategy of interest is assuming that an eavesdropper attaches an ancilla, $|\mathcal{E}\rangle$ (which is a quantum system possibly of a higher dimension than a qubit) to each of Alice's qubit, let them interact, and then measures her ancilla one after the other. This kind of an attack is called the *individual attacks*. When Eve processes several of Alice's qubits coherently, then the attack is known as *coherent attacks*. When Eve attaches one ancilla per qubit as in individual attacks,

but measures several of her ancillas coherently, as in coherent attacks, this type of attacks are called *collective attacks*. For collective attacks, it is usually assumed that Eve's measurement of her ancilla is done only after Alice's and Bob's discussion about basis reconciliation, error correction and privacy amplification on a public channel. While for the individual attacks, Eve only waits till the public discussion of basis reconciliation.

An example of an eavesdropping strategy (known as symmetric-collective eavesdropping) has been discussed in the following section, in the calculation of secret-key rate for the BB84 protocol.

3.4 Key-rate analysis

In this section, we calculate the secret key-rate for the BB84 protocol, for a symmetric-collective eavesdropping strategy. Suppose, Eve attaches an ancilla $|\mathcal{E}\rangle$ to Alice's qubit (where Alice's state is in computational basis). This interaction can be described by a unitary transformation [Pirandola 19]:

$$U|0\rangle|\mathcal{E}\rangle = \sqrt{F_0}|0\rangle|\mathcal{E}_{00}\rangle + \sqrt{D_1}|0\rangle|\mathcal{E}_{01}\rangle \tag{3.10}$$

$$U|0\rangle|\mathcal{E}\rangle = \sqrt{F_1}|1\rangle|\mathcal{E}_{00}\rangle + \sqrt{D_1}|0\rangle|\mathcal{E}_{01}\rangle \tag{3.11}$$

where the states $\{|\mathcal{E}_{00}\rangle, |\mathcal{E}_{01}\rangle, |\mathcal{E}_{10}\rangle, |\mathcal{E}_{11}\rangle\}$ are the states of Eve after interaction with Alice's qubits. The equations (3.10) and (3.11) imply that when Alice sends state $|0\rangle$ ($|1\rangle$), the probability of Bob getting the correct state is F_0 (F_1) when he makes a measurement in the $\mathbb{Z}$ basis, and D_0 (D_1) when he makes a measurement in the $\mathbb{X}$ basis.

Suppose, Alice's original state was $|\theta\rangle$, where $|\theta\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. The equations (3.10) and (3.11) can also be written as:

$$U|\theta\rangle = \sqrt{F_\theta}|\theta\rangle|\mathcal{E}_{\theta\theta}\rangle + \sqrt{D_\theta}|\theta^\perp\rangle|\mathcal{E}_{\theta\theta^\perp}\rangle \tag{3.12}$$

where $\langle\theta|\theta^{\perp}\rangle = 0$. The unitarity conditions on U imply the following conditions:

$$\langle\mathcal{E}_{\theta\theta}|\mathcal{E}_{\theta\theta}\rangle = F_{\theta}, \tag{3.13}$$

$$\langle\mathcal{E}_{\theta\theta^{\perp}}|\mathcal{E}_{\theta\theta^{\perp}}\rangle = D_{\theta}, \tag{3.14}$$

$$\langle\mathcal{E}_{\theta\theta}|\mathcal{E}_{\theta\theta^{\perp}}\rangle = F_{\theta}, \tag{3.15}$$

and

$$F_{\theta} + D_{\theta} = 1. \tag{3.16}$$

In equation (3.12), F_{θ} represents the *fidelity*, and D_{θ} is the Quantum Bit Error Rate (ratio of the number of wrong bits to the total number of received bits) or QBER. Thus, the mutual information between Alice and Bob is given by:

$$I_{AB} = 1 - H_2(D_{\theta}), \tag{3.17}$$

where $H_2(D_{\theta})$ is the binary Shannon entropy calculated over $\mathcal{D}_{\theta}$.

In the BB84 protocol, the errors are symmetric in both $\mathbb{Z}$ and $\mathbb{X}$ bases (since the usage of both $\mathbb{Z}$ and $\mathbb{X}$ bases is symmetric in the case of BB84 protocol). This leads to additional conditions described as follows [Fuchs 97, PIRANDOLA 08]:

$$\langle\mathcal{E}_{\theta\theta}|\mathcal{E}_{\theta^{\perp}\theta^{\perp}}\rangle = F_{\theta}\ \cos(x), \tag{3.18}$$

$$\langle\mathcal{E}_{\theta\theta}|\mathcal{E}_{\theta^{\perp}\theta}\rangle = 0, \tag{3.19}$$

$$\langle\mathcal{E}_{\theta\theta^{\perp}}|\mathcal{E}_{\theta^{\perp}\theta^{\perp}}\rangle = D_{\theta}\ \cos(y), \tag{3.20}$$

where x, $y \in \mathbb{R}$. This implies that QBER is:

$$D_{\theta} = \frac{1 - \ \cos x}{2 - \ \cos x + \ \cos y}. \tag{3.21}$$

Now, suppose that Eve's ancillary system is still in the quantum memory till the completion of Alice's and Bob's public discussion of basis reconciliation. In this way, she can differentiate her two states $|\mathcal{E}_{\theta\theta}\rangle$ and $|\mathcal{E}_{\theta^{\perp}\theta^{\perp}}\rangle$.

Suppose, Eve can also perform a collective attack, in which she makes a joint measurement on her quantum memory. The maximum classical information that Eve can obtain is equal to the Holevo information (refer Section 2.6):

$$\chi_{AE} = S(\rho_E) - \frac{S[\rho_E(\theta)] + S[\rho_E(\theta^{\perp})]}{2}, \tag{3.22}$$

where $S(\rho) = -\mathrm{Tr}(\rho \log_2 \rho)$, is the von Nuemann entropy, and $\rho_E(\theta\rangle)$ and $\rho_E(\theta^{\perp}\rangle)$ are Eve's states for Alice's state $|\theta\rangle$ and $|\theta\rangle$ respectively. Therefore, as a consequence, the secret key rate is lower bounded by the Devetak-Winter rate [Devetak 05]:

$$R_{DW} = I_{AB} - \chi_{AE}. \tag{3.23}$$

For a symmetric collective attack, using equations (3.12), (3.17) and (3.22), this rate is equal to [PIRANDOLA 08]:

$$R = 1 - S(\rho_E) = 1 - 2H_2(D_\theta). \tag{3.24}$$

Therefore, it can be concluded that the maximum value of QBER, for which a secret key can be generated between Alice and Bob is approximately 11%.

The unconditional security of the BB84 protocol uses the idea to reduce the quantum key distribution protocol in an entanglement distillation one. For a set of non-maximally entangled states (say k pairs), entanglement distillation distills m entangled pairs with higher levels of entanglement using only LOCC methods. Due to the basis of protocol on entanglement, Eve cannot get any information about the measurements that Alice and Bob make.

The security-proof of BB84 protocol given by Shor and Preskill [Shor 00] uses quantum error correction codes (CSS codes [Nielsen 11]) to perform entanglement distillation, which dissociates phase errors (e_p) from bit errors (e_b), which helps in performing bit correction and phase correction independent from each other. In this case, the secret key rate is given by:

$$R = 1 - H_2(e_b) - H_2(e_p), \tag{3.25}$$

which reduces to a similar equation like equation (3.24) in case of phase errors and bit

error being equal. This also implies that the maximum value of e_b ($=e_p$), for which a secret key can be generated between Alice and Bob is approximately 11%.

3.5 Loopholes and drawbacks of device-dependent quantum key distribution: The need for device-independence

Although, the rigorous security proofs for many so-called standard device-dependent quantum key distribution protocols have been published, there are several limitations associated with them. Some of them are described as follows.

- It has been discovered that these security proofs are vulnerable due to imperfections in the physical implementations of the protocols associated with them. The apparatus used in the protocol could be easily manipulated by a third party (Eve), who could use it in her favour to gain some information, resulting in the protocol being completely insecure.

- It is required that the devices used in the protocol work perfectly. Suppose Alice encodes her qubit in state $|0\rangle$ and send it to Bob, who performs a measurement in the $\mathbb{Z}$ basis. But, it is possible that the devices performing the encoding and measurement are faulty. For example, say both Alice's and Bob's devices always use the same basis for encoding and measurement, instead of two different bases chosen at random. The eavesdropper can take advantage of the situation, and performs her measurement in that same basis. In this way, she would be able to learn the bit perfectly, without causing any disturbance.

- Also, the users have to regularly check the functionality of the devices used in the protocol, to ensure that the devices work in accordance with the assumptions in the security proof. This is a technically challenging task.

- The security analysis of quantum key distribution protocols requires the *dimension* of the Hilbert space in in various calculations. Therefore, the security proofs of these protocols hold only when the dimension of the system used is known (for eg. BB84 is proven secure only for a 2-dimensional Hilbert space,

but is proven to be unsecure while using systems of higher dimensions (refer Appendix B)). This is not always the case, since Eve can modify the source which shares the entangled pair, and provide a system of a different dimension without the knowledge of Alice and Bob.

- There could be many attacks and eavesdropping strategies, known as the *side-channel attacks*, that exploit some features which are not modelled in the security analysis of the protocol. These attacks could hamper the security of the protocol.

Moreover, the proofs of quantum key distribution protocols are said to be unconditionally secure, but they do make several assumptions:

- It is mandatory that Alice and Bob have secure laboratories. This means that no information is leaked from Alice's and Bob's laboratories. Also, Eve is not able to look into Alice's and Bob's inputs. If this is not the case, and somehow Eve is able to get information about the user's inputs via looking over their shoulder or via placing a transmitter in the devices used that sends information about raw data to Eve, then surely the security is not possible. Thus, this assumption of secure laboratories is a very crucial one, and it cannot be removed.

- It is also assumed that in quantum key distribution protocols, Alice and Bob have complete control over their physical devices. They know the exact specifications and working of their devices. As discussed above, a failure of this assumption opens doors for Eve, to have an easy access to the information shared.

- Additionally, it is also believed that, Alice and Bob have a reliable local source of randomness. The measurement bases and the check bits used to check the presence of an adversary in the system, should be chosen at random, independent from an eavesdropper. If the eavesdropper is somehow aware about which bases are being used or which bits are being used as check bits, then it would be easy for her to attack, without causing disturbance.

- A further assumption is made that there is no error in the classical computations performed by Alice and Bob. For example, the measurement outcomes are noted

down correctly, the number of bits in which both Alice and Bob measured in the same basis are correctly discussed etc. This is necessary to estimate the error rate, and check for the presence of eavesdropper in the channel.

The aim of device-independent quantum key distribution (DI-QKD) is to reduce the above assumptions to the bare minimum, and particularly, to remove all assumptions that state about the operation of the physical devices used in the protocols. The devices could then even be manufactured by the adversary, Eve. Ideally, the security should only rely on testable features of the devices, such as their input-output behavior, which could be tested in the protocol. This forms the fundamental basis for device-independence. For a secure communication, the honest users, now, would only need to make sure that their laboratories are isolated from the adversary (i.e. there is no unwanted flow of information from the laboratories of Alice and Bob to the outside) and they compute the classical statistics correctly. The next chapter provides an introduction to device-independence, and discusses how it could be utilized for key distribution.

Chapter 4

Device-independent quantum key distribution

The laws of quantum mechanics provide us with key distribution protocols that are unconditionally secure. But, as discussed in the previous chapter, the security of these protocols rely on a critical assumption, that the quantum devices used in the protocols are trustworthy. Device-independent quantum key distribution (DI-QKD) provides a relaxation even to this assumption of the devices being trustful; the devices used in DI-QKD protocols may have been prepared by an adversary and/or may not work according to their specifications. Thus, it offers the strongest form of secure communication, as in the security proof of device-independent quantum key distribution protocols, no assumptions are made about the internal working of the quantum devices used for key distribution.

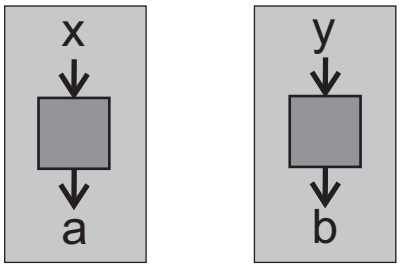

Figure 4.1: Quantum apparatuses as *black boxes* used by Alice and Bob in DI-QKD [Scarani 13]

In device-independent quantum key distribution protocols, the quantum apparatuses

used by Alice and Bob are treated as *black boxes* (see Figure 4.1), each of them producing an output (corresponding to the measurement outcome), based on some classical inputs (such as the measurement settings). This scenario is referred to as *Bell scenario* [Brunner 14]. Although, it is thought that these devices implement quantum processes, there are no assumptions made on states, operators, or the dimensions of Hilbert space used.

4.1 Motivation for device-independence

The motivation for device-independent quantum key distribution can be interpreted by comparing it with the usual device-dependent quantum key distribution techniques. In the entanglement-based protocol [Bennett 92] of DD-QKD, Alice and Bob receive pairs of an entangled state emitted by a common source. They perform some measurements on them in some chosen bases to generate a secret key from the measurement outcomes. Here, since the source is situated between Alice and Bob, it is possible that the source is under the control of an eavesdropper Eve, who could manipulate it (say by changing the emitted state) in a way to gain information about Alice's and Bob's measurement outcomes. Hence, it is distrusted by the users. However, Alice and Bob can perform measurements in a chosen basis on a randomly chosen fraction of their particles (known as the *check bits*) to estimate the state that they got from the source, and decide whether a secret key can be generated from them or not.

In device-independent quantum key distribution, Alice and Bob not only distrust the source of the particles, but also distrust their measurement apparatuses. It is possible that the apparatuses wear out with time, and therefore produce some imperfections while performing measurements. It can also be the case that the devices are manufactured by the adversary, and are manipulated in such a way that there is no guarantee that the actual measurement bases correspond to the actual ones. Therefore, in DI-QKD, Alice and Bob aim to bound information accessible to Eve, by choosing the worst possible states and measurement bases (in arbitrary dimensions of Hilbert space), that also agree with the observed input-output behavior. In the usual DD-QKD, the measurement bases and the Hilbert state dimension of the emitted state were perfectly known to them, and they could easily use this information to

bound Eve's accessible information, while looking for worst possible states and measurement bases compatible with their observed statistics . But this is not the case in DI-QKD.

The security of DI-QKD is based on the observed statistics of the black boxes that Alice and Bob use. Assuming that the behavior of the black boxes remain the same in each run, the *observed statistics* can be represented by a set of probability distribution [Scarani 13]:

$$\mathcal{P}_{\mathcal{AB}} = \{P(xy|ab), x \in \mathcal{X}, y \in \mathcal{Y}; a \in \mathcal{A}, b \in \mathcal{B}\} \tag{4.1}$$

where a and b are Alice's and Bob's inputs and x and y are their respective outputs. From these statistics, and without making any assumption about the internal working of the devices, Alice and Bob should be able to conclude, whether they can generate a secret key against the eavesdropper or not.

4.2 Assumptions in DI-QKD

As discussed in the previous section, device-independent quantum key distribution provides a relaxation of the assumptions made in the security proof of standard DD-QKD. But, still there are some fundamental assumptions that are needed to be fulfilled for DI-QKD to be carried out (note that these assumptions are made in the trusted devices case as well)[Pirandola 19]. These assumptions are described below:

- The laboratories of Alice and Bob are perfectly secure and they have full control over the channels connecting their laboratory with the outdoors i.e. for any devices present in their labs, no unwanted information can leak between them as well as to the outside.

- Alice and Bob can generate perfectly random (and private) bits using a trusted random number generator within their own laboratories, which produces a classical random output.

- Each party has trusted classical devices which provide them a reliable way to store and process classical data generated by their quantum devices.

- Alice and Bob are connected by an authenticated (but otherwise public) classical

channel, on which Eve could listen without being detected.

- Alice and Bob also share an insecure quantum channel which could be intercepted by Eve such that she could modify the signals in validation with quantum mechanics.

Assuming that the mandatory basic assumptions mentioned above are taken care of, device-independent quantum key distribution paves a way for a much better and stronger alternative to the traditional QKD.

4.3 Advantages of DI-QKD

Device-independent quantum key distribution provides a stronger security than the usual device-dependent quantum key distribution. DD-QKD makes several crucial assumptions about the quantum systems used in the protocol. For example, in the security proof of BB84 protocol, the dimension of Hilbert space of quantum system is usually assumed to be 2 (qubits). But, the security of the protocol is totally compromised if four-dimensional system are used. The proof for this is given in Appendix B. Whereas, in DI-QKD, no assumptions are made about the dimensions of the quantum system used in the protocol.

DI-QKD makes it easier to test the components of the QKD protocol in which they are used. Since, the security of the DI-QKD protocol is relied on the input-output behavior of the devices, errors as well as wearing out of the devices with time can be easily detected and accounted for *during the protocol*.

The security proof of the usual QKD protocols do not take into account the real life implementations of the protocols. Due to some noise in the quantum channel or some uncontrolled *side-channels*, the actual implementation of the protocols may differ from the ideal case. The user needs to regularly characterize the functionality of the quantum devices very precisely, to ensure that their behavior is still in line with the assumptions made in the security proof, which is a very challenging task. Whereas, DI-QKD does not need any sophisticated testing is required to check whether the devices are functioning well or not.

DI-QKD also provides a solution to the case where the measurement apparatuses

are not trusted. Suppose, the Eve had access to the quantum apparatuses, and she manipulates it to her own benefit aiming to get some information about Alice's and Bob's measurement outcomes before sending it out to Alice and Bob. But, since the security of DI-QKD is based only on the input-output behavior, it does not matter whether the devices are manipulated or not. It could be possible that Eve modifies the mechanism of the devices, such that it send out the measurement settings and results directly to her. But, this violates the first assumption that Alice and Bob's laboratories are secure, which is a necessary assumption for key distribution.

4.4 Security of DI-QKD

The security of device-independent quantum key distribution is based on the quantum phenomena of *non-locality* and violation of Bell's inequalities [Bell 04]. It is based on the idea that quantum correlations allows one to perform classically impossible task like violating the Bell's inequalities. It follows from the intuition that entangled states require non-local correlations for their generation, whose measurement outcomes corresponding to some basis, cannot be completely known to an adversary. Thus, if Alice's and Bob's devices are unable to communicate, and are provided with random inputs such that their input-output behavior gives rise to a distribution that violates a Bell inequality, then the outputs could not have been pre-determined by Eve. The concept of non-locality and Bell violation has been analyzed in detail in the next chapter.

Chapter 5

Bell violation and unpredictability

Prediction of quantum correlations is one of the most astonishing aspects of quantum mechanics. Indeed, the correlations between the measurements performed on systems comprising of several components of an entangled state have no analog in the classical domain. In 1964, an important feature of quantum correlations was derived by John Bell, in his paper titled *On the Einstein Podolsky Rosen paradox* [Bell 64], which stated that the predictions of quantum theory are incompatible with those of any physical theory satisfying a natural notion of locality, i.e the quantum correlations for states of entangled composite systems cannot be reproduced by a classical local-variable theory. He proved that the observed correlations between two spin-$\frac{1}{2}$ particles in a singlet state violate some inequalities, known as the *Bell inequalities*, which are satisfied by a local variable theory.

This provided a possible definition of *non-locality*: the impossibility to reproduce quantum correlations with theories based on local variables. Thus, a state is said to be non-local, if the correlations corresponding to it violates a Bell inequality. In this chapter, we discuss Bell inequalities and analyze the relation of their violation to the unpredictability of correlations produced by quantum mechanics. Further, the importance of Bell violation as a fundamental necessity in device-independent quantum key distribution is also analyzed.

We consider the following scenario: Say, each of the two users, Alice and Bob, has a measurement apparatus which performs measurements on the halves of pair of

entangled qubits in some particular basis. Each device can take in one of the two possible inputs (which corresponds to a particular measurement setting, say the choice of measurement basis) and produces one of the two possible outputs (corresponding to the measurement outcome). It is assumed that that one device cannot access the input of the other device. Crucially, although for the security argument in a DI case no details about the state and measurement settings are required, this may be a good staring point for honest parties to set up their devices.

In order to describe the behavior of devices, the following notation is used:

Alice's input: a Bob's input: b

Alice's output: x Bob's output: y

It is possible that from one run of the experiment to the other, the measurement outcomes a and b that are obtained may vary, even when the inputs x and y are made same in each run. Therefore, these outcomes are thus in general described by a joint probability distribution $P(xy|ab)$.

The conditional distribution $P(xy|ab)$ as a 4×4 matrix can be described using the following table [Pirandola 19]:

$P(xy\|ab)$	b	0		1	
	y	0	1	0	1
a	x				
0	0	$P(00\|00)$	$P(01\|00)$	$P(00\|01)$	$P(01\|01)$
	1	$P(10\|00)$	$P(11\|00)$	$P(10\|01)$	$P(11\|01)$
1	0	$P(00\|10)$	$P(01\|10)$	$P(00\|11)$	$P(01\|11)$
	1	$P(10\|10)$	$P(11\|10)$	$P(10\|11)$	$P(11\|11)$

Table 5.1: Conditional probability distribution $P(xy|ab)$

Let's say, Alice's and Bob's device follow some particular probability distribution $P(xy|ab)$. Imagine an eavesdropper Eve acquires some additional classical information about the devices, denoted by the random variable Z. Eve exploits this classical information to further enhance her knowledge about what is happening. This can be interpreted as follows: Suppose, Eve is the manufacturer of the devices to be used by Alice and Bob, and let's assume that she supplies devices that behave according to a

probability distribution $P_z(xy|ab)$, but chooses z with probability p_z, such that from Alice and Bob's point of view the devices behave in the same way. Formally,

$$P(xy|ab) = \sum_z p_z P_z(xy|ab). \tag{5.1}$$

For non-communicating devices (i.e. no device can access the input of the other), the probability distribution of the devices must follow conditions of locality. This implies

$$P_z(x|ab) = P_z(x|a) \text{ and } P_z(y|ab) = P_z(x|a). \tag{5.2}$$

Now, the question arises that is it possible for Eve to supply such deterministic devices giving rise to the observed distribution? Mathematically, the question is whether $P(xy|ab)$ can be penned in the form of (5.1) with $P_z(xy|ab) = P_z(x|a)P_z(y|b)$, and $P_z(x = \tilde{x}|a = i)$, $P_z(y = \tilde{y}|b = j) \in \{0,1\}$ for all $\tilde{x}, \tilde{y}, i, j \in \{0, 1\}$.

In other words, *is $P(xy|ab)$ a convex combination of 16 local deterministic distributions* [Pirandola 19]

$$\left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right), \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right), \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{array}\right), \ldots\ldots\ldots, \left(\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{array}\right) ?$$

If yes, then Eve can have complete knowledge of Alice's and Bob's measurement results after knowing their inputs. If not, then at least some of the time Eve must be sending a distribution $P_z(xy|ab)$ to which she doesn't have information about either Alice's or Bob's outcome after learning their inputs (i.e. there is some kind of randomness). We provide a formal picture to the above concept of local deterministic distributions in the following section.

5.1 Defining Bell's Inequality

In this section, we describe quantum correlations mathematically using an expression known as the Bell's inequality.

Definition 5.1.1. A Bell inequality is a relation satisfied by all local correlations

(i.e., all $P(xy|ab)$ that can be written as a convex combination of local deterministic distributions), but can be *violated* by suitable measurements on a pair of quantum particles in an entangled state.

An example of Bell inequality is the CHSH inequlaity [Clauser 69], given by John Clauser, Michael Horne, Abner Shimony, and Richard Holt in 1969. Let's take the case where there are two measurement choices per observer a, $b \in \{0,1\}$, with only two possible measurement outcomes x, $y \in \{+1,-1\}$. The expectation value of the product xy, for the measurement settings (a,b) is given by $\langle x_a x_b \rangle = \sum_{x,y} xy\ p(xy|ab)$. Consider the expression: $S = \langle x_0 y_0 \rangle + \langle x_0 y_1 \rangle + \langle x_1 y_0 \rangle - \langle x_1 y_1 \rangle$, which is a function of probabilities $p(xy|ab)$. Thus, if the probabilities can be written as a convex combination of local deterministic distributions, as described in the previous section, we necessarily have

$$S = \langle x_0 y_0 \rangle + \langle x_0 y_1 \rangle + \langle x_1 y_0 \rangle - \langle x_1 y_1 \rangle \leq 2. \tag{5.3}$$

which is known as the CHSH inequality. The derivation of the above result is provided in Appendix C.

Equation (5.3) can also be represented in terms of the probability distribution $P_z(xy|ab)$ as $S = \langle C, P \rangle \leq 2$, where $P = P_z(xy|ab)$, and the matrix C is given by

$$C = \left(\begin{array}{cc|cc} 1 & -1 & 1 & -1 \\ -1 & 1 & -1 & 1 \\ \hline 1 & -1 & -1 & 1 \\ -1 & 1 & 1 & -1 \end{array}\right).$$

$\langle C, P \rangle = \mathrm{Tr}(C^T P)$ is known as the Hilbert-Schmidt inner product .

5.2 Violation of CHSH Inequality: An example of state $|\phi^+\rangle$

Bell's theorem states that there are quantum correlations that violate the CHSH inequality. This implies that quantum theory is non-local. To describe the above correlations, a particular class of distributions are parameterized in terms of $\varepsilon \in \left[0, \frac{1}{2}\right]$

as follows:

$$P_\varepsilon := \left(\begin{array}{cc|cc} \frac{1}{2}-\varepsilon & \varepsilon & \frac{1}{2}-\varepsilon & \varepsilon \\ \varepsilon & \frac{1}{2}-\varepsilon & \varepsilon & \frac{1}{2}-\varepsilon \\ \hline \frac{1}{2}-\varepsilon & \varepsilon & \varepsilon & \frac{1}{2}-\varepsilon \\ \varepsilon & \frac{1}{2}-\varepsilon & \frac{1}{2}-\varepsilon & \varepsilon \end{array}\right). \tag{5.4}$$

A state is defined as $|\phi_\theta\rangle := cos\frac{\theta}{2}|0\rangle + sin\frac{\theta}{2}|1\rangle$. Suppose, Alice and Bob measure the two halves of the maximally entangled-state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ corresponding to their inputs in the following bases:

$$\begin{aligned} \{|\phi_0\rangle, |\phi_\pi\rangle\} \qquad & \text{for } a = 0, \\ \{|\phi_{\pi/2}\rangle, |\phi_{3\pi/2}\rangle\} \qquad & \text{for } a = 1, \\ \{|\phi_{\pi/4}\rangle, |\phi_{5\pi/4}\rangle\} \qquad & \text{for } b = 0, \\ \{|\phi_{3\pi/4}\rangle, |\phi_{7\pi/4}\rangle\} \qquad & \text{for } b = 1. \end{aligned}$$

This gives rise to the following probability distribution:

$$P_{calculated} := \left(\begin{array}{cc|cc} \frac{1}{4}+\frac{\sqrt{2}}{8} & \frac{1}{4}-\frac{\sqrt{2}}{8} & \frac{1}{4}+\frac{\sqrt{2}}{8} & \frac{1}{4}-\frac{\sqrt{2}}{8} \\ \frac{1}{4}-\frac{\sqrt{2}}{8} & \frac{1}{4}+\frac{\sqrt{2}}{8} & \frac{1}{4}-\frac{\sqrt{2}}{8} & \frac{1}{4}+\frac{\sqrt{2}}{8} \\ \hline \frac{1}{4}+\frac{\sqrt{2}}{8} & \frac{1}{4}-\frac{\sqrt{2}}{8} & \frac{1}{4}-\frac{\sqrt{2}}{8} & \frac{1}{4}+\frac{\sqrt{2}}{8} \\ \frac{1}{4}-\frac{\sqrt{2}}{8} & \frac{1}{4}-\frac{\sqrt{2}}{8} & \frac{1}{4}+\frac{\sqrt{2}}{8} & \frac{1}{4}-\frac{\sqrt{2}}{8} \end{array}\right) = P_{\varepsilon_{QM}}. \tag{5.5}$$

Comparing the form of P_ε of the calculated distribution, with the distribution of (5.4), we get

$$\varepsilon = \frac{1}{4} - \frac{\sqrt{2}}{8} = \frac{1}{8}(2-\sqrt{2}) =: \varepsilon_{QM} \tag{5.6}$$

The above value of ε_{QM} leads to the value of CHSH inequality $\langle C, P_{\varepsilon_{QM}}\rangle = 2\sqrt{2} \geq 2$, which contradicts equation (5.3), and thus the locality constraints as well. This violation implies the correlations corresponding to the measurement on state $|\phi^+\rangle$ are non-local, and therefore cannot be pre-determined via any LV theory, and thus concluding that quantum theory is indeed non-local. Note that $S = 2\sqrt{2}$ is the maximal violation of this inequality. The Tsirelson's bound [Cirel'Son 80] states that if a probability distribution P is quantum-correlated, then $S \leq 2\sqrt{2}$.

The randomness of the outcomes can be seen by decomposing the distribution $P_{\varepsilon_{QM}}$, in a way that the local components of the decomposition is maximized. For $0 \leq \varepsilon \leq 1/8$, this is achieved by the following distribution:

$$P_\varepsilon := \varepsilon \Bigg[\left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right) + \left(\begin{array}{cc|cc} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{array}\right) + \left(\begin{array}{cc|cc} 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{array}\right) + \left(\begin{array}{cc|cc} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ \hline 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right)$$

$$+ \left(\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \end{array}\right) + \left(\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ \hline 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right) + \left(\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{array}\right) + \left(\begin{array}{cc|cc} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ \hline 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{array}\right) \Bigg]$$

$$+ (1 - 8\varepsilon) \left(\begin{array}{cc|cc} \frac{1}{2} & 0 & \frac{1}{2} & 0 \\ 0 & \frac{1}{2} & 0 & \frac{1}{2} \\ \hline \frac{1}{2} & 0 & 0 & \frac{1}{2} \\ 0 & \frac{1}{2} & \frac{1}{2} & 0 \end{array}\right).$$

5.3 Implications of P_ε: Linking non-locality and randomness

From the above distribution of P_ε, the probability that Eve would be able to guess Alice's outcomes using the above description is equal to $8\varepsilon + \frac{1}{2}(1 - 8\varepsilon) = \frac{1}{2} + 4\varepsilon$, which implies that Alice's outcome would have some randomness w.r.t. Eve. The first eight terms in the decomposition are local, and the last term is a maximally non-local distribution (i.e. it is not one of the 16 local deterministic distributions) [Popescu 94], and therefore Eve would not have information about Alice's and Bob's outcomes in this case. The above argument intends to given an intuition to the idea of why violating a Bell inequality implies some randomness in the outcomes. It suggests that it would be much difficult for Eve to extract information about Alice and Bob's

outputs.

So, if two devices limited by no-signalling principle (i.e. a particular device cannot have access to other device's input), are able to produce correlations that are non-local, then their measurement outcomes cannot be fully-determined, and they must necessarily exhibit some randomness. This forms the basic principle for *device-independent quantum key distribution* protocols, in which violation of Bell inequality, which can be asserted without any assumptions on the physical working of the devices, ensures the generation of secure cryptographic keys that cannot be pre-determined. Some device-independent protocols are discussed in the following chapters.

Chapter 6

Spot-checking CHSH QKD protocol

Device-independent quantum key distribution allows two isolated parties to share a secret key, provided they have an access to an authenticated public channel and an insecure quantum channel. In the last chapter, we discussed the idea of a Bell inequality and the consequences of its violation in quantum theory. The violation of Bell inequalities guarantee the presence of a randomness but only in the condition that the users are non-signalling. Therefore, in a model that is intrinsically no-signalling, the measurement outcomes cannot therefore be fully determined in each run of a Bell test, and they must necessarily exhibit some kind of randomness. This forms the intuition behind the development of DI-QKD protocols.

The application of Bell non-locality in quantum key distribution was first given by Ekert in 1991 in his paper *Quantum cryptography based on Bell's theorem* [Ekert 91], in which he presented a key distribution protocol based on CHSH inequality using two qubit maximally entangled state $|\phi_+\rangle$ as a source, but the idea of security of his protocol on the basis of violation of Bell inequalities was not recognized at that time.

The idea of device-independence was first described by Mayers and Yao, by their *self-testing* protocol [Mayers 98a], but it was not directly based on violations of Bell-inequalities. Barret, Hardy and Kent presented the first explicit device independent protocol known as the BHK protocol [Barrett 05a], which was based on the violation of

chained Bell inequalities. It was also the first DI-QKD protocol proven secure against general attacks by no-signalling eavesdropper. Since then, significant developments have been made in the formulation as well as the security of various DI-QKD protocols. Eavesdropping analysis has contributed immensely in development of even stronger protocols, secure against a wide range of eavesdropping strategies.

A general class DI-QKD protocols comprises mainly of the following steps:

- **Measurement step**: Alice and Bob measure a series of entangled quantum systems.
- **Estimation step**: Alice and Bob publicly announce a fraction of their measurement inputs and outputs to test the violation of Bell inequality and calculate the error rate in the raw data.
- **Error correction step**: This step involves the correction of errors using a classical protocol, which involves public communication.
- **Privacy-amplification step**: In this step, a shorter secure key is distilled from the raw key based on the bound on the eavesdropper information, calculated from the violation of Bell's inequality.

In the following section, we describe a particular example of a DI-QKD protocol, with its security based on the violation of CHSH inequalty.

6.1 The Spot-Checking CHSH QKD Protocol

We describe a particular DI-QKD protocol for a maximally entangled qubit state $|\phi^+\rangle = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$. Note that, the assumptions for DI-QKD described in Section 4.2 are to be considered here. As the name suggests, the protocol we discuss here is based on the CHSH (Clauser-Horne-Shimony-Holt) game with spot-checking. Few parameters have been defined: $\alpha \in (0,1)$, $\mathrm{n} \in \mathbb{N}$, $\beta \in (2, 2\sqrt{2}]$, $\delta \in (0, 2(\sqrt{2}-1))$, which are to be chosen by the user at the start. The protocol is described as follows [Pirandola 19]:

- Alice generates an entangled pair $|\phi^+\rangle$ using a preparation device. She keeps one half to herself and sends the other to Bob.
- Bob stores it and announces reception of his half of the entangled pair to Alice.

- Alice chooses a random bit Q_i, comprising of 0's and 1's, in which $Q_i = 0$ occur with probability $1-\alpha$, and $Q_i = 1$ occur with probability α.
- Q_i is then sent to Bob over an authenticated classical channel.
- Let Alice's measurement outcomes are denoted by x_i, corresponding to her inputs a_i. Similarly, Bob's outcomes are denoted by y_i, corresponding to his inputs b_i.
- Suppose that $Q_i = 0$ is chosen as a scenario *corresponding to no test*. In this case, Alice and Bob perform measurements corresponding to the inputs $a_i = 0$ and $b_i = 2$ respectively, and record the outcomes, x_i and y_i.
- $Q_i = 1$ is chosen as a scenario *corresponding to a CHSH test*. In this case, Alice and Bob each independently pick uniformly random inputs $a_i \in \{0, 1\}$ and $b_i \in \{0, 1\}$, and record the outcomes, x_i and y_i, corresponding to their measurements.
- The above steps are repeated n times, increasing i each time.
- For all the cases with $Q_i = 1$, Bob sends his inputs and outputs to Alice who computes the average CHSH value. If the value is below $\beta - \delta$, the protocol is aborted.
- If the protocol does not abort, Alice and Bob use the rounds with $Q_i = 0$ to *generate a key* using error correction and privacy amplification over the authenticated classical channel.

To understand the above mentioned protocol, let us consider an ideal scenario, in the absence of an eavesdropper, Eve. The state generated is a maximally entangled state $\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$. For inputs $a, b \in \{0, 1\}$, the measurements are same as described in Section 5.2. Furthermore, for $b = 2$, the measurement is in $\{|\psi_0\rangle, |\psi_\pi\rangle\}$ basis, which is the same basis as for $a = 0$.

If α is chosen to be small, then on most of the rounds, both parties measure in $\{|0\rangle, |1\rangle\}$ basis, which should provide perfectly correlated outcomes, suitable for the generation of a key. For any other case, the outcomes are completely uncorrelated. Therefore, for the rounds with $Q_i = 1$, a CHSH test is performed, in order to keep

the devices honest. These are known as the *spot-checks*. The parameter β is the expected CHSH value of the setup, which is equal to $2\sqrt{2}$ (the maximal violation) in the ideal scenario, and δ is known as the tolerance to statistical fluctuations. The probability that an ideal implementation with no eavesdropping leads to an abort is called the *completeness error*. Using the implementation given above, this occurs when the statistical fluctuations cause devices with an expected CHSH value of β to produce a value below $\beta - \delta$.

6.2 Remarks

Some worthful remarks about the above-mentioned spot-checking CHSH QKD protocol are described below:

- It is important that the preparation device used by Alice to generate the entangled pair $|\phi^+\rangle$ is unable to access information from Alice's measurement device, even though these may be in the same lab (this is because the preparation device may be provided by Eve, and if access were granted, it could send previous measurement results to Eve via the quantum channel).

- The choice Q_i needs to be communicated after the state is shared (otherwise Eve can choose whether to intercept and modify the quantum state depending on whether or not a test will be performed).

- It is possible for Bob's device to tell when it is being used to generate key ($b_i = 2$). Crucially though, Alice's device cannot (Alice's device learns only A_i and not the value of Q_i), and it is this that forces her device to behave honestly; not doing so will lead her getting caught out if the round is a test. If Bob's device does not behave close enough to the way it should in the case $b_i = 2$, then the protocol will abort during error correction step.

- Another important aspect of Bell violation is that, in a quantum experiment, the violation of a Bell inequality reveals the presence of entanglement in a device-independent way. In fact, in some cases, certain quantum correlations can only be reproduced by performing specific local measurements on a specific entangled state. Therefore, in some cases, by observing such correlations, it is possible to

identify the characteristics of an unknown source of quantum states as well that of measurement devices in a device-independent way. For example, the observation of maximal violation of the CHSH inequality implies that the underlying quantum state on which measurements are performed is necessarily equivalent to a two-qubit singlet state.

- It is also worth noting that, as discussed in Section 4.2, there is no sophisticated testing required to check the functionality of the working of the devices. Device-independent QKD protocols check that the devices are functioning sufficiently well during the protocol itself.

There are many other DI-QKD protocols possible, but they also are based on the similar idea of generating randomness via the violation of some kind of Bell inequalities, as in the CHSH protocol described in the previous section. The protocol discussed in this chapter describes an ideal case where there is no eavesdropper present in the channel. But, in real-life implementations, this is not always the case. As discussed in Section 3.3, there are many possible strategies that an eavesdropper could utilize to attack the channel to gain access to the information shared between Alice and Bob. Therefore, it is necessary to analyze the security of a protocol against the strategies available to the eavesdropper. In the next chapter, we describe a QKD scheme and analyze its security against an eavesdropper limited only by the no-signalling principle.

Chapter 7

DI-QKD against no signalling eavesdropper

Non-signalling cryptography (also called relativistic quantum cryptography) bases its security on the impossibility of signalling between parties that are space-like isolated from each other, as justified by special relativity. It states that an eavesdropper cannot prepare two or more physical systems in a joint state such that a local measurement on one system might send information to another discrete system.

Two parties are able to share a secret key between them, which is secure not only against an eavesdropper Eve which follows the laws of quantum mechanics, but is also secure against an Eve which is limited by on the no-signalling principle only. Here, the eavesdropper cannot be forced to interact with the legitimate parties. Given the eavesdropper's measurement outcome, the two parties, namely Alice and Bob, must not be able to signal to each other by interacting with their quantum systems. The security of the scheme is based on the existence of non-local correlations which imply that the outcomes must be completely independent of any information the eavesdropper can possibly hold. These correlations can be realized by measuring an entangled quantum state and additionally have the property that Alice's and Bob's outcomes are perfectly correlated.

An advantage of non-signalling constraint is that the security proof is based on observed correlations. It is independent from the question how these correlations were

realized, such as the physical particles used to distribute them, the dimension of the Hilbert space or the exact working of the measurement device. Therefore, these protocols are naturally *device-independent*.

In this chapter, we describe a protocol which is secure against an eavesdropper Eve who is limited by only the no-signalling principle. This protocol uses the idea of [Acín 06b] and [Ekert 91], in which the parties (Alice and Bob) perform a CHSH non-locality test on a fraction of their particles to check the violation of the CHSH inequality, and perform the measurements on the rest of the particles in the same basis, for the successful generation of key as well as maximizing the key-rate. The CHSH test is performed to guarantee that the knowledge that the eavesdropper (Eve) has about the systems of Alice and Bob is limited [Barrett 05b]. The protocol [Acín 06b] is described below.

7.1 Protocol

The protocol for quantum key distribution is based on the CHSH inequality.

- A quantum channel is shared between Alice and Bob, which consists of a source, which emits pairs of qubits in maximally entangled state $|\phi_+\rangle = \frac{(|0\rangle_A|0\rangle_B+|1\rangle_A|1\rangle_B)}{\sqrt{2}}$, where subscript A represents Alice's qubit and subscript B represents Bob's qubit.

- But due to noise, there are some imperfections present in the channel. The noise transforms the state $|\phi_+\rangle$ in a Werner state

$$\rho = p|\phi_+\rangle\langle\phi_+| + (1-p)\frac{I}{4}. \tag{7.1}$$

- Both parties choose their measurement settings randomly and independent from each other, and record the corresponding outcomes. They are denoted as follows:

Alice's input (measurement): a	Bob's input (measurement): b
Alice's outcome: x	Bob's outcome: y

The observed statistics of their devices (refer Chapter 5) are represented by

$P(xy|ab)$, which represents the joint probability to obtain outcomes a and b, given measurements x and y.

- Alice can perform one of the three measurements, $a = 0$, 1 or 2, which corresponds to measurement of her qubit in the following bases:

$$\begin{aligned} \{|0\rangle \pm e^{\frac{i\pi}{4}}|1\rangle\} \qquad & \text{for } a = 0, \\ \{|0\rangle \pm |1\rangle\} \qquad & \text{for } a = 1, \\ \{|0\rangle \pm e^{\frac{i\pi}{2}}|1\rangle\} \qquad & \text{for } a = 2. \end{aligned}$$

  The probability that Alice chooses her measurement along $\pi/4$ ($a = 0$) is q, and probability that she chooses her measurement along 0 ($a = 1$) or $\pi/2$ ($a = 2$) are both $(1 - q)/2$.

- Similarly, Bob can perform two measurements, $b = 0$ or 1, which corresponds to measurement of his qubit in the following bases:

$$\begin{aligned} \{|0\rangle \pm e^{\frac{-i\pi}{4}}|1\rangle\} \qquad & \text{for } b = 0, \\ \{|0\rangle \pm e^{\frac{i\pi}{4}}|1\rangle\} \qquad & \text{for } b = 1. \end{aligned}$$

  Probability that Bob chooses his measurement along $\pi/4$ ($x = 0$) is q', and probability that he chooses his measurement along $-\pi/4$ ($x = 1$) is $(1 - q')$.

- Alice and Bob perform the chosen measurements on each of their qubits.

- After measuring all the pair of particles, the measurement bases are revealed by Alice and Bob.

- Alice's measurement $a = 0$ or $\pi/2$ is a case which leads to a maximum violation of the CHSH inequality. Therefore, in this scenario, Alice and Bob, both reveal their measurement outcomes, and then compute the value of the CHSH quantity.

- If both Alice and Bob measure along $\pi/4$, then their outcomes are strongly correlated, which will be further used for key generation.

- The case where Alice measures along $\pi/4$ and Bob measures along $-\pi/4$, their outcomes are completely uncorrelated. The data corresponding to this case will

be discarded.

- Privacy amplification and information reconciliation steps on the strongly correlated outcomes will provide a pair of identical secret keys.

  We note that the security of the protocol follows from the fact that the observed statistics of Alice's and Bob's device violate the CHSH inequality. To maximize the key rate, q and q' should be chosen as close to 1 as possible. Within the next sections, we address the eavesdropping strategies and evaluate the security of this protocol.

7.2 Eavesdropping strategies: Individual attacks

This section describes the strategies used by an eavesdropper Eve to gain information from the insecure quantum channel shared by Alice and Bob. We make an assumption that Eve controls the particle source, and therefore, she has the ability to prepare Alice's and Bob's particles as well as any other system in a joint non-signalling state. Moreover, she is also restricted to individual attacks, in which she attacks each particle separately and acquires independent knowledge about each individual bit of the key.

Eve prepares a state of three particles, say $|\Psi\rangle_{ABE}$, corresponding to Alice, Bob and herself, and shares it with Alice and Bob. Say, Eve performs a measurement e on the state $|\Psi\rangle_{ABE}$, and receives an outcome z. We define a set of joint measurement probability distributions, $P(xyz|abe)$. The no-signalling condition implies that:

$$\begin{aligned} \sum_z P(xyz|abe) &\equiv P(xy|ab) \quad \forall\, e, \\ \sum_z P(xyz|abe) &\equiv P(yz|be) \quad \forall\, a, \\ \sum_z P(xyz|abe) &\equiv P(xz|ae) \quad \forall\, b. \end{aligned} \tag{7.2}$$

This states that the marginal distributions of any subset of particles do not depend on the measurement choices chosen by the other parties.

Eve wants to perform a measurement on her particle that will provide her with the maximum information about the outcomes of Alice and Bob. Since, only the mea-

surement outcomes corresponding to $a = 0$ and $b = 0$ are used in the key generation process, Eve is only interested in Alice's and Bob's outcomes corresponding to the measurements $a = 0$ and $b = 0$, respectively. Moreover, due to the no-signalling constraint on Eve, she could also not affect Alice's and Bob's outcomes by her choice of measurement. Therefore, it is assumed that she always performs the same measurement $\tilde{e}$, which gives her the maximum information about the measurement pair $(a = 0, b = 0)$.

Let's say Eve gets an outcome z corresponding to her measurement $\tilde{e}$, with probability $p_z = P(z|\tilde{e})$. Eve will therefore prepare Alice's and Bob's particles in a state, satisfying the no-signalling conditions $P_z(xy|ab) = P(xy|ab\tilde{e}z)$.

The individual attack of Eve would be to prepare a mixture of probability distributions $\sum_z P_z(xy|ab)$, satisfying the no-signalling conditions, providing her Alice's and Bob's observed correlations $P(xy|ab) = \sum_z p_z P_z(xy|ab)$, and therefore the secret key. It is also assumed that each non-signalling term in the mixture, $P_z(ab|xy)$ is extremal, i.e., it cannot itself be decomposed as a convex sum of other no-signalling correlations.

The outcomes of Alice and Bob (x and y), can take values either 0 or 1. For each of Alice's measurement a, either the outcome x is predetermined, i.e. $P(x|a) = 0$ or 1 or is uniformly random, i.e. $P(x|a) = 1/2$. For $P(x|a) = 1/2$ case, the measurement a corresponds to the set containing two measurements for Alice and two measurements for Bob, such that for this set CHSH inequality is maximally violated. Similarly, for Bob, it is either $P(y|b) = 0$ or 1, or $P(y|b) = 1/2$.

7.3 Security analysis and key rate

The strategy of individual attack by Eve has been described in the previous section. We now try to analyse how much secure is the above protocol against such attack. Using the definition of Bell's inequality described in Section 5.1, we calculate the value of the CHSH quantity for the Werner state (7.1) for the measurements described in the protocol. It is represented by $\langle S_{n.s.} \rangle$[Acín 06b]. The value of CHSH quantity

comes out to be:

$$\langle S_{n.s.} \rangle = P(x_1 \neq y_0) + P(x_1 \neq y_1) + P(x_2 \neq x_1) + P(x_2 = y_0) = 2 - \sqrt{2}p. \quad (7.3)$$

Note that, this expression is calculated for inputs $a = 1, 2$ and $b = 0, 1$, since these inputs are used by Alice and Bob to check the violation of the CHSH inequality. Equation (7.3) is the same as equation (5.3), but written in a different notation. Here, the local correlations satisfy $\langle S_{n.s.} \rangle \geq 1$, and the non-local correlations satisfy $0 \leq \langle S_{n.s.} \rangle \leq 1$. Thus, the CHSH expression is violated, for $p \leq \sqrt{2}$.

When Alice and Bob measure the pair ($x = 0$, $y = 0$) (the case of interest of Eve), the correlations between them can be described by:

$$\langle C_{n.s.} \rangle = P(a_0 = b_0) - P(a_0 \neq b_0). \quad (7.4)$$

The value of the above quantity turns out to be equal to p. The strategies of Eve can be classified according to whether the outcomes corresponding to $x = 0$ or $y = 0$ yield pre-determined or uniformly random outcomes [Barrett 05c, Jones 05]. These strategies are described in the table below:

i	**Strategies**	$\langle S_{n.s.} \rangle$	$\langle C_{n.s.} \rangle$	$H(A\|E)$	$H(B\|E)$	$I(A:B\|E)$	p_i
1.	(D,D)	$\geqslant 1$	$\leqslant 1$	0	0	0	p_1
2.	(D,R)	$\geqslant 0$	0	0	1	0	p_2
3.	(R,R)	$\geqslant 0$	$\leqslant 1$	1	1	1	p_3

Table 7.1: Extremal strategies available to Eve for measurement inputs $x = 0$ and $y = 0$ (used to generate a key) [Acín 06b].

In the table above, (D,D) represents the scenario where both measurements $x = 0$ and $y = 0$ produce deterministic outcomes, (D,R) represents the scenario where the measurement $x = 0$ produces deterministic outcome and the measurement $y = 0$ produces a random outcome and (R,R) represents the scenario where both $x = 0$ and $y = 0$ produce random outcomes. Eve could choose any of the above 3 strategies with probability p_i, as represented in the table. For each of the cases, the conditional entropies $H(A|E)$ and $H(B|E)$ (representing the ignorance of Eve) and mutual information between Alice and Bob (refer Chapter 2) are calculated.

The secret key rate for privacy amplification with one-way communication is defined

by using the Csiszár-Körner condition [Csiszar 78] as:

$$K = \max\{I(A:B) - I(A:E), I(A:B) - I(B:E)\}. \tag{7.5}$$

The mutual information between Alice and Eve can be calculated using equation (2.10)

$$I(A:E) = H(A) - \sum_i p_i H_i(A|E). \tag{7.6}$$

From Table 7.1,

$$\begin{aligned} I(A:E) &= 1 - p_1 H_1(A|E) - p_2 H_2(A|E) - p_3 H_3(A|E) && (7.7)\\ &= 1 - p_1(0) - p_2(0) - p_3(1) \\ &= 1 - p_3. && (7.8) \end{aligned}$$

Similarly, the mutual information between Bob and Eve is given by:

$$\begin{aligned} I(B:E) &= H(B) - \sum_i p_i H_i(B|E) && (7.9)\\ &= 1 - p_1 H_1(B|E) - p_2 H_2(B|E) - p_3 H_3(B|E) && (7.10)\\ &= 1 - p_1(0) - p_2(1) - p_3(1) \\ &= 1 - p_2 - p_3 && (7.11)\\ &= p_1. && (7.12) \end{aligned}$$

Comparing equations (7.8) and (7.11), we see that $I(A:E) \geq I(B:E)$, which implies $I(A:B) - I(A:E) \leq I(A:B) - I(B:E)$. Thus, the key rate equals

$$K = I(A:B) - I(B:E). \tag{7.13}$$

The mutual information between Alice and Bob is $I(A:B) = 1 - h(\frac{1+p}{2})$, where h is the binary entropy, as defined in Subsection 2.2.1. Therefore, the secret key rate becomes

$$K = 1 - h\Big(\frac{1+p}{2}\Big) - p_1. \tag{7.14}$$

Since, for the DD strategy, $\langle S_{n.s.} \rangle \geq 1$, and $0 \leq p_i \leq 1$, therefore

$$p_1 \leq \langle S_{n.s.} \rangle. \tag{7.15}$$

Thus, combining equations (7.3), (7.14) and (7.15), we put an upper-bound on the key rate as follows:

$$\begin{aligned} K &= 1 - h\Big(\frac{1+p}{2}\Big) - p_1 \\ &\geq 1 - h\Big(\frac{1+p}{2}\Big) - (2 - \sqrt{2}p). \end{aligned} \tag{7.16}$$

This gives us the following equation for the key rate of the protocol:

$$K \geq \sqrt{2}p - h\Big(\frac{1+p}{2}\Big) - 1. \tag{7.17}$$

Thus, in the noise free case (i.e. when $p = 1$), $K \geq \sqrt{2} - 1$, which is much higher compared to the protocol given in [Acín 06a]. The key generation ceases (K=0) when $p = 0.903$, and therefore this protocol is much more noise-resistant than the protocol in [Acín 06a] (which had $K = 0$ for $p = 0.931$).

7.4 Generalization of the protocol

The protocol described above can also be generalized using chained Bell inequality for N measurements (in the previous section, we described the case for $N = 2$). The generalized protocol is described as follows [Acín 06b]:

- Alice carries out $(N + 1)$ measurements $x = 0, 1, ..., N$, corresponding to measurement in the bases $\{|0\rangle \pm e^{i\phi(x)|1\rangle}\}$, with $\phi(0) = \pi/2n$ and $\phi(x) = \pi x/N$ for $x = 1, 2, ..., N$.

- Bob can perform N measurements $y = 0, 1, ..., N-1$ corresponding to measuring in bases $\{|0\rangle \pm e^{-i\phi(y)|1\rangle}\}$, where $\phi(y) = \pi(y + 1/2)/N$.

- Similar to the previous case, the measurement outcomes of $x = 0$ and $y = 0$ provide highly correlated bits which are used in key generation.

- The mutual information between Alice and Bob is $I(A : B) = 1 - h(1/2 + p/2)$.

- The other measurements are used to calculate $P(ab|xy)$, and therefore are used to check the violation for the chained inequality, described in [Barrett 05a].

The chained inequality for N measurements is defined as:

$$\langle \tilde{S}_{n.s.} \rangle = \sum_{i=1}^{N} [P(x_i \neq y_{i-1}) + P(x_i \neq y_i)]. \tag{7.18}$$

Here, b_N stands for $b_0 + 1 \mathrm{mod}\ 2$.

For the Werner State (7.1) and the given measurements, the value $\langle S_{n.s.} \rangle = N[1 - p\mathrm{cos}(\pi/2N)]$. The eavesdropping strategies of an eavesdropper limited only by no-signalling constraint are in some sense similar to the previous case. We note that Alice's measurement $a = 0$ is not a part of the non-locality test. This is because, Eve can fix the output corresponding to $a = 0$, as well as produce an arbitrary violation of the chained inequality, thus faking a violation. In general, Eve's knowledge of Alice's outcome will be greater than that of Bob's outcome $[I(A : E) > I(B : E)]$, and therefore the communication goes from Bob to Alice.

Similar to the previous case, for each no-signalling distribution, either the measurement outcome corresponding to $b = 0$ is deterministic or completely random. For any measurement b used in chained inequality, [Barrett 06] shows that $\langle \tilde{S}_{n.s.} \rangle \geqslant 2P(y|b) - 1$. When $b = 0$ has a deterministic outcome, then $P(b|y) = 1$, and therefore $\langle \tilde{S}_{n.s.} \rangle \geqslant 1$, and $H(B|E) = 0$. When $b = 0$ has a uniformly random outcome, then $P(y|b) = 1/2$, and therefore $\langle \tilde{S}_{n.s.} \rangle \geqslant 0$, and $H(B|E) = 1$. It follows that:

$$I(B : E) \leqslant \langle \tilde{S}_{n.s.} \rangle. \tag{7.19}$$

Here also, the key rate K_N is defined using the Csiszár-Körner condition as follows:

$$K_N = I(A : B) - I(B : E). \tag{7.20}$$

Substituting value of $I(A : B)$ in the above equation and using inequality in Equation (7.19), we get a lower bound on K_N as:

$$K_N \geqslant 1 - h\Big(\frac{1+p}{2}\Big) - N\Big[1 - p\mathit{cos}\Big(\frac{\pi}{2N}\Big)\Big] \gtrsim 1 - h\Big(\frac{1+p}{2}\Big) - p\frac{\pi^2}{8N} - N(1-p). \tag{7.21}$$

Corresponding to equation (7.21), the key rates (K_N) for different values of N compared to the purity p of the Werner state (7.1) are plotted below:

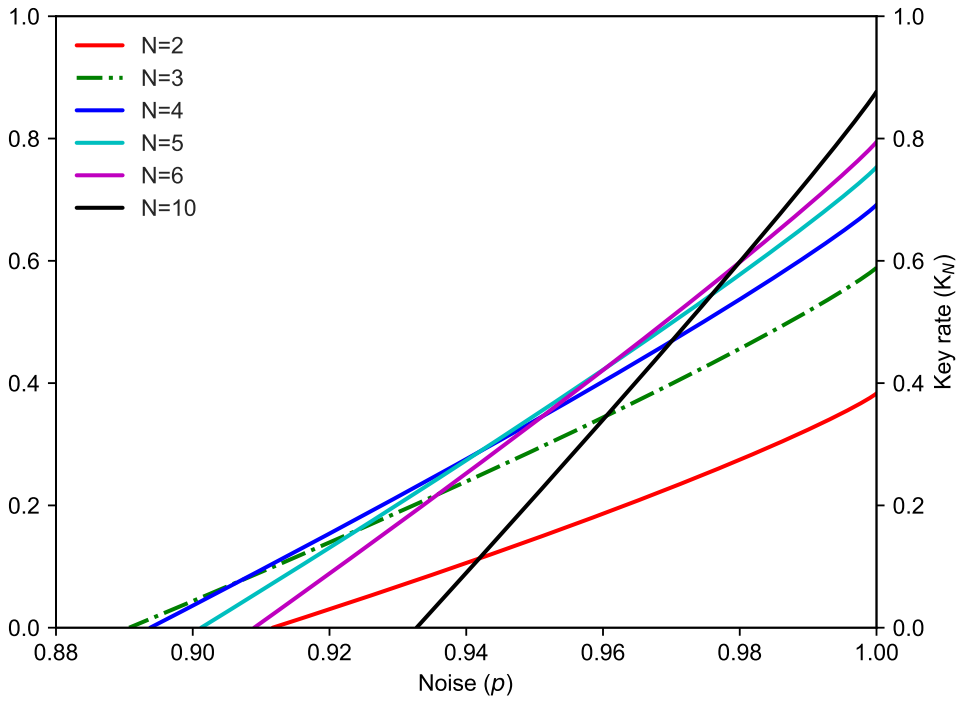

Figure 7.1: Key rate (K_N) *versus* noise (p) for different values of N

7.5 Analysis of key rate

As shown in Figure 7.1, the protocols corresponding to $N = 3$, 4 and 5 are more efficient than the CHSH based protocol ($N = 2$), for all noise levels. $N = 3$ provides the best noise resistance, as the key rate goes to zero for $p = 0.889$. Thus, in comparison to the CHSH test (where two measurements were performed), the key rate and noise resistance significantly increases by just adding one more measurement. As N increases, the protocols become more and more sensitive to noise, since they require $p \geqslant 1 - O(1/N)$. In the case with no noise (i.e. $p = 1$), $K_N \geqslant 1 - \frac{\pi^2}{8N}$, and therefore, as N increases key rate tends to 1. This implies that in absence of noise, when N is infinite, the correlations introduced are maximally non-local.

Chapter 8

DI-QKD using 3-level systems

8.1 Introduction

The study of quantum cryptography and quantum entanglement has been widely based and thoroughly discussed for two dimensional quantum variables (qubits). There have been a vast number of protocols that have been proven secure for them. The optimal attacks have been known about many qubit based schemes, and as a result strong bounds have been derived, which are quite essential in the analysis of the respective scheme of interest. But, in recent times the focus has shifted towards the underdeveloped area of quantum cryptography for higher dimensions. In this chapter, we extend the notion of device independence for higher dimensions (d dimensional *qudit* based schemes) and provide a detailed analysis for three level systems or qutrits. We describe a quantum key distribution protocol using a maximally entangled qutrit state $|\psi_3^+\rangle$, and discuss its security, for an individual eavesdropping strategy, known as cloning based attacks.

The maximally entangled qutrit state is defined as:

$$|\psi_3^+\rangle = \frac{1}{\sqrt{3}}(|0\rangle_A \otimes |0\rangle_B + |1\rangle_A \otimes |1\rangle_B + |2\rangle_A \otimes |2\rangle_B). \tag{8.1}$$

where, as usual, subscript A represents Alice's half of the maximally entangled pair, and subscript B represents Bob's half. Following the same intuition of Bell-violation as a fundamental notion for any device-independent security (as discussed in Chapter

4), we describe a Bell inequality for qutrits in the next section.

8.2 Bell violation for qutrits

We extend the novel approach of Bell inequalities for bipartite quantum systems (as discussed in Chapter 5) for higher dimensions, based on similar formalisms of linking quantum correlations and 'non-locality' i.e. the impossibility to reproduce quantum correlations with local realistic theories. Let us suppose, the two parties sharing the maximally entangled qutrit states are Alice and Bob. Alice can perform two possible measurements A_1 or A_2 and Bob can perform two measurements B_1 or B_2, with each measurement having 3 possible outcomes: 0, 1, and 2. The generalized Bell expressions corresponding to 3-dimensional quantum systems are of the form [Collins 02]:

$$\begin{aligned} S_3 = {} & P(A_1 = B_1) + P(A_1 = B_2 - 1) + P(A_2 = B_2) \\ & + P(A_1 = B_2) - P(A_1 = B_1 - 1) - P(A_2 = B_1) \\ & - P(A_2 = B_2 - 1) - P(A_1 = B_2 + 1) \leqslant 2, \end{aligned} \tag{8.2}$$

where

$$P(A_a = B_b + k) \equiv \sum_{j=0}^{2} P(A_a = j, B_b = j + k \bmod 3)$$

are the probabilities of observers A and B measuring A_a and B_b differ by k (modulo 3). The maximum value of S_3 for a local variable theory is 2 i.e. $S_3(local) \leq 2$, which is same as the CHSH inequality. For a non-local theory, S_3 can attain a maximum value of 4, i.e. $S_3(\text{non-local}) \leq 4$, which produces a violation of the inequality in equation (8.2). The protocol is based on the violation of the above inequality to ensure that the quantum correlations produced by Alice and Bob could not be completely known to an eavesdropper, which ensures security. Similar to the case of CHSH inequality used by Ekert in the E91 protocol [Ekert 91], here also the we consider the bases which produces the maximal violation of the above inequality.

The E91 entanglement-based protocol uses four bases (two pairs of mutually unbiased bases) that produce the maximal violation of the CHSH inequalities. Similarly, there

is a natural generalization of this set of bases for the qutrits as well [Durt 01], which produces the maximal violation for the state $|\psi_3^+\rangle$.

In terms of the computational bases $\{|0\rangle, |1\rangle, |2\rangle\}$, these bases are [Durt 03]:

$$|l_\phi\rangle = \frac{1}{\sqrt{3}} \sum_{k=0}^{2} e^{ik(\frac{2\pi l}{3}+\phi)}|k\rangle \tag{8.3}$$

$$= \frac{1}{\sqrt{3}}\Big[|0\rangle + e^{i(\frac{2\pi l}{3}+\phi)}|1\rangle + e^{2i(\frac{2\pi l}{3}+\phi)}|2\rangle\Big] \tag{8.4}$$

$$= \frac{1}{\sqrt{3}} e^{i(\frac{2\pi l}{3}+\phi)}\Big[\cos\big(\frac{2\pi l}{3}+\phi\big)\Big(|0\rangle + |2\rangle\Big) + |1\rangle + \sin\big(\frac{2\pi l}{3}+\phi\big)(-i)\Big(|0\rangle - |2\rangle\Big)\Big], \tag{8.5}$$

with l= 0, 1 and 2, and $\phi_i = \frac{2\pi}{12}.i$ (with i = 0,1,2,3). The maximal violation for the state $|\psi_3^+\rangle$ given by equation (8.1), corresponding to the above set of bases comes out to be equal to $\left(\frac{4}{6\sqrt{3}-9}\right) \approx 2.8729$.

Theorem 8.2.1. *The maximally entangled qutrit state $|\psi_3^+\rangle$ can be written as:*

$$|\psi_3^+\rangle = \frac{1}{\sqrt{3}} \sum_{k=0}^{2} |\beta_l\rangle \otimes |\beta_l^*\rangle, \tag{8.6}$$

where β and β^* are conjugate of each other.

Proof. We consider two bases: an arbitrary chosen bases β (with $\langle\beta_i|j\rangle = U_{ij}$), and its conjugate basis β^* (with $\langle\beta_i^*|j\rangle = U_{ij}^*$). Using the unitary matrix U_{ij}, $|\psi_3^+\rangle$ can be written as:

$$\begin{aligned}
|\psi_3^+\rangle &= \frac{1}{\sqrt{3}} \sum_{k,l,m=0}^{2} |\beta_l\rangle\langle\beta_l|k\rangle \otimes |\beta_m^*\rangle\langle\beta_m^*|k\rangle \\
&= \frac{1}{\sqrt{3}} \sum_{k,l,m=0}^{2} |\beta_l\rangle U_{lk}|\beta_m^*\rangle U_{mk}^* \\
&= \frac{1}{\sqrt{3}} \sum_{l,m=0}^{2} |\beta_l\rangle|\beta_m^*\rangle\delta_{lm} \\
&= \frac{1}{\sqrt{3}} \sum_{l=0}^{2} |\beta_l\rangle|\beta_l^*\rangle.
\end{aligned}$$

□

Thus, whenever Alice projects the state $|\psi_3^+\rangle$ in the basis β, she projects Bob's component into the conjugate basis β^*, and vice versa. Moreover, the state $|\psi_3^+\rangle$ can also be written as:

$$|\psi_3^+\rangle = \frac{1}{\sqrt{3}} \sum_{l=0}^{2} |l_\phi\rangle \otimes |l_\phi^*\rangle, \tag{8.7}$$

where

$$|l_\phi^*\rangle = \frac{1}{\sqrt{3}} \sum_{k=0}^{2} e^{-ik(\frac{2\pi l}{3}+\phi)} |k\rangle. \tag{8.8}$$

Therefore, when Alice performs a measurement in $|l_\phi\rangle$ and Bob makes a measurement in conjugate basis $|l_\phi^*\rangle$, their outcomes are perfectly correlated. The correlation of the four bases producing the maximum violation can be shown as follows: The phase term in equation (8.8) can be written as

$$-\Big[(\frac{2\pi}{3})l + \phi\Big] = k\Big[\frac{2\pi}{3}(3-l-j) - \phi + j(\frac{2\pi}{3})\Big] \text{mod } 2\pi, \tag{8.9}$$

where j is an arbitrary number. Since, $3-l-j$ varies from 0 to 1(mod 2) when l varies from 0 to 2, therefore ϕ^* basis is the same $\tilde{\phi}$, where $\tilde{\phi} = \phi + j(\frac{2\pi}{3})$. Thus, the basis with even values of i [i=0,2, $\phi_i = \frac{2\pi}{4d}i$] are preserved under phase conjugation, whereas the bases associated with the odd values of i [$i = 1,3$] are interchanged. Thus, the four bases are pairwise correlated. Following the above discussion, the maximally entangled state for qutrits can be written as:

$$|\psi_3^+\rangle = \frac{1}{\sqrt{3}}(|0_\phi\rangle \otimes |0_\phi^*\rangle + |1_\phi\rangle \otimes |1_\phi^*\rangle + |2_\phi\rangle \otimes |2_\phi^*\rangle). \tag{8.10}$$

Since there exists a 100% correlation between the two measurement bases $|l_\phi\rangle$ and $|l_\phi^*\rangle$ when Alice and Bob make a measurement in the same phase ϕ_i, the case where the phases of Alice's and Bob's bases match are suitable for generation of a secure key. The cases where there's a difference in their phases could be used to detect the presence of an eavesdropper via the calculation of Bell violation. Based on the above discussion, a protocol for maximally entangled qutrits is given below.

8.3 Device-independent protocol for qutrits

We describe a secure device-independent quantum key distribution protocol for 3-dimensional quantum system (qutrits). It is described as follows:

- A source, situated in the quantum channel shared between Alice and Bob, emits a maximally entangled qutrit state $|\phi_3^+\rangle$, which is shared between Alice and Bob.
- Both parties choose their measurement settings randomly and independent from each other, and record the corresponding outcomes.
- Alice can perform one of the three measurements, $a = 0$, 1 or 2, which correspond to measurement of her qutrit in the following bases:

$$\{|l_{\phi_0}\rangle\} = \Big\{\frac{1}{\sqrt{3}}\sum_{k=0}^{2} e^{ik(\frac{2\pi l}{3})}|k\rangle\Big\}, \qquad l = 0,1,2 \qquad \text{for } a{=}0$$

$$\{|l_{\phi_1}\rangle\} = \Big\{\frac{1}{\sqrt{3}}\sum_{k=0}^{2} e^{ik(\frac{2\pi l}{3}+\frac{\pi}{6})}|k\rangle\Big\}, \qquad l = 0,1,2 \qquad \text{for } a{=}1$$

$$\{|l_{\phi_2}\rangle\} = \Big\{\frac{1}{\sqrt{3}}\sum_{k=0}^{2} e^{ik(\frac{2\pi l}{3}+\frac{\pi}{3})}|k\rangle\Big\}, \qquad l = 0,1,2 \qquad \text{for } a{=}2$$

- Similarly, Bob can perform one of the three measurements, $b = 0$, 1 or 2, which correspond to measurement of his qutrits in the following bases:

$$\{|l^*_{\phi_0}\rangle\} = \Big\{\frac{1}{\sqrt{3}}\sum_{k=0}^{2} e^{-ik(\frac{2\pi l}{3})}|k\rangle\Big\}, \qquad l = 0,1,2 \qquad \text{for } b{=}0$$

$$\{|l^*_{\phi_2}\rangle\} = \Big\{\frac{1}{\sqrt{3}}\sum_{k=0}^{2} e^{-ik(\frac{2\pi l}{3}+\frac{\pi}{3})}|k\rangle\Big\}, \qquad l = 0,1,2 \qquad \text{for } b{=}1$$

$$\{|l^*_{\phi_3}\rangle\} = \Big\{\frac{1}{\sqrt{3}}\sum_{k=0}^{2} e^{-ik(\frac{2\pi l}{3}+\frac{\pi}{2})}|k\rangle\Big\}, \qquad l = 0,1,2 \qquad \text{for } b{=}2$$

- Alice and Bob perform the chosen measurements on each of their qutrits.
- After measuring all pair of their particles, the measurement bases are revealed by Alice and Bob.
- When Alice makes a measurement $a = 0$ and Bob makes a measurement $b = 0$, their outcomes are perfectly correlated (as discussed in the previous section),

and therefore are suitable for raw key generation.

- The other measurements ($a = 1, 2$ and $b = 1, 2$) produce the maximal violation of the Bell inequality. Therefore, in this case both Alice and Bob reveal their outcomes and compute the violation of the Bell inequality. Privacy amplification and information reconciliation steps on the strongly correlated outcomes will provide an identical pair of secret keys.

Similar to the protocol described in the previous chapters, the security of this protocol is also based on the violation of a 3-dimensional Bell inequality. In the next section, we analyze the security of the protocol for cloning based attacks.

8.4 Eavesdropping strategy and key rate

In this section, we analyze the security of the protocol against individual attacks (i.e. where Eve monitors each of the qutrit separately). We discuss eavesdropping strategies known as cloning-based attacks, which is based on quantum cloning machines. In these kinds of attacks, Eve imperfectly clones Alice's qutrit and keeps the original with herself, while sending the copy to Bob.

A general class of cloning transformations are used as defined in [Cerf 00b, Cerf 00a]. Suppose, Alice sends the input state $|\psi\rangle$, the transformed state become:

$$|\psi\rangle \longrightarrow \sum_{m,n=0}^{3} a_{m,n} U_{m,n} |\psi\rangle_A |B_{m,-n}\rangle_{B,C} \tag{8.11}$$

$$= \sum_{m,n=0}^{3} b_{m,n} U_{m,n} |\psi\rangle_B |B_{m,-n}\rangle_{A,C}. \tag{8.12}$$

Here, amplitudes a_{mn} characterize the cloner with $\sum_{m,n}^{2} |a_{m,n}|^2 = 1$, and the states $|B_{m,n}\rangle_{A,C}$ are 3-dimensional Bell states, which are a set of 9 orthonormal entangled states of two qutrits, described as:

$$|B_{m,n}\rangle = \frac{1}{\sqrt{3}} \sum_{k=0}^{2} e^{2\pi i (kn/3)} |k\rangle |k+m\rangle,$$

with $m, n = 0, 1, 2$. The kets must be taken modulo 2 here.

The operators $U_{m,n}$ form a group of qutrit error operators, generalizing the Pauli matrices for qutrits, where m represent the *shift errors* (corresponding to bit flip σ_x) and n represent the *phase errors* (corresponding to phase flip σ_z). The form of $U_{m,n}$ is described as:

$$U_{m,n} = \sum_{k=0}^{2} e^{2\pi i(kn/3)} |k+m\rangle\langle k|.$$

Tracing over the systems B and C in equation (8.11) gives the final state of clone A described by:

$$\rho_A = \sum_{m,n=0}^{2} |a_{m,n}|^2 |\psi_{m,n}\rangle\langle\psi_{m,n}|, \tag{8.13}$$

where $|\psi_{m,n}\rangle = U_{m,n}|\psi\rangle$. Similarly, tracing over the systems A and C in equation (8.12) gives the final state of clone B described by:

$$\rho_B = \sum_{m,n=0}^{2} |b_{m,n}|^2 |\psi_{m,n}\rangle\langle\psi_{m,n}|. \tag{8.14}$$

Note that $a_{m,n}$ and $b_{m,n}$ are amplitude functions that are dual under a Fourier transformation [Cerf 00a]:

$$b_{m,n} = \frac{1}{3} \sum_{x,y=0}^{2} e^{2\pi i \frac{nx-my}{3}} a_{x,y}. \tag{8.15}$$

Let's assume that Eve clones the state $|\psi\rangle$ sent by Alice to Bob, and resends the imperfect clone (A) to Bob, while keeping the original (B) with her. Eve will measure her clone in same basis as Bob (ϕ-basis) and her ancilla (C) in the conjugate basis (ϕ^*-basis). We rewrite the cloning transformations in these bases. These are describes as:

$$|B_{m,n}\rangle = \frac{1}{\sqrt{3}} \sum_{l=0}^{2} e^{im(\frac{2\pi}{3}(l-n)+\phi)} |l_\phi\rangle |(l-n)^*_\phi\rangle = e^{im(\frac{-2\pi}{3}n+\phi)} |\tilde{B}_{-n_\phi, m^*_\phi}\rangle, \tag{8.16}$$

where,

$$|\tilde{B}_{m_\phi, n^*_\phi}\rangle = \frac{1}{\sqrt{3}} \sum_{k=0}^{2} e^{2\pi i(\frac{kn}{3})} |k_\phi\rangle |(k+m)^*_\phi\rangle \tag{8.17}$$

and

$$U_{m,n} = \sum_{k=0}^{2} e^{-im(\frac{2\pi}{3}(k+n)+\phi)} |(k+n)_\phi\rangle\langle k_\phi| = e^{-im(\frac{2\pi}{3}n+\phi)} \tilde{U}_{n_\phi, -m_\phi}, \tag{8.18}$$

where the subscript tilde refer to the new (ϕ and ϕ^*) bases. After substitution in equation (8.11), we get:

$$|\psi\rangle \longrightarrow \sum_{m,n=0}^{3} a_{m,n} U_{m,n} |\psi\rangle_A |B_{m,-n}\rangle_{B,C} = \sum_{m,n=0}^{2} \tilde{a}_{m,n} \tilde{U}_{m_\phi,n_\phi} |\psi\rangle_A |\tilde{B}_{m_\phi,n_\phi}\rangle_{B,C}, \quad (8.19)$$

where the amplitudes $\tilde{a}_{n,-m} = a_{m,n}$. The cloning machine which has same effect when expressed in the four optimal bases i.e. when $\phi_i = \frac{2\pi}{12}.i$ (i=0,1,2,3), which imposes the constrains on amplitudes $a_{m,n}$ characterizing the cloner, must be of the form

$$a_{m,n} = \begin{pmatrix} v & x & x \\ y & y & y \\ z & z & z \end{pmatrix}. \quad (8.20)$$

The fidelity of the clone A that is sent to Bob, when copying a state $|\psi\rangle$ can be written in general as:

$$F_A = \langle\psi|\rho_A|\psi\rangle = \sum_{m,n=0}^{2} |a_{m,n}|^2 \langle\psi|\psi_{m,n}\rangle|^2. \quad (8.21)$$

Using the cloning machine defined in equation (8.20), the fidelity F_A can be written as:

$$F_A = \langle l_\phi|\rho_A|l_\phi\rangle = v^2 + y^2 + z^2. \quad (8.22)$$

Similarly, the fidelity of the clone kept by Eve is given by

$$F_B = \langle\psi|\rho_B|\psi\rangle = \sum_{m,n=0}^{2} |b_{m,n}|^2 \langle\psi|\psi_{m,n}\rangle|^2. \quad (8.23)$$

Using equation (8.15), it comes out to be equal to:

$$F_B = \frac{v^2 + 2x^2 + 12y^2 + 8xy + 4vy}{3}. \quad (8.24)$$

The value of F_B is maximum when y and z are equal. After the basis of Alice and Bob are revealed, Eve makes a measurement on her copy B and the cloning machine C, in the same basis as Bob, the difference (modulo 3) of the outcomes gives Bob's error m. Thus, conditional on whether error is 0 or not, the mutual information between

Alice and Eve is given by:

$$I(A:E|m=0) = \log_2(3) - H\Big[\frac{(v+2y)^2}{3F_A}, \frac{(v-y)^2}{3F_A}, \frac{(v-y)^2}{3F_A}\Big] \tag{8.25}$$

$$I(A:E|m\neq 0) = \log_2(3) - H\Big[\frac{2(x+2y)^2}{3(1-F_A)}, \frac{2(x-y)^2}{3(1-F_A)}, \frac{2(x-y)^2}{3(1-F_A)}\Big], \tag{8.26}$$

where $F_A = v^2 + 2y^2$, since $y = z$, as previously discussed. On an average, Eve's information is

$$I_{AE} = F_A I(A:E|m=0) + (1-F_A) I(A:E|m\neq 0). \tag{8.27}$$

The mutual information between Alice and Bob is given by:

$$I_{AB} = log_2 3 - H\Big[F_A, \frac{1-F_A}{2}, \frac{1-F_A}{2}\Big] \tag{8.28}$$

To get a lower-bound on the secret key rate i.e. the rate R at which Alice and Bob can generate a secret key via privacy amplification, we use the Csisżar and Körner theorem [Csiszar 78], which states that if Alice, Bob and Eve share many independent realizations of a probability distribution $p(a,b,e)$, then there exists a protocol that generates a number of key bits per realization satisfying

$$R \geq \max(I_{AB} - I_{AE}, I_{AB} - I_{AE}) \tag{8.29}$$

Since Eve exactly knows Bob's error m, $I_{AE} = I_{BE}$, for one-way communication on the classical channel, $I_{AB} > I_{AE}$ is the necessary and sufficient condition to generate a key between Alice and Bob. Thus, the protocol ceases to generate secret key bits when Eve's and Bob's information match.

The maximal fidelity F_A, which provides the minimal error rate, such that $I_{AB} = I_{AE}$, comes out to be equal to:

$$F_A = 0.7753 \tag{8.30}$$

Thus, the acceptable error rate D equals to

$$D = 1 - F_A = 0.2247. \tag{8.31}$$

8.5 Conclusion and furthur discussion

The protocol described for qutrits in the previous section can be genralized for even higher dimensions. Say, the dimension of the quantum system used is described by d. The maximally entangled d-dimensional state is:

$$|\psi_d^+\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |jj\rangle. \tag{8.32}$$

The Bell inequality for d dimensions is defined as [Collins 02]:

$$\begin{aligned} S_d = \sum_{k=0}^{[\frac{d}{2}]-1} \Big(1 - \frac{2k}{d-1}\Big)\Big\{ &+ [P(A_1 = B_1 + k) + P(B_1 = A_2 + k + 1) \\ &+ P(A_2 = B_2 + k) + P(B_2 = A_1 + k)] - [P(A_1 = B_1 - k - 1) + \\ &P(B_1 = A_2 - k) + P(A_2 = B_2 - k - 1) + P(B_2 = A_1 - k - 1)]\Big\}. \end{aligned} \tag{8.33}$$

Similar to the qutrit case, the bases that maximally violate d dimensional Bell inequality are:

$$|l_\phi\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{ik(\frac{2\pi l}{d} + \phi)} |k\rangle, \tag{8.34}$$

with $l = 0,1,...,(d-1)$, and $\phi_i = \frac{2\pi}{4d} i$ (with $i = 0,1,2,3$). The state $|\psi_d^+\rangle$ can be written as the following:

$$|\psi_d^+\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} |l_\phi\rangle \otimes |l_\phi^*\rangle, \tag{8.35}$$

where

$$|l_\phi^*\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} e^{-ik(\frac{2\pi l}{d} + \phi)} |k\rangle. \tag{8.36}$$

The maximal violation of the Bell inequality described in equation (8.33) for the maximally entangled state for two qudits $\mathcal{C}^d \otimes \mathcal{C}^d$ is described in Table 8.1. It can be seen that the maximal violation of Bell inequality for the maximally entangled state $|\psi_d^+\rangle$ increases with dimension d.

The generalized protocol will be similar to the protocol described for qutrits, where Alice chooses her measurements in basis $|l_\phi\rangle$ described in equation (8.34), and Bob chooses his measurements in the conjugate basis $|l_\phi^*\rangle$. The cases with both of them

Dimension d	**Violation for $\|\psi_d^+\rangle$**
3	2.8729
4	2.8962
5	2.9105
6	2.9202
7	2.9272
8	2.9324

Table 8.1: Violation of Bell inequality for state $|\psi_d^+\rangle$ [Acín 02].

measuring the same phase ϕ_i could be use to generate the secret key, and the rest of the cases could be use to check the Bell violation (similar to the case of qutrits).

In presence of some noise, the maximally entangled state $|\psi_d^+\rangle$ transforms in a state ρ described by:

$$\rho = p|\psi_d^+\rangle\langle\psi_d^+| + (1-p)\frac{\mathbb{1}}{d^2} \tag{8.37}$$

where p is the probability that the state is unaffected by noise. The value of Bell inequality for state ρ is given by [Collins 02]

$$S_d(\rho) = pS_d(|\psi_d^+\rangle). \tag{8.38}$$

This implies that the Bell inequality $S_d(\rho)$ is violated if $p > \frac{2}{S_d(|\psi_d^+\rangle)} = p_{min}$. Since, the violation of Bell violation increases with dimension d, therefore p_{min} decreases with increase in dimensions. Thus, as dimension d increases, the robustness against noise increases.

Chapter 9

Drawbacks and loopholes of DI-QKD

As discussed in previous chapters, device-independent quantum key distribution in principle provides a higher security than the standard device-dependent QKD. But till now, we have only looked at the theoretical aspects of it. The physical implementations of DI-QKD are quite challenging. Since the security of DI-QKD rely on the violation of some Bell inequalities, the protocols are subject to loopholes and drawbacks, which impacts its security. We describe some of those drawbacks and loophole of DI-QKD as follows:

- ***The detection loophole***: In the physical implementation to distribute entanglement between Alice and Bob, photon-based signals are used. But, the detection of single photons is difficult. It is possible that these signals may not get detected. This may happen due to some inefficiencies of the detectors or due to some particle losses that occurred between the source and the detectors. This means that some trials in a Bell experiment give a "no outcome" result. The *detection-loophole* exploits the idea that it is a local variable that determines whether a photon signal will be registered or not. Only if the measurement settings of the device agrees with a scheme that is pre-determined, then only the signal will be detected. In this way, provided that the detector efficiencies η are below a certain threshold, non-local correlation can be reproduced by a purely local model.

Experiments testing non-locality have been performed to overcome the detection loophole, by only recording the events in which both Alice's and Bob's measurement devices produced an output, and discarding events in which no signal has been detected. This accounts to performing a post-selection on the measurement data. In a non-adversarial setting this is not problematic [Pearle 70], but if it is presumed that the measurement devices are adversarial (provided by an untrusted party) and "no outcome" results are discarded, then it is possible that, the adversary might selectively choose a "no outcome" result, allowing them to post-select for favourable conditions. In particular, the devices may post-select for a particular measurement setting, allowing the adversary to have control over the measurement settings. Thus, post-selection makes it possible for the adversary to fake the violation of a Bell inequality, even in a purely local theory [Clauser 74].

One possible remedy to the above problem is as follows: The proper security analysis of DI-QKD with inefficient detectors must take into account all measurement outcomes produced by Alice's and Bob's devices, which should also include a "no-detection" outcome. A possible strategy would be to make a pre-agreement, that a lack of answer would be treated as one of the measurement outcome (which shall remain same during the experiment). *A violation of Bell inequalities produced by the above statistics is conclusive.*

- ***The locality loophole*** : While performing the key distribution, there is a possibility that devices could talk to each other, such that one party may have information about the input (measurement settings) of the other, before producing his/her own output. It is then trivial for a classical model to account for the non-locality of the correlations that are observed i.e. it is trivial to violate a Bell's inequality in a classical deterministic way, and therefore the security is compromised. This is known as the *locality loophole*[Aspect 75].

  The locality loophole is overcome by performing measurements at a space-like separation between Alice and Bob, such that no signals with speed less than the speed of light could travel between their devices. In this way, the parties cannot have the knowledge about the measurement settings of the other.

In the context of device-independence, it is not necessary to close the locality loophole. It is sufficient just to guarantee that no photon signals could travel between Alice and Bob. This can be achieved by creating Alice's and Bob's laboratories to be secure, such that no unwanted information can leak to the outside. This is similar to the assumption made in standard QKD. Without this assumption, any kind of quantum key distribution does not make sense.

- Many of the first DI-QKD protocols using violation of Bell inequality as a basis for key distribution [Barrett 05a, Mayers 98b] have *negligible key rates* as well *poor noise tolerance* as compared to the standard QKD. The protocol by Barret, Haardy and Kent require as many number of device as the number of entangled pairs in the protocol, so as to keep up with the no-signalling requirements in the protocol. This is a major drawback. Many protocols have been developed since then, which provide much better key rates and noise tolerance, but only within certain restrictions [Pironio 09, Acín 06a, McKague 09].

- Even if the locality loophole is closed, the practical applications of DI-QKD are challenging, because at large separations, it is difficult to generate correlations that violate a Bell inequality.

- ***The coincidence loophole***: Photons used in most of the Bell experiments are very much likely to get absorbed in the air or some other surfaces before reaching the detector. It is also possible that photons from some other source (non-signal photons) or dark counts lead to clicks in one of the detector. Therefore, after the experiment, the users pick out coincidences (i.e the times when detectors of both parties clicked simultaneously) from the collected data for further analysis, by making a decision about whether their detection times are close or not. This could be exploited by Eve. She could manufacture devices that delay the detection time of each of the two particles by some amount on the basis of some hidden variables carried by the particles and the detector settings, which can lead to fake correlations being observed [Larsson 04].

  The coincidence loophole can be ruled out by working with some fixed detection windows, which should be short enough that most photon pairs interacting with the detectors in the same window originate with the same emission statistics

(representing a single click), and long enough that the two components of a particular photon pair are not separated into two different windows due to the window boundary.

Although DI-QKD contains many drawbacks and loopholes, it is still considered to be the one which provides the strongest form of secure communication. The practical value of DI-QKD is still limited, due to various loopholes and negligible key rate it achieves, but its theoretical advancements are extensive. In recent developments, much of the focus is laid towards designing loophole-free Bell experiments, which should be within experimental reach in the near future.

Chapter 10

Summary & Conclusions

In this thesis, we have looked at the quantum key distribution process in a device-independent scenario. Quantum key distribution (QKD) protocols allow two separated parties to share secure private key over a public channel. The security of the key is guaranteed by the laws of quantum mechanics, given that the error rate is below a certain threshold. But the security of the traditional QKD schemes is based on several assumptions, which could result in unsafe communications in their practical applications.

Device-independent quantum key distribution provides a relaxation to the assumption of devices being truthful, which is one of the fundamental assumptions of standard QKD. In DI-QKD, no assumptions are made even about the operational specifications of the devices. Rather, their security is based on some tests of non-locality, such as the violation of Bell inequality. Several protocols based on the concept of device independence have been formulated.

We analyzed the basic device-independent protocol for qubits (2-level systems), whose security is based on the violation of CHSH inequality. The security of the protocol, in the presence of an adversary, which was limited only by no-signalling alone, was analyzed. We extended the notion of device independence for qutrits (3-level systems) and higher dimensions. The basis of security was still the violation of higher dimensional Bell inequalities. We concluded that, as the dimensions of the quantum systems increases, the protocols for key sharing become more and more robust to

noise. Further, the limitations in physical implementations of DI-QKD due to many loopholes and drawbacks were also assessed.

Future outlook

The research in DI-QKD has a lot of potential and several of its possible domains are yet to be explored. We discuss some of the possible future directions of the field, that could yield significant results in the near future.

A significant area of research in DI-QKD is to overcome its shortcomings, so as to make DI-QKD experimentally feasible. Some possibilities to overcome the drawbacks and loopholes of DI-QKD has been discussed in Chapter 9, but still a lot of work has to be done to make DI loophole-free.

Throughout the thesis, we have looked at eavesdropping strategies for DI corresponding to individual attacks only. It could be analyzed how the security of the protocols is modified in case of collective attacks. It is worth looking at whether the violation of Bell inequalities is a sufficient condition for security against collective attacks as well. Some part of this has been analyzed in [Pironio 09].

Although, there has been significant amount of research in the field of device independence quantum key distribution, but it only had success from a theoretical point of view. The protocols discussed in Chapter 8 as well in [Masanes 06], prove unconditional security of QKD protocols against eavesdroppers limited by no-signalling, but the key rates and noise resistance achieved cannot be practically implemented, when they are applied to quantum correlations. The possibility of incorporating new constraints associated with quantum mechanics to enhance key rates and resistance to noise can be looked upon.

Till now, DI-QKD is said to be practically impossible. Techniques such as semi-device-independent quantum key distribution (SDI-QKD), have been thought of as an alternative of DI-QKD. In SDI-QKD, devices used by trusted parties are still non-characterized (similar to the DI case), but the dimensions of the quantum systems used in the protocol are assumed to be bounded. In this form of DI security, the devices are assumed to produce quantum systems of a particular dimension. This assumption

make this form of quantum key distribution experimentally feasible. SDI-QKD for one-way communication has been proven in [Pawłowski 11], but applying it to more general attacks, as well as study of robustness against imperfections such as detection efficiency and losses still remains an open question. It would also be interesting to find relationship between the entanglement-based DI and one-way SDI based QKD.

Appendix A

Basic probability theory

The knowledge of some elementary probability theory is necessary in the study of quantum computation and information. As discussed, the concept of device-independence in entirely based on the family of conditional probability distributions of the observed statistics of the devices used. Therefore, some fundamental definitions of probability are needed to be understood. This appendix reviews some basic definitions and results of probability theory that have been used in some calculations in this thesis.

The essence of probability theory comes from the concept of a *random variable*. The possible values a random variable may take represents the possible outcomes of an event that is yet to occur. The random variable is denoted by capital letters, A, and the value that it takes is denoted by small letters, a. A random variable A may take a value a, from a set of possible values, with probability $P(A = a)$. For a random variable, its probability distribution describes how the probabilities are distributed over the possible values of the random variable. In this discussion, we assume that the set of possible values Ω of a random variable is finite.

Some basic definitions of probabilities of random variables are described as follows.

Definition A.0.1. The *conditional probability* of a random variable $A = a$ given another random variable $B = b$ is defined as

$$P(A = a|B = b) = \frac{P(A = a, B = b)}{P(B = b)} \tag{A.1}$$

where $P(A, B)$ is the probability of $A = a$ *and* $B = b$, also known as the *joint probability distribution*.

When $P(B = b) = 0$, it is by convention that $P(A = a|B = b) = 0$. A conditional probability distribution can be seen as a system taking as input the random variable B and giving a (probabilistic) output A, depending on the input b.

Definition A.0.2. Random variables A and B are said to be *independent*, if

$$P(A = a,\ B = b) = P(A = a)P(B = b), \qquad \forall\ a,\ b. \tag{A.2}$$

When the joint probability distribution of two (or more) random variables is given, we sometimes consider the *marginal distribution* of X. This is the distribution of the random variable A of a joint distribution when the value of the second random variable B is ignored.

Definition A.0.3. Given the joint probability distribution $P(A = a, B = b)$, of two random variables $A = a$ and $B = b$, the marginal distribution of A is given by

$$P(A = a) = \sum_b P(A = a, B = b). \tag{A.3}$$

Here, the sum is over all possible values b of B.

The relationship between conditional probabilities for B given A to those for A given B is given by *Bayes' theorem*.

Definition A.0.4. For random variables $A = a$ and $B = b$, Bayes' theorem states that

$$P(A = a|B = b) = P(B = b|A = a)\frac{P(A = a)}{P(B = b)}. \tag{A.4}$$

Proof. By equation (A.1),

$$P(A = a|B = b) = \frac{P(A = a, B = b)}{P(B = b)}.$$

Multiplying and dividing the right side of equation (A.4) by $P(A = a)$, gives

$$P(A = a|B = b) = \frac{P(A = a,\ B = b)P(A = a)}{P(B = b)P(A = a)}, \tag{A.5}$$

where $\frac{P(A=a,\ B=b)}{P(A=a)} = P(B = b|A = a)$. Hence,

$$P(A = a|B = b) = P(B = b|A = a)\frac{P(A = a)}{P(B = b)}. \tag{A.6}$$

□

Another important result of probability theory is the *law of total probability*. It is defined as

Definition A.0.5. For two random variables A and B, the probability of B can be expressed in terms of probabilities of A, and the conditional probabilities B given A,

$$P(B = b) = \sum_a P(B = b|A = a)P(A = a). \tag{A.7}$$

Here, sum is taken over all possible values a of A.

Proof. Using equation (A.1),

$$P(B = b|A = a) = \frac{P(A = a, B = b)}{P(A = a)}.$$

Therefore,

$$\sum_a P(B = b|A = a)p(A = a) = \sum_a \frac{P(A = a, B = b)}{P(A = a)}P(A = a) \tag{A.8}$$

$$= \sum_a P(A = a, B = b). \tag{A.9}$$

Since, the sum is over all possible values A can take, therefore

$$\sum_a P(B = b|A = a)P(A = a) = P(B = b).$$

□

We also define the expectation or average for a random variable A.

Definition A.0.6. The *expectation* of a random variable A is given by:

$$\mathbf{E}(A) \equiv \langle A \rangle = \sum_a P(a)a. \tag{A.10}$$

Here also, the sum is taken over all possible values of A.

We have provided a very brief overview of some definitions of probability theory. There are many texts available which provide a more detailed introduction to the theory of probability. One such text for reference is: Probability and random processes by Grimmett and Stirzaker [Grimmett 01].

Appendix B

BB84: not secure in the device-independent scenario

We mentioned in Chapter 4, that the BB84 quantum key distribution protocol is no longer secure, if Alice and Bob share four dimensional quantum systems, instead of qubits. We illustrate this using the following example.

We consider the entanglement-based version of the BB84 protocol [Bennett 14]. Both Alice and Bob have a measuring device each. Suppose Alice's device takes in a classical input (measurement setting) $a \in \{0,1\}$, and produces an output (measurement outcome) $x \in \{0,1\}$. Similarly, Bob's device takes an input $b \in \{0,1\}$, and produces an output $y \in \{0,1\}$. We assume that both devices act on a two-dimensional Hilbert space of the incoming particles emitted by a source. Say, the measurement setting '0' corresponds to measurement in σ_x basis and the measurement setting '1' corresponds to measurement in σ_z. Suppose that, in the absence of noise, Alice and Bob observe the correlations given below:

$$\begin{aligned} P(xy|00) = P(xy|11) = 1/2 \qquad & \text{if } x = y, \\ P(xy|01) = P(xy|10) = 1/4 \qquad & \forall\ x, y. \end{aligned} \tag{B.1}$$

This implies that, if Alice and Bob make a measurement in the same bases, their outcomes are always perfectly correlated, otherwise, they get completely random outcomes. Suppose, that the state $|\phi\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^2$ correspond to the two-qubit state of the

incoming particles. Therefore, the above correlations in terms of operators σ_x and σ_z can be described as:

$$\begin{aligned} \langle\phi|\sigma_z \otimes \sigma_z|\phi\rangle &= \langle\phi|\sigma_z \otimes \sigma_z|\phi\rangle = 1, \\ \langle\phi|\sigma_z \otimes \sigma_x|\phi\rangle &= \langle\phi|\sigma_x \otimes \sigma_z|\phi\rangle = 0. \end{aligned} \tag{B.2}$$

For the maximally entangled state $\frac{(|00\rangle+|11\rangle)}{\sqrt{2}}$, the above set of conditions perfectly hold. Therefore, Alice and Bob can securely extract a key from their measurement data, using the state and measurement settings described above [Pironio 09].

But, in the case of DI scheme, Alice and Bob cannot presume that their device's measurement settings '0' and '1' correspond to σ_x and σ_z respectively. Also, there can be no assumption made on the dimension of the Hilbert space. Suppose that the source (controlled by Eve) emits a 4-dimensional ($\mathbb{C}^4 \otimes \mathbb{C}^4$) state, given by a density matrix ρ_{AB}:

$$\rho_{AB} = \frac{1}{4} \sum_{s_0,s_1=0}^{1} (|s_0, s_1\rangle\langle s_0 s_1|)_A \otimes (|s_0, s_1\rangle\langle s_0 s_1|)_B, \tag{B.3}$$

and the device's measurement settings '0' and '1' correspond to $\sigma_z \otimes I$ and $I \otimes \sigma_z$ respectively. Similar to the device-dependent case, here also Alice's and Bob's outcomes are perfectly correlated if their measurement bases are the same, and are completely uncorrelated otherwise. However, instead of the state ρ_{AB}, suppose Eve sends a tripartite state ρ_{ABE} given by:

$$\rho_{ABE} = \frac{1}{4} \sum_{s_0,s_1=0}^{1} (|s_0, s_1\rangle\langle s_0 s_1|)_A \otimes (|s_0, s_1\rangle\langle s_0 s_1|)_B \otimes (|s_0, s_1\rangle\langle s_0 s_1|)_E. \tag{B.4}$$

Now, Eve can have a perfect copy of Alice's and Bob's local states, and therefore will have complete knowledge of their measurement outcomes.

Thus, the device-independent variant of BB84 protocol is insecure, and the assumption of a 2-dimensional Hilbert space in the usual BB84 protocol is really crucial. Relaxing this assumption (as seen in the above example) invalidates the security of the protocol.

Appendix C

Derivation of CHSH inequality

In this appendix, we derive the results of the CHSH inequality, as defined in Section 5.1. First, we provide an overview of the idea of local polytope and its facets, which will be furthur used to calculate the constraints for the inequality. Suppose, the measurement settings of Alice are described by $a \in \mathcal{A}$ and her measurement outcomes are denoted by $x \in \mathcal{X}$. Similarly, the measurement settings of Bob are described by $b \in \mathcal{B}$, and his measurement outcomes are denoted by $y \in \mathcal{Y}$. Here $(\mathcal{A}, \mathcal{B})$ and $(\mathcal{X}, \mathcal{Y})$ denote the sets of possible inputs and outputs of Alice's and Bob's devices. For a particular scenario: $(\mathcal{A}, \mathcal{X}; \mathcal{B}, \mathcal{Y})$, the set $\mathcal{L}$ of all probability distributions that can be obtained from a local variable theory is *convex* [Scarani 13]. Mathematically stating, if probability distributions $\mathcal{P}_i \in \mathcal{L}$ and $\mathcal{P}_j \in \mathcal{L}$, then $\alpha\mathcal{P}_i + (1-\alpha)\mathcal{P}_j \in \mathcal{L}$, for all $\alpha \in [0,1]$.

The set $\mathcal{L}$ can be completely determined by describing all extremal points belonging to that set. Extremal points are those points that cannot be written as convex combination of other points. Any $\mathcal{P} \in \mathcal{L}$ can be written as a convex sum of deterministic local variables. Moreover, each deterministic local point is an extremal point of $\mathcal{L}$. A convex set with a finite number of extremal points is called a *polytope*. Thus, $\mathcal{L}$ is a *local polytope* for the scenario $(\mathcal{A}, \mathcal{X}; \mathcal{B}, \mathcal{Y})$.

A polytope $\mathcal{L}$ in $\mathbb{R}^k$ is bound by $(k-1)$-dimensional hyperplanes called *facets*. These facets must have at least D extremal points lying on it, while the other extremal points lie on the same side of it. Mathematically, it can be stated as follows: if the

points $\mathcal{P}$ of the facet follow the equation $n.\mathcal{P} = f$, then

$$n.\mathcal{P} \leq f \qquad \forall\ \mathcal{P} \in \mathcal{L}, \tag{C.1}$$

where $n \in \mathbb{R}^k$ is the vector normal to the facet, directed outside the polytope. In case of probability polytope like $\mathcal{L}$, some facets are given by equations $P(x, y|a, b) = 0$ and $P(x, y|a, b) = 1$. These facets are *trivial*, since these constraints are satisfied by all probability distributions, $0 \leq P(x, y|a, b) \leq 1$. We ought to look at other non-trivial facets given by equation (C.1). These non-trivial facets form the well-known Bell inequalities.

For the case of CHSH inequality, there are two measurement settings and two possible measurement outcomes each for Alice's and Bob's device. We denote the measurement settings by (a,b) and assume that the outcomes of the measurements are binary. We aim to look for constraints for set of probability distribution $\mathcal{P}$ belonging to $\mathcal{L}$, by working out the facets of $\mathcal{L}$.

For such a scenario, the *correlation-coefficient* is defined as:

$$E_{xy} = P(x = y|a, b) - P(x \neq y|a, b). \tag{C.2}$$

We note that any quadruple of numbers $m = (E_{00}, E_{01}, E_{10}, E_{11})$ is a valid correlation vector, with an additional constraint

$$-1 \leq \ E_{ab} \ \leq 1. \tag{C.3}$$

Therefore, vectors with $||m||^2 = 4$, corresponding to all those vectors with $+1$ and -1 as their components, are the extremal points of a polytope in $\mathbb{R}^4$. There exist 16 such vectors.

We assume that the measurement outcome x, $y \in \{+1,-1\}$, implying that $E_{ab}=\langle x_a, y_b\rangle$. For deterministic local points, $E_{ab} \stackrel{\mathrm{D}}{=} x_a y_b$, which implies

$$E_{00}E_{01}E_{10}E_{11} = 1. \tag{C.4}$$

So, the extremal points of the *local correlation polytope* are the vectors given by:

$$\begin{aligned} t_1 &= (+1,+1,+1,+1) \qquad & t_5 &= -t_1 = (-1,-1,-1,-1) \\ t_2 &= (+1,+1,-1,-1) \qquad & t_6 &= -t_2 = (-1,-1,+1,+1) \\ t_3 &= (+1,-1,+1,-1) \qquad & t_7 &= -t_3 = (-1,+1,-1,+1) \\ t_4 &= (+1,-1,-1,+1) \qquad & t_8 &= -t_4 = (-1,+1,+1,-1). \end{aligned} \tag{C.5}$$

The set $\{t_1,\ t_2,\ t_3,\ t_4\}$ are mutually orthogonal, and are therefore linearly independent. This signifies that $\mathbb{R}^4$ is the minimum dimension for a possible local correlation polytope. Now, to define a three dimensional hyperplane, we require 4 linearly independent vectors. The sets of four linearly independent vectors are given by:

$$U_{\overline{r}} = \{r_1 t_1, r_2 t_2, r_3 t_3, r_4 t_4\}, \tag{C.6}$$

with $\overline{r} = [r_1, r_2, r_3, r_4] \in \{+1,\text{-}1\}^4$. The solution of equation $n_{\overline{r}} \cdot (r_k t_k) = 4$, gives the normal to the hyperplane $U_{\overline{r}}$, which comes out to be equal to $n_{\overline{r}} = \sum_{k=1}^{4} r_k t_k$, since $t_i \cdot t_k = 4\delta_{ij}$. Therefore, each set of $U_{\overline{r}}$ defines a facet of the local polytope $\mathcal{L}$ following:

$$n_{\overline{r}} \cdot m \ = 4, \tag{C.7}$$

where $n_{\overline{r}} = \sum_{k=1}^{4} r_k t_k$. There are 16 facets for the local correlation polytope. Examining these facets, we calculate the constraints for $\mathcal{L}$. These are described as follows.

$$\begin{aligned} n_{[+1,+1,+1,+1]} = (4,0,0,0) \quad &\Longrightarrow \quad 4E_{00} \ \leq \ 4, \\ n_{[+1,+1,+1,-1]} = (2,2,2,-2) \quad &\Longrightarrow \quad 2E_{00} + 2E_{01} + 2E_{10} - 2E_{11} \ \leq \ 4, \\ n_{[+1,+1,-1,+1]} = (2,2,-2,2) \quad &\Longrightarrow \quad 2E_{00} + 2E_{01} - 2E_{10} + 2E_{11} \ \leq \ 4, \\ n_{[+1,-1,+1,+1]} = (2,-2,2,2) \quad &\Longrightarrow \quad 2E_{00} - 2E_{01} + 2E_{10} + 2E_{11} \ \leq \ 4, \\ n_{[+1,+1,-1,-1]} = (0,4,0,0) \quad &\Longrightarrow \quad 4E_{01} \ \leq \ 4, \\ n_{[+1,-1,+1,-1]} = (0,0,4,0) \quad &\Longrightarrow \quad 4E_{10} \ \leq \ 4, \\ n_{[+1,-1,-1,+1]} = (0,0,0,4) \quad &\Longrightarrow \quad 4E_{11} \ \leq \ 4, \\ n_{[-1,+1,+1,+1]} = (-2,2,2,2) \quad &\Longrightarrow \ -2E_{00} + 2E_{01} + 2E_{10} + 2E_{11} \ \leq \ 4, \end{aligned} \tag{C.8}$$

The other 8 constraints would be similar, as $n_{-\bar{r}} = -n_{\bar{r}}$. The constraints $E_{00} \leq 1$, $E_{01} \leq 1$, $E_{10} \leq 1$, and $E_{11} \leq 1$ are trivial, as given by equation (C.3). The other four equations (on relabeling of inputs and/outputs) give the constraint:

$$S \equiv E_{00} + E_{01} + E_{10} - E_{11} \leq 2. \tag{C.9}$$

This constraint is known as the *CHSH inequality* and is the same as given in equation (5.3). It is not trivial, and can be violated by some valid correlation vectors, which do not belong to the local correlation polytope. For example, a vector (+1,+1,+1,−1) is a valid correlation vector, but violates the above inequality up to the value of $S = 4$. This concludes the derivation.

Bibliography

[Acín 02] A. Acín, T. Durt, N. Gisin & J. I. Latorre. *Quantum nonlocality in two three-level systems.* Phys. Rev. A, vol. 65, page 052325, May 2002.

[Acín 06a] Antonio Acín, Nicolas Gisin & Lluis Masanes. *From Bell's Theorem to Secure Quantum Key Distribution.* Physical review letters, vol. 97, page 120405, 10 2006.

[Acín 06b] Antonio Acín, Serge Massar & Stefano Pironio. *Efficient quantum key distribution secure against no-signalling eavesdroppers.* New Journal of Physics, vol. 8, no. 8, page 126–126, Aug 2006.

[Aspect 75] A. Aspect. *Proposed experiment to test separable hidden-variable theories.* Physics Letters A, vol. 54, no. 2, pages 117 – 118, 1975.

[Barrett 05a] Jonathan Barrett, Lucien Hardy & Adrian Kent. *No Signaling and Quantum Key Distribution.* Phys. Rev. Lett., vol. 95, page 010503, Jun 2005.

[Barrett 05b] Jonathan Barrett, Noah Linden, Serge Massar, Stefano Pironio, Sandu Popescu & David Roberts. *Nonlocal correlations as an information-theoretic resource.* Phys. Rev. A, vol. 71, page 022101, Feb 2005.

[Barrett 05c] Jonathan Barrett & Stefano Pironio. *Popescu-Rohrlich Correlations as a Unit of Nonlocality.* Phys. Rev. Lett., vol. 95, page 140401, Sep 2005.

[Barrett 06] Jonathan Barrett, Adrian Kent & Stefano Pironio. *Maximally*

Nonlocal and Monogamous Quantum Correlations. Physical Review Letters, vol. 97, no. 17, Oct 2006.

[Bell 64] J. S. Bell. *On the Einstein Podolsky Rosen paradox.* Physics Physique Fizika, vol. 1, pages 195–200, Nov 1964.

[Bell 04] J. S. Bell & Alain Aspect. Speakable and unspeakable in quantum mechanics: Collected papers on quantum philosophy. Cambridge University Press, 2 edition, 2004.

[Bennett 84] Charles H. Bennett & Gilles Brassard. *Quantum cryptography: Public key distribution and coin tossing.* Theor. Comput. Sci., vol. 560, pages 7–11, 1984.

[Bennett 92] Charles H. Bennett, Gilles Brassard & N. David Mermin. *Quantum cryptography without Bell's theorem.* Phys. Rev. Lett., vol. 68, pages 557–559, Feb 1992.

[Bennett 14] Charles H. Bennett & Gilles Brassard. *Quantum cryptography: Public key distribution and coin tossing.* Theoretical Computer Science, vol. 560, pages 7 – 11, 2014. Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[Brunner 14] Nicolas Brunner, Daniel Cavalcanti, Stefano Pironio, Valerio Scarani & Stephanie Wehner. *Bell nonlocality.* Reviews of Modern Physics, vol. 86, no. 2, page 419–478, Apr 2014.

[Cerf 00a] Nicolas J. Cerf. *Asymmetric quantum cloning in any dimension.* Journal of Modern Optics, vol. 47, no. 2-3, page 187–209, Feb 2000.

[Cerf 00b] Nicolas J. Cerf. *Pauli Cloning of a Quantum Bit.* Phys. Rev. Lett., vol. 84, pages 4497–4500, May 2000.

[Cirel'Son 80] B. S. Cirel'Son. *Quantum generalizations of Bell's inequality.* Letters in Mathematical Physics, vol. 4, no. 2, pages 93–100, March 1980.

[Clauser 69] John F. Clauser, Michael A. Horne, Abner Shimony & Richard A.

Holt. *Proposed Experiment to Test Local Hidden-Variable Theories.* Phys. Rev. Lett., vol. 23, pages 880–884, Oct 1969.

[Clauser 74] John F. Clauser & Michael A. Horne. *Experimental consequences of objective local theories.* Phys. Rev. D, vol. 10, pages 526–535, Jul 1974.

[Collins 02] Daniel Collins, Nicolas Gisin, Noah Linden, Serge Massar & Sandu Popescu. *Bell Inequalities for Arbitrarily High-Dimensional Systems.* Phys. Rev. Lett., vol. 88, page 040404, Jan 2002.

[Cover 06] Thomas M. Cover & Joy A. Thomas. Elements of information theory (wiley series in telecommunications and signal processing). Wiley-Interscience, USA, 2006.

[Csiszar 78] I. Csiszar & J. Korner. *Broadcast channels with confidential messages.* IEEE Transactions on Information Theory, vol. 24, no. 3, pages 339–348, May 1978.

[Devetak 05] Igor Devetak & Andreas Winter. *Distillation of secret key and entanglement from quantum states.* Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences, vol. 461, no. 2053, page 207–235, Jan 2005.

[Durt 01] T. Durt, D. Kaszlikowski & M. Żukowski. *Violations of local realism with quantum systems described by N-dimensional Hilbert spaces up to* $N = 16$. Phys. Rev. A, vol. 64, page 024101, Jul 2001.

[Durt 03] Thomas Durt, Nicolas J. Cerf, Nicolas Gisin & Marek Żukowski. *Security of quantum key distribution with entangled qutrits.* Phys. Rev. A, vol. 67, page 012311, Jan 2003.

[Ekert 91] Artur K. Ekert. *Quantum cryptography based on Bell's theorem.* Phys. Rev. Lett., vol. 67, pages 661–663, Aug 1991.

[Fuchs 97] Christopher A. Fuchs, Nicolas Gisin, Robert B. Griffiths, Chi-Sheng Niu & Asher Peres. *Optimal eavesdropping in quantum*

cryptography. I. Information bound and optimal strategy. Phys. Rev. A, vol. 56, pages 1163–1172, Aug 1997.

[Grimmett 01] G.R. Grimmett & D.R. Stirzaker. Probability and random processes, volume 80. Oxford university press, 2001.

[Hänggi 10] Esther Hänggi. *Device-independent quantum key distribution*, 2010.

[Jones 05] Nick S. Jones & Lluís Masanes. *Interconversion of nonlocal correlations.* Phys. Rev. A, vol. 72, page 052312, Nov 2005.

[Larsson 04] J.-Å Larsson & R. D Gill. *Bell's inequality and the coincidence-time loophole.* Europhysics Letters (EPL), vol. 67, no. 5, page 707–713, Sep 2004.

[Masanes 06] Ll. Masanes, R. Renner, M. Christandl, A. Winter & J. Barrett. *Full security of quantum key distribution from no-signaling constraints*, 2006.

[Mayers 98a] Dominic Mayers & Andrew Yao. *Quantum Cryptography with Imperfect Apparatus*, 1998.

[Mayers 98b] Dominic Mayers & Andrew Yao. *Quantum Cryptography with Imperfect Apparatus.* In Proceedings of the 39th Annual Symposium on Foundations of Computer Science, FOCS '98, page 503, USA, 1998. IEEE Computer Society.

[McKague 09] Matthew McKague. *Device independent quantum key distribution secure against coherent attacks with memoryless measurement devices.* New Journal of Physics, vol. 11, no. 10, page 103037, oct 2009.

[Nielsen 11] Michael A. Nielsen & Isaac L. Chuang. Quantum computation and quantum information: 10th anniversary edition. Cambridge University Press, New York, NY, USA, 10th edition, 2011.

[Pawłowski 11] Marcin Pawłowski & Nicolas Brunner. *Semi-device-independent*

security of one-way quantum key distribution. Physical Review A, vol. 84, no. 1, Jul 2011.

[Pearle 70] Philip M. Pearle. *Hidden-Variable Example Based upon Data Rejection.* Phys. Rev. D, vol. 2, pages 1418–1425, Oct 1970.

[PIRANDOLA 08] STEFANO PIRANDOLA. *SYMMETRIC COLLECTIVE ATTACKS FOR THE EAVESDROPPING OF SYMMETRIC QUANTUM KEY DISTRIBUTION.* International Journal of Quantum Information, vol. 06, no. supp01, page 765–771, Jul 2008.

[Pirandola 19] S. Pirandola, U. L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. S. Shaari, M. Tomamichel, V. C. Usenko, G. Vallone, P. Villoresi & P. Wallden. *Advances in Quantum Cryptography*, 2019.

[Pironio 09] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar & Valerio Scarani. *Device-independent quantum key distribution secure against collective attacks.* New Journal of Physics, vol. 11, no. 4, page 045021, apr 2009.

[Popescu 94] Sandu Popescu & Daniel Rohrlich. *Quantum Nonlocality as an Axiom.* Foundations of Physics, vol. 24, no. 3, pages 379–385, 1994.

[Scarani 13] Valerio Scarani. *The device-independent outlook on quantum physics (lecture notes on the power of Bell's theorem)*, 2013.

[Shannon 01] C. E. Shannon. *A Mathematical Theory of Communication.* SIGMOBILE Mob. Comput. Commun. Rev., vol. 5, no. 1, page 3–55, January 2001.

[Shor 00] Peter W. Shor & John Preskill. *Simple Proof of Security of the BB84 Quantum Key Distribution Protocol.* Physical Review Letters, vol. 85, no. 2, page 441–444, Jul 2000.

Index

Accessible information, 18
accessible information, 18
adversary, 35
ancilla, 23
assumptions, 33, 37
auxiliary, 16, 19

basis reconciliation, 29
Bayes' theorem, 86
Bell inequality, 41
Bell's inequality, 43
Binary entropy, 7
bit errors, 31

check bits, 36
CHSH inequality, 44
cloning based attacks, 65
cloning-based attacks, 70
coherent attacks, 28
coincidence loophole, 79
collective attacks, 29
communication, 5
completeness error, 52
compression, 5
concave, 7
conditional entropy, 9
conditional mutual information, 12
conditional probability, 85
correlations, 41, 78
Cryptography, 1
cryptosystem, 2
CSS, 31

data-processing inequality, 13
density operator, 15
detection loophole, 77
detection windows, 79
deterministic, 43
Devetak-Winter rate, 31
device-independence, 32
Device-independent quantum key distribution, 35

eavesdropper, 1, 23
eavesdropping strategies, 28
Einstein Podolsky Rosen paradox, 41
entanglement, 27
entanglement distillation, 31
Entanglement-based, 25
expectation, 6, 88
extremal, 59

fidelity, 30

Hilbert-Schmidt inner product, 44
Holevo, 31
Holevo bound, 18

individual attack, 28
information, 1
information reconciliation, 24
Information theory, 5

joint entropy, 8
joint probability, 86

key, 24
Kullback–Leibler distance, 8

local realistic theories, 66
locality, 41, 43
locality loophole, 78
LOCC, 31
loophole-free, 80

Markov Chain, 13
mixture, 16
mutual information, 10, 30

no-cloning principle, 23
non-locality, 39, 41
non-repudiation, 1
Non-signalling cryptography, 55
norm, 24

observed statistics, 37

phase errors, 31
polarization, 25
POVM, 18
pre-determined, 39, 45
Prepare and measure, 25
presented, 7
privacy amplification, 24
private key cryptography, 2
probability theory, 85
projective, 17
protocol, 3

QBER, 30
QKD, 23
Quantum Bit Error Rate, 30
quantum cloning machines, 70
quantum cryptography, 2
Quantum key distribution, 23
quantum memory, 31
qutrit, 65

random variable, 6
relative entropy, 8

self-information, 11
self-testing, 49
Shannon, 6
spectral decomposition, 15
Spot-Checking CHSH QKD, 50
spot-checks, 52
symmetric-collective eavesdropping, 29

transmission, 5
Tsirelson, 45

uncertainty, 6

violation, 45
Von Neumann entropy, 15