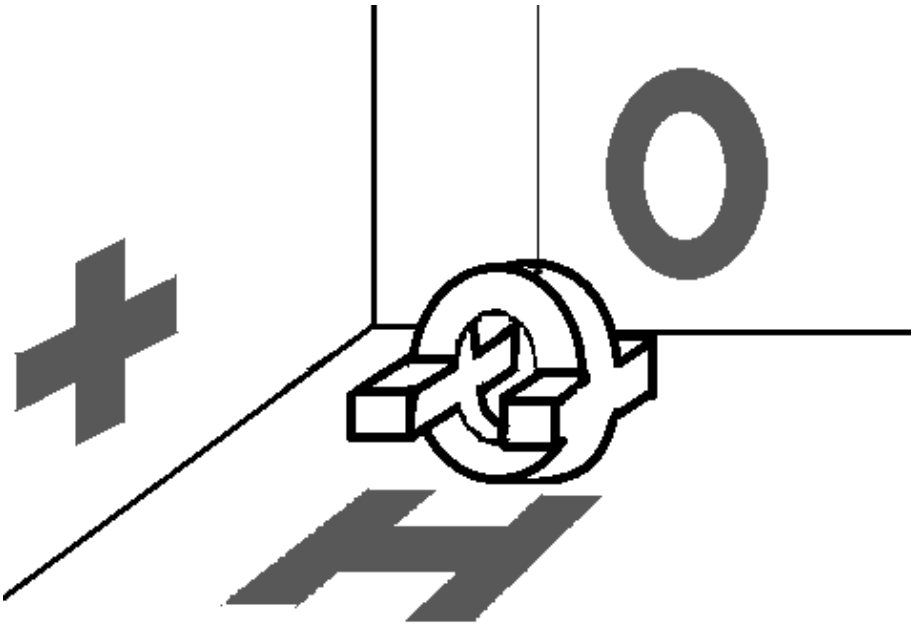
DEVICE INDEPENDENT QUANTUM KEY DISTRIBUTION IN THE FINITE KEY REGIME

KANVI PAREKH

15 August 2018

Delft University of Technology



Device Independent Quantum Key Distribution In The Finite Key Regime

Master Thesis

by

Kanvi Parekh

to obtain the degree of Master of Science
at the Delft University of Technology,
to be defended publicly on 15 August 2018 at 15:00

Student Number:	4617371	
Project Duration:	November 2017 to August 2018	
Thesis Committee:	Prof. dr. Stephanie Wehner	(Promoter)
	Dr.Gláucia Murta Guimarães	(Supervisor)
	Dr. ir. Przemysław Pawełczak	
	Dr. Tim Taminiau	

Sans toi, les émotions d'aujourd'hui ne seraient que la peau morte des émotions d'autrefois.

— Le Fabuleux Destin d'Amélie Poulain

Dedicated to Mum.
Thanks for being the unwavering North star of my world.

"In Africa there is a concept known as ubuntu—the profound sense that we are human only through the humanity of others; that if we are to accomplish anything in this world it will in equal measure be due to the work and achievement of others."

— Nelson Mandela

ACKNOWLEDGEMENTS

To be able to pursue a specialization in the field of quantum computing without leaving my existing background in computer science, was what prompted me to apply for a Master programme at TU Delft. And a project in the branch of quantum cryptography at QuTech has definitely been a great way to conclude this programme. Naturally, my journey till here is a result of the help and support offered by the people who I had the privilege of being associated with along the way. In no specific order of importance, I hereby convey my gratitude.

Many thanks to my teachers, near-and-dear ones, and benefactors from India! Your aide has been an instrumental ***device*** in facilitating a smooth turn of events in my favour. To all the friends I've made over the past couple years, I'd like to express my strong adulation. Learning to become ***independent*** during this span in Delft has surely been replete with "gezelligheid"!

In the past two years, I have been able to develop a clearer foundation of concepts from ***quantum*** mechanics and quantum information theory. This has been possible thanks to the joint effort of all those who collaborate to make QuTech what it is. A special shout out to my peers at Wehner group for some constructive feedback and lots of one-sided assimilation, with me, of course, on the receiving end, trying to grasp concepts.

This section is incomplete without the explicit mention of my supervisors, Prof. Stephanie Wehner and Dr. Gláucia Murta , who have played a ***key*** role throughout the course of this project. Firstly, I am grateful to them for giving me an opportunity to work on this project. I also appreciate their patience to simplify and explain me a lot of concepts. It was not just their timely guidance and feedback, but also their constant encouragement that helped me stay consistently confident.

To "stand on the shoulders of giants" (as Google Scholar would call it), and to participate in the ***distribution*** of new ideas, are what encompass any research work. I'd, finally, like to thank all the readers for investing their time to go through this thesis. And apart from the readers, I'd like to extend my thanks to all the authors, upon whose works I have expounded this project.

CONTENTS

LIST OF FIGURES

ABSTRACT

Relaxing the assumptions about the experimental setup in Quantum Key Distribution protocols lays the foundation for Device Independent Quantum Key Distribution (DIQKD). In the finite key regime of DIQKD, the protocols employ the use of only the CHSH inequality, so far. A natural question therefore arises whether are there other Bell inequalities that help achieve better results (in terms of higher rates, greater noise tolerance and lower number of minimum rounds required for positive rates) than those achieved using CHSH inequality? For the inequalities considered, we find that CHSH fares the best on account of noise tolerance. However, considering the other two parameters of interest we present two bipartite Bell-inequalities with three outcomes per party that perform better than CHSH for a certain range of noise involved.

1 INTRODUCTION

1.1 KEY DISTRIBUTION

Key distribution is an important task in cryptography, as it is quite relevant to the current need of transmitting information over a network in a secure as well as a correct manner. Usually, the main information to be communicated is encrypted using a symmetric key cryptosystem. Symmetric key cryptosystems are effective in performing quick encryption and decryption of large amounts of data. However, these cryptosystems require a common shared-key to be established among the two communicating parties. In order to communicate the common secret key required for this symmetric encryption and decryption to the concerned remote users, the classical public-key cryptography schemes are being used extensively. Also known as asymmetric key cryptography, public-key cryptography involves each party having its private and public key components. The users broadcast their public keys. A sender encrypts a particular message (which is usually the secret key for the symmetric key cryptosystem) using the receiver's public key. The receiver can decrypt this encrypted message using his/her private key. For a detailed survey on public-key cryptography, we redirect readers to a relevant survey [Nec91].

In a symmetric key encryption-decryption scheme, the sender encrypts the message using a secret key and the receiver can decrypt it using the same secret key.

These public-key cryptosystems are computationally secure. On the other hand, Quantum Key Distribution (QKD) protocols are the ones that help achieve the same objective of key distribution, whilst being information-theoretically secure. It is therefore, worth taking a careful look at QKD.

Information -theoretic security implies unconditional security, as long as the laws of physics hold. And therefore, it is more supreme compared to computational security, which is subject to the notion that a scheme is secure till the appropriate computational power (to break it) is not available. Naturally, computational security also requires the laws of physics to hold true.

1.2 QUANTUM KEY DISTRIBUTION (QKD)

In 1984, Bennett and Brassard developed a protocol that laid the foundation for quantum cryptography [Ben84; BB14]. Known as BB84, this QKD protocol involves two parties Alice and Bob that wish to communicate with each other and establish a secret key. The protocol is also robust; in the sense that in case of noise or small disturbance by an eavesdropper Eve, the protocl can still be secure.

Using similar steps as in case of BB84, a new protocol was proposed by Artur Ekert in 1991 [Eke91]. Known as the E91 protocol, unlike BB84, as per this protocol Alice and Bob shared an entangled state to begin with. With their measurement outcomes being correlated, they can broadcast the choice of their bases and the corresponding outcomes for some of the rounds, called the test rounds. This broadcast is exercised after performing the measurements to see if they can

achieve the expected Bell violation using the correlations. If they cannot, then they abort that round and start with a new round again; else they use the remaining data to generate the key.

For the BB84 protocol, a noise tolerance of $\mathrm{QBER} = 11\%$ *is encountered. Generally, the noise tolerance is measured in terms of the Quantum Bit Error Rate (QBER).*

QKD protocols not only help ensure correct and secure transmission of information, but they also provide with constructs to cross-check if information was being intercepted by a third party, Eve, or not. During the transmission of information from one party to another, some noise in the channel can cause error in transmission. One type of error induced can be in the form of bit flips of the classical data being transmitted. Naturally, a suitable error correction scheme is chosen to correct these erroneous transmissions. An important factor pertaining to a QKD scheme is that of noise tolerance, which is often quantified by the Quantum Bit Error rate (QBER). Simply put, QBER quantifies the amount of bit flips taking place at the time of transmission. In addition to all of this, it should also be noted that several assumptions are made in these protocols regarding Alice's and Bob's respective experimental set-up, as well as about Eve's attacking capabilities. Relaxing many of these assumptions lays the foundation for Device Independent Quantum Key Distribution (DIQKD), which is introduced in context with our project in the following section.

1.3 DEVICE INDEPENDENT QUANTUM KEY DISTRIBUTION (DIQKD)

While using a normal QKD scheme, it could be the case that the devices of the two parties - Alice and Bob - are faulty. It could also be the case that an unauthorized distributor has distributed deliberately manipulated device(s) or states among Alice and Bob, so as to be able to gain information during the key generation phase. It, therefore, becomes important to perform analysis by not assuming beforehand the ideal functioning of the devices of the communicating parties. While doing so, we must also consider the possibility of Eve possessing all the computational power available. Performing QKD by setting these thumb rules gives rise to what we call Device Independent Quantum Key Distribution (DIQKD).

It is assumed (even in case of DIQKD) that Alice and Bob each have appropriately functioning local, classical apparatuses, as well as trusted random number generators. It is also assumed that they can communicate over a public, classical authenticated channel. In some of the DIQKD protocols, the settings are assumed to be independent and identically distributed [Pir+09].

DIQKD is the branch of QKD protocols wherein there are no assumptions made regarding the quantum set-up of the parties Alice and Bob. At one point in the analysis of the protocols, it is even assumed that, the eavesdropper, Eve, could prepare and distribute the state shared by Alice and Bob. This in turn gives greater power to Eve. Surely, a lot of other assumptions made in case of QKD are also taken into consideration in case of DIQKD. For a detailed introduction to DIQKD, we refer the readers to section 1 of [Pir+09]. In Figure 1, we represent how DIQKD is a niche class of key distribution protocols.

The BHK05 protocol by Barrett, Hardy and Kent [BHK05] was the earliest DIQKD protocol to be proven secure. Following that, several other variants of secure DIQKD protocols have been put forth [Pir+09;

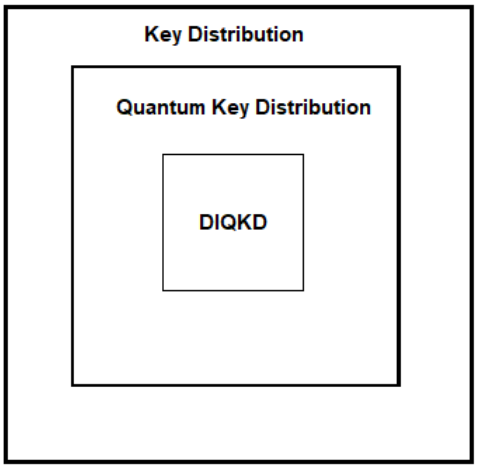


Figure 1: By preferring information-theoretic secutiy over computational security, the class of key distribution protocols is restricted to QKD protocols. Further, relaxing the assumptions pertaining to the settings and shared apparatuses of the communicating parties, the focus is narrowed down from QKD to DIQKD protocols.

Dha+11; MPA11; VV14]. In fact, in [Pir+09], the key rate analysis performed has been shown to have a noise tolerance of 7.1% (not too distant from the noise tolerance of 11%, achieved for BB84 protocol).

All these protocols and their corresponding analyses have been performed in a theoretically-oriented asymptotic key regime. In the asymptotic key regime, one assumes an infinite number of rounds for key generation. A realistic setting should take into account the finite key regime, which involves large, but a finite number of rounds for key generation. Before delving into DIQKD in the finite regime, let us first have a look at DIQKD in the asymptotic key regime.

1.4 DIQKD IN THE ASYMPTOTIC KEY REGIME

Throughout this section and the following one as well, we shall present the entire framework with respect to the famous CHSH inequality [Cla+69]. It is a bipartite two-input two-output inequality. The general form of this inequality is given as:

$$\langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle \leqslant 2. \tag{1}$$

We will denote the expression in the above inequality by I_{CHSH}. Now, the full correlations in I_{CHSH} can be expressed as follows:

$$\begin{aligned}
\langle A_0B_0\rangle &= p(A_0 = B_0) - p(A_0 \neq B_0);\\
\langle A_0B_1\rangle &= p(A_0 = B_1) - p(A_0 \neq B_1);\\
\langle A_1B_0\rangle &= p(A_1 = B_0) - p(A_1 \neq B_0);\\
\langle A_1B_1\rangle &= p(A_1 \neq B_1) - p(A_1 = B_1).
\end{aligned} \tag{2}$$

For a DIQKD protocol based on the CHSH inequality, we consider that Alice has two choices of measurements, represented by observables A_0, A_1 and Bob has three measurement choices, represented by observables B_0, B_1, B_2. With the extra observable, B_2, that Bob has, he can fix that measurement to be such that it helps ensure as high correlation between his and Alice's outcomes as possible.

The overall protocol is composed of a few test rounds followed by the actual key generation rounds. During the test rounds, Alice and Bob make use of the aforementioned observables, namely A_0, A_1, B_0, B_1, to test if they achieve the appropriate violation for the inequality or not. However, during the key generation rounds, they use one specific measurement operator each, A_0 and B_2 respectively. Also, for n total number of rounds, we denote the fraction of test rounds by γ throughout this report. As such, the entire DIQKD protocol based on the CHSH inequality, can be jotted using the following steps:

- Alice and Bob share a bipartite state and they can choose to apply one of the measurements out of their respective set of measurements.
- First, an approach similar to the approach in the QKD protocol of E91 [Eke91] is used to check whether, for the measurements chosen by Alice and Bob, is the chosen Bell inequality violated or not.
- In case of the occurrence of violation, (we shall denote the violation value by g), the post-processing is performed. This post-processing comprises of the error correction phase, parameter estimation phase and the privacy amplification phase.
- The error correction phase involves communication of classical information from Alice to Bob regarding the outcome obtained. The need for high correlation among Alice's and Bob's outcomes during this phase is due to the fact that for higher correlation, lesser and lesser classical information will have to be communicated across and this will ensure that lesser information gets leaked to the adversary Eve.
- The parameter estimation step allows Alice and Bob to determine the QBER and the violation value g. A detailed definition of this step can be found in [AFRV16].
- The final step of privacy amplification is the one wherein a privacy amplification protocol (such as universal hashing) is used to generate the keys of length l on Alice and Bob's respective ends. The length l of the keys generated is lesser in value than the total number of rounds n. These keys that are generated, are almost-ideal. Ideal keys are perfectly random strings that are uncorrelated with Eve's knowledge.

For the different DIQKD protocols, if l is the length of the key generated at the end of privacy amplification step, and n is the number of

rounds in the finite key scenario, then the key rate can be expressed as:

$$\text{rate} = \frac{l}{n}. \tag{3}$$

As such, the key rate is the effective amount of information communicated per round of the protocol between Alice and Bob. In the context of key distribution, the effective information concerns the amount of information pertaining to the key that is to be generated. In the asymptotic key regime, this key rate is given by [Reno8]:

$$\text{rate} \geqslant H(A \mid E) - EC. \tag{4}$$

In the above equation, the conditional entropy $H(A \mid E)$ quantifies Eve's knowledge of Alice's measurement outcomes. As mentioned earlier, we consider that g denotes the value of the CHSH expression (Equation 1). Our goal then, is to express this conditional entropy in terms of the violation g. Now, one guaranteed way of expressing $H(A \mid E)$ as a function of g is by using the following bound:

$$H(A \mid E) \geqslant H_{min}(A \mid E) = -\log_2(p_{guess}). \tag{5}$$

Here, $H_{min}(A \mid E)$ stands for the min-entropy and p_{guess} denotes Eve's guessing probability. A description of min-entropy can be found in chapter 3 of [Reno8].

In the above equation, p_{guess} denotes Eve's guessing probability. As shown in [Dha+11; MPA11], Eve's guessing probability can be expressed as $\max\{p(A_0 = 0)\}$. It is basically, optimized over all the probability distributions that lead to the observed violation. This means that computing p_{guess} can be reduced to the computation of the maximum probability of Alice getting an outcome $a = 0$ or $a = 1$ for a fixed input x. This computation can be performed by solving a Semi-Definite Programming (SDP) problem. SDP problems are analogous to linear programming (LP) problems, in the sense that the linear variables and constants in an LP problem are now replaced by variables and constants in form of matrices. Also, the non-negativity constraint on variables in an LP problem is now replaced by the positive semi-definite constraint on the matrices. This constraint states, that the variable matrices ought to be $\succeq 0$ (i.e. they need to be positive semi-definite). The SDP problem to compute Eve's guessing probability is given as:

A positive semi-definite matrix is the one which has only non-negative eigenvalues.

$$\begin{aligned} &\text{maximize } p(A_0 = 0) \\ &\text{subject to } I_{CHSH} = g; \\ &\text{and } p(A_0 = 0) \text{ and probability distribution in} \\ &I_{CHSH} \text{ satisfy NPAHierarchy constraints.} \end{aligned} \tag{6}$$

This SDP problem can be solved using the NPAHierarchy script of the QETLAB package [Joho3]. The NPA Hierarchy constraints [NPAo8] specify the constraints that should be satisfied by a superset of the set of probabilities generated by quantum mechanical systems. This hierarchy has levels starting from 1. With an increase in the level number, the scope of the superset decreases and the reduced set approaches the truly quantum set of probability distributions. Now, having solved the SDP problem for the CHSH inequality scenario, the

It should be noted that the quantum set of probability distributions cannot be specified by any level of the NPA Hierarchy. However, for higher levels of the hierarchy, the set of probability distributions under consideration is very close to the truly quantum set.

analytic expression for p_{guess}, which has already been derived in [Dha+11; MPA11; Pir+10], is given by:

$$p_{guess} \leqslant \frac{1+\sqrt{2-\frac{g^2}{4}}}{2}. \tag{7}$$

The second term (i.e. EC) in the expression for the bound on the key rate (Equation 4) quantifies the amount of information given away in the form of error correction. For a depolarising noise model, the bipartite state, ρ, shared by Alice and Bob is given by the following Werner state:

$$\rho = v \cdot |\phi^+\rangle\langle\phi^+| + (1-v) \cdot \frac{\mathbb{I}}{4}, \tag{8}$$

Note that, the state $|\phi^+\rangle$ in in the above equation is the maximally entangled two-qubit state $\frac{1}{\sqrt{2}} \cdot (|00\rangle + |11\rangle)$. Well-known as one of the four Bell pair states, this state helps achieve the maximum quantum violation of $2\sqrt{2}$ for the CHSH expression (I_{CHSH} in Equation 1). Also, the variable v in Equation 8 denotes the visibility of this maximally entangled state in its mixture with the maximally mixed state.

Now, the error correction term can be expressed as a function of the visibility v. Assuming that the error correction information is passed from Alice to Bob, the minimum leakage error correction term is equal to:

$$EC = H(A \mid B); \tag{9}$$

This conditional entropy takes into account the probability Alice and Bob getting equal outcomes (i.e. either both get 0s or both get 1s), and the probability that Alice and Bob get opposite outcomes. As mentioned earlier, QBER quantifies the number of bit flips. Therefore, we can state that, $QBER = p(a \neq b)$. Thus, the error correction term (Equation 9) can be further elaborated as:

h in Equation 10 denotes the binary Shannon entropy.

$$\begin{aligned} H(A \mid B) &= -p(a=b) \cdot \log_2 p(a=b) - p(a \neq b) \cdot \log_2 p(a \neq b); \\ &\implies H(A \mid B) = h(QBER). \end{aligned} \tag{10}$$

For the state ρ defined in Equation 8, $QBER = \frac{(1-v)}{2}$. Thus, from Equation 10 we can say that the value of error correction term is given by $h\left(\frac{1-v}{2}\right)$. So now, the bound on the rate defined using the min-entropy can be stated as:

$$\begin{aligned} rate &\geqslant -\log_2\left(\frac{1+\sqrt{2-\frac{g^2}{4}}}{2}\right) - h\left(\frac{1-v}{2}\right); \\ \implies rate &\geqslant 1 - \log_2\left(1+\sqrt{2-\frac{g^2}{4}}\right) - h\left(\frac{1-v}{2}\right). \end{aligned} \tag{11}$$

In [Dha+11; MPA11], the bound described in the above equation is used to study the key rates resulting from the application of the

CHSH inequality in the asymptotic key regime. A noise tolerance (in terms of QBER) that is slightly over 5.2% is encountered. The same computational approach is used to see the implications of the use of the Chained inequality [BC90] with three inputs for DIQKD in the asymptotic regime. It turns out that the protocol based on the CHSH inequality performs slightly better than the Chained inequality, with the Chained inequality achieving a noise tolerance of: QBER $\approx 5\%$.

Now, it must be noted that the min-entropy is not a tight bound on $H(A \mid E)$. When it comes to the CHSH inequality, in [Pir+09], the authors have found the von Neumann entropy to bound $H(A \mid E)$. The resultant expression for the key rate is given by:

$$\text{rate} \geqslant 1 - h\left(\frac{1+\sqrt{(\frac{g}{2})^2 - 1}}{2}\right) - h(\text{QBER}). \tag{12}$$

Recall that, g stands for the quantum violation value; and here, $\text{QBER} = \frac{(1-v)}{2}$ if the state ρ is as defined in Equation 8.

With the use of this tight von Neumann entropy bound to define the key rate, the overall rate value and the noise tolerance (of 7.1%) turns out to be better than the rate and noise tolerance encountered in case of using CHSH inequality with the min-entropy bound (as given by Equation 11). The rate curves in Figure 2 show that in case of CHSH inequality, indeed, the von Neumann entropy leads to considerably higher rates.

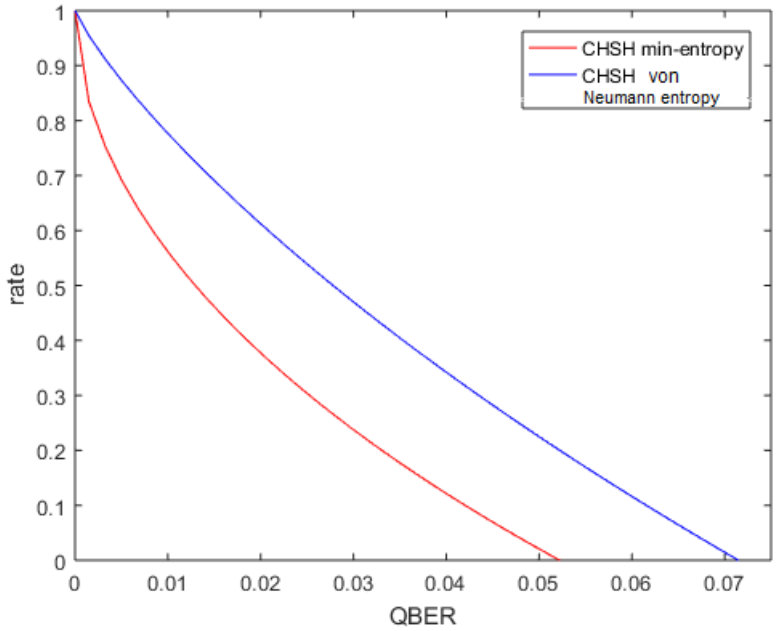


Figure 2: Key rate versus QBER plots for CHSH inequality in the asymptotic regime, with the respective rate curves bounded by min-entropy (Equation 11) and von Neumann entropy (Equation 12).

1.5 DIQKD IN THE FINITE KEY REGIME

Analysis of DIQKD in a robust and truly device independent sense (as established in [AFRV16]) has been possible only recently, by us-

ing the Entropy Accumulation Theorem [DFR16]. All the analyses proposed prior to this analysis makes one important assumption that the bits in the string for the key are independent and identically distributed (i.i.d.). This implies that, the measurements made by Alice and Bob remain the same over all the rounds. It also narrows down Eve's attacks from the general one to collective attacks. Collective attacks involve the same kind of attack being performed by Eve on both, Alice and Bob's respective systems. However, the analysis using the Entropy Accumulation Theorem relaxes even this assumption of independent and identically distributed keys. Using the approach from [AFRV16], the rate in Equation 3 can be expressed as:

$$\mathrm{rate} \geqslant f[\eta] - \mathrm{leak} + \mathcal{O}\left(\frac{1}{\sqrt{n}}\right) - \gamma. \tag{13}$$

Owing to the fact that n would be large, the third term in the above equation (which is of the order of $\frac{1}{\sqrt{n}}$) is not significant enough. The second term (i.e. leak) quantifies the amount of information given away during the error correction phase. If γ denotes the fraction of test rounds out of the total number of rounds n for the finite regime, then leak is a function of the visibility v as well as of γ.

The first term in the bound on the rate curve, as specified in Equation 13, is a function of the entropy term η. In case of use of the min-entropy, η is equal to the min-entropy; and in case of use of von Neumann entropy, η is equal to the von Neumann entropy. Since, for CHSH inequality, a tight bound on the von Neumann entropy $H(A \mid E)$ is known, the focus is only on von Neumann entropy to define η. In this way, the key rate has been defined for the finite regime. This approach has been first introduced and used to define the key rate in the finite regime in [AFRV16]. It is important to note that throughout our work, we will be focusing on the use of the original Entropy Accumulation Theorem as put forth in the main text of [AFRV16]. Later on, the authors have proposed a modified entropy accumulation theorem that reduces the requirement of number of rounds n by an offset value. It is, however, intuitive that the overall rate curves for different parameters in the finite regime will have similar trends when compared with each other, irrespective of whether the modification in the entropy accumulation theorem is taken into account or not.

The minimum number of rounds required for CHSH using min-entropy turn out to be significantly higher than the ones encountered while using CHSH and the von Neumann entropy.

Now, so far, only the use of the CHSH inequality in the finite regime has been considered. Figure 3 shows the rate curves obtained by using CHSH and its associated von Neumann entropy. These curves are for fixed values of QBER, and the proportion of test round (denoted by γ) is also fixed to be 0.5%.

In order to be able to generate key for QBER ranging from 6% up to 7.1%, for the same value of γ (i.e. 7.1%), the minimum number of rounds required will have to be even higher that the ones shown in Figure 3. And even the minimum number of required rounds show-

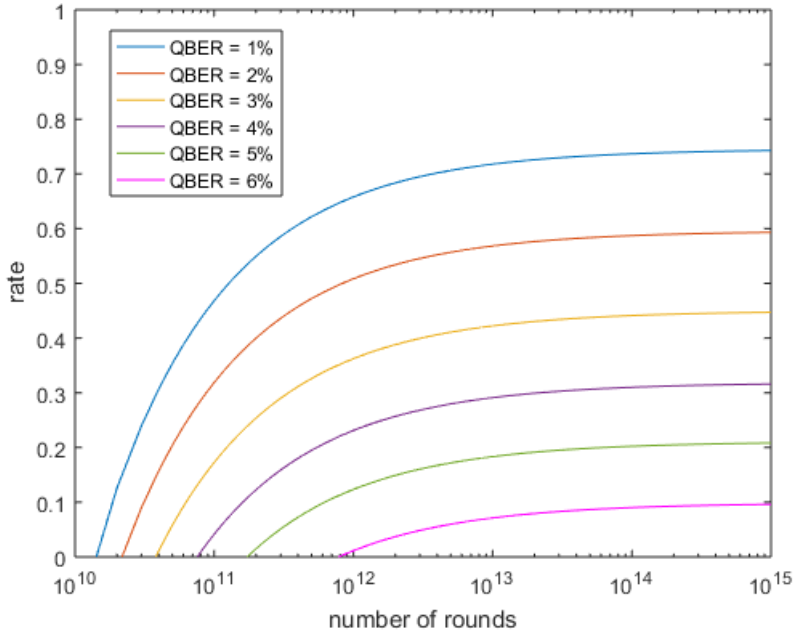


Figure 3: Key rate versus number of rounds for CHSH inequality in the finite regime, with rate curve given by Equation 13. The fraction of test rounds, (γ), is 0.5% and QBER are fixed for the different curves.

cased is too large to be implemented practically. It, therefore, becomes a good motivation to find ways to reduce this requirement of minimum number of rounds, especially for greater values of noise. One way of achieving this could potentially be in lines with one of the open questions discussed in [AFRV16]; namely, of using a Bell inequality other than CHSH inequality and studying the implications arising in the finite regime. In the following section we specify the problem statement for the project and elaborate a bit on a few parameters that need explicit specification.

1.6 PROBLEM STATEMENT AND DESCRIPTION OF PARAMETERS OF INTEREST

Problem statement: The main objective of the project is to employ the use of Bell inequalities other than CHSH inequality in the finite key regime, and consequently, study the implications on the three parameters of interest.

So what are our parameters of interest? While it may already be evident from the previous section; nevertheless, we give a quick description regarding each of those below:

- **Rates achievable:** These correspond to the value of key rates at a particular instance. This means that we are interested in studying the rates achievable at a fixed value of noise, and number of rounds n. It is intuitive that we would want this parameter to be as high as possible.

The perfect case, here, corresponds to the pure entangled, bipartite state that maximally violates a Bell inequality.

- **Noise tolerance:** Here we take noise tolerance to be a function of the visibility (v) of the implementation with respect to the perfect case. This perfect case is characterized by the depolarizing noise model and the bipartite state that maximally violates the Bell inequality under consideration. In case of depolarizing noise model, and Bell inequalities with two-outcomes per party (meaning scenario with the state specified in Equation 8), the noise tolerance is expressed in the form of the Quantum Bit Error Rate (QBER), which is of the form $\frac{(1-v)}{2}$ in such a scenario. For other Bell inequalities, we compare noise tolerance in terms of the least value of visibility (v) that can be tolerated while still being able to generate some key. Naturally, it is desired to have as much noise tolerance as possible (meaning, as low a value of v that can be considered while still producing some positive key rate).

- **Minimum number of rounds required:** This parameter is very important when it comes to realizing and implementing finite key regime protocols practically. As the name suggests, it is the least number of rounds that are required to generate some positive key rates. For a particular scenario, we would want this parameter to have as low a value as possible, especially when the visibility of the state in use is quite low. This is because, low visibility would characterize a scenario with greater, and therefore, more realistic value of noise that is encountered and dealt with in experiments.

To conclude this chapter, we now proceed to give an overview of the organization of the chapters that follow.

1.7 ORGANIZATION OF CHAPTERS

- Chapter 2: This, along with Chapter 3 deals entirely with only the two-outcome Bell inequalities that are maximally violated by the maximally entangled qubit state. All such kinds of inequalities that we apply and study in the framework of DIQKD are first introduced and studied in detail in this chapter. More specifically, the derivations of their quantum bounds are presented.

- Chapter 3:
  - Having laid the base for the inequalities in question, we go on to specify the set-up conditions to ensure an optimal error correction term and lay a foundation to derive generic bound on the von Neumann entropy.
  - It turns out that, the tightness of the bound we derive depends on how high the value of the ratio of the quantum bound to the classical bound of the inequality is. From the inequalities being considered, the highest value for this ratio is $\sqrt{2}$, occurring for CHSH inequality.

  - For some of the remaining inequalities, this bound on the von Neumann entropy does offer some improvement over the respective min-entropy bound for a low noise regime. Consequently, none of the inequalities from among the groups considered, is able to achieve even equal, let alone better results than CHSH in the finite key regime.

- Chapter 4: This chapter explores the use of tilted inequalities, introduced in [AMP12; BP15], to perform DIQKD. These inequalities are maximally entangled by non-maximally entangled states and have been conjectured to lead to DIQKD with almost separable states [AMP12].
  - The main highlight of this chapter is the derivation of the error correction term. The amount of information sent during the error correction phase is high for the tilted inequalities. This results in some sort of an extra penalty to the key rate. Therefore, in the almost-separable state scenario, when the rates are expected to be optimal for tilted inequalities [AMP12], such results are not obtained due to a high penalty from the error correction term.
  - In comparison to the use of CHSH inequality, the use of tilted inequalities does not offer any advantage in terms of better rates, higher noise tolerance or a requirement of lesser number of rounds.

- Chapter 5: In case of standard QKD it is advantageous to upgrade from a two-outcome to a multiple-outcome Bell inequality scenario, in order to obtain better noise tolerance and key rates [SS10]. To see if this holds true for DIQKD as well, or not, we take into account two different Bell inequalities, namely: CGLMP-3, and tailored-CGLMP-3.
  - For near-pure, bipartite, entangled qutrit state, the rates achievable using CGLMP-3 are better than the rates achieved by using CHSH inequality and considering the state to be of the form mentioned in Equation 8 for lower proportion of test rounds. Also, in such low noise scenarios, the rates achieved using the tailored-CGLMP-3 inequality turn out to be better than the rates achieved using CHSH or even CGLMP-3 inequality while considering smaller n.
  - Noise tolerance is a parameter for which these three-outcome inequalities cannot outperform CHSH inequality.
  - Within the bracket of tolerable noise and for lower proportion of test rounds , the minimum number of rounds required by CGLMP-3 inequality are lesser than the minimum number of rounds required by CHSH inequality. For a low noise scenario, the minimum number of rounds required by tailored-CGLMP-3 inequality are the least among all of these inequalities.

  - For relatively higher noise regime, after optimizing over all possible values of the fraction of test rounds γ, CHSH inequality outperforms even these multiple-outcome inequalities on account of all three parameters of interest (i.e. rate, noise tolerance and minimum number of rounds required).

- Chapter 6: Offers a summary of the results and gives a brief overview of an inequality that is an extension of CHSH inequality in a three-inputs, three-outcomes setting, per party. The chapter ends with a couple open questions.

2

INEQUALITIES MAXIMALLY VIOLATED BY MAXIMALLY ENTANGLED STATE

Based on the CHSH inequality [Cla+69], we introduce different families of inequalities in each section. Each of these bipartite inequalities has two outcomes per party. Additionally, these inequalities are full correlation inequalities, meaning that their expressions bear no single marginals of the form $\langle A_x \rangle$ or $\langle B_y \rangle$. In fact, the terms in the expressions of these inequalities are of the form $\langle A_x B_y \rangle$. As we will show, all these inequalities are maximally violated by the maximally entangled state. Next, the maximum quantum bound for each of these families are established and proved. Additionally, relations between the correlators $\langle A_x B_y \rangle$ at the occurrence of quantum bound are put forth. This shall help in determining a set of optimal measurements in the following chapter. The results from this chapter shall help in applying the inequality expressions, thus defined, as information theoretic resources in the asymptotic and finite key regimes of DIQKD.

One important construct that shall be used throughout this chapter is the theory of Semi-Definite Programming (SDP). Indeed, we will use SDP to compute the quantum bound for inequality expressions. This approach has been proposed in [Cir80; Weh06]. As per the approach, the primal problem is defined for the inequality under consideration. Moreover, for every primal problem we can define a dual problem such that the value of the objective function of the dual problem is always greater than or equal to the value of the objective function of the primal problem. Both these problems are solved to see if the corresponding optimal solutions of the primal and dual problem satisfy the strong duality conditions or not. The duality condition, arising from the construction of dual problem, requires all the feasible solutions of the dual problem to be greater than or equal to the quantum bound of the inequality. It also requires all the feasible solutions of the primal problem to be lesser than or equal to the quantum bound. The strong duality condition, on the other hand, implies that the optimal solutions of the primal and dual problems are equal. This optimal value is in fact, the exact quantum bound for the Bell inequality under consideration. Below, in Equation 14 and Equation 15, we mention the primal and dual problems, introduced in [Weh06], to prove the quantum bound on the expression for CHSH inequality, which is a full correlation inequality. It has been shown that the quantum bound of a full correlation inequality can be computed by solving the following problems:

In order to compute the precise value of the quantum bound, it is necessary for the strong duality condition to hold.

Primal SDP problem:	Dual SDP problem:
$$\begin{aligned} &\text{maximize } \frac{1}{2}\cdot \mathrm{Tr}[(GW)] \\ &\text{subject to } G \succeq 0;\ \&\ G_{ii} = 1\ \forall\ i. \end{aligned} \tag{14}$$	$$\begin{aligned} &\text{minimize } \mathrm{Tr}[\mathrm{diag}(\lambda)] \\ &\text{subject to } -\frac{1}{2}\cdot W + \mathrm{diag}(\lambda) \succeq 0. \end{aligned} \tag{15}$$

The matrix W corresponding to CHSH inequality is given by:

$$W = \begin{pmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \\ 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \end{pmatrix}. \tag{16}$$

Recall from Equation 1 that the expression for the CHSH inequality is: $\langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle$.

It is important to note how the non-zero elements of the matrix W correspond to the coefficients of the correlators in the expression of the CHSH inequality.

The variable in the primal problem is the 4×4 positive semi-definite matrix G; and for the dual problem, the variable is the vector λ with four components. Naturally, $\mathrm{diag}(\lambda)$ implies a diagonal matrix with the elements of the vector λ along the diagonal. Now, consider matrix G to comprise of scalar products of four real, unit vectors x_1, x_2, y_1 and y_2. More specifically, let G be:

$$G = \begin{pmatrix} x_1\cdot x_1 & x_2\cdot x_1 & y_1\cdot x_1 & y_2\cdot x_1 \\ x_1\cdot x_2 & x_2\cdot x_2 & y_1\cdot x_2 & y_2\cdot x_2 \\ x_1\cdot y_1 & x_2\cdot y_1 & y_1\cdot y_1 & y_2\cdot y_1 \\ x_1\cdot y_2 & x_2\cdot y_2 & y_1\cdot y_2 & y_2\cdot y_2 \end{pmatrix}. \tag{17}$$

Now, Tsirelson's theorem states that the full correlations in a Bell inequality can be expressed in the form of scalar products of real valued unit vectors [Cir80; Weho6]. The full correlations from the CHSH inequality map to the following scalar products from the matrix G:

$$\begin{aligned} &\langle A_0B_0\rangle = x_1\cdot y_1;\ \langle A_0B_1\rangle = x_1\cdot y_2; \\ &\langle A_1B_0\rangle = x_2\cdot y_1;\ \langle A_1B_1\rangle = x_2\cdot y_2. \end{aligned} \tag{18}$$

Then, it is intuitive that with the suitably picked elements in matrix W, the objective function of the primal problem indeed maps to the expression for the CHSH inequality.

On solving the primal and dual problems in Equation 14 and Equation 15, it can be seen that the conditions of duality as well as strong duality are satisfied. The common optimal value is equal to $2\sqrt{2}$, which is indeed the quantum bound of CHSH inequality. At this point, the value of the variables G and λ are as follows:

$$G = \begin{pmatrix} 1 & 0 & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 1 & \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & 1 & 0 \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & 0 & 1 \end{pmatrix};\quad \lambda = \frac{1}{\sqrt{2}}\cdot(1,1,1,1). \tag{19}$$

As an additional remark, it can be noted that when the strong duality condition is met, the following relation holds true:

$$\lambda_i = \frac{1}{2} \cdot \sum_{j=1}^{4} G_{ij}\, W_{ji} \quad \forall\, i = 1 \text{ to } 4. \tag{20}$$

For the Bell inequalities that we will be considering in this chapter, we use the same approach of formulating and solving the SDP problems to compute the quantum bounds of their expressions.

Table 1 gives an overview of results from this chapter. The derivation of expressions for maximum quantum violation and the choice of domain for the parameters for a particular family of inequality expressions can be found in the respective section.

Table 1: Overview of results from Chapter 2

Section	Family of expressions	Quantum Bound	Domain of parameters
Section 2.1	$\alpha - \text{CHSH}$	$\sqrt{\frac{(\alpha+1)^3}{\alpha}}$	$\alpha \geqslant \frac{1}{3}$
Section 2.2	$\alpha\beta - \text{CHSH}$	$(\alpha+\beta)\cdot\sqrt{\frac{(1+\alpha\beta)}{\alpha\beta}}$	$\alpha > 0,\ \beta > 0, \frac{\lvert\alpha-\beta\rvert}{\alpha\beta} \leqslant 2$
Section 2.3	$\alpha - \text{MagicSquare}$	$(\alpha+5)$	$\alpha \geqslant 0$
Section 2.4	$\alpha^2 - \text{MagicSquare}$	$2\cdot(\alpha+2)$	$\alpha \geqslant \frac{1}{3}$
Section 2.5	$\alpha^3 - \text{MagicSquare}$	$3\cdot(\alpha+1)$	$\alpha \geqslant \frac{1}{2}$

2.1 α – CHSH INEQUALITIES

The main aim of this section is to prove the following claim:

Claim: For $\alpha \geqslant \frac{1}{3}$, the maximum value achievable by expressions of the α – CHSH inequalities, using quantum correlations, is given by,

$$S_\alpha = \sqrt{\frac{(\alpha+1)^3}{\alpha}}. \tag{21}$$

Note: Substituting $\alpha = 1$ in Equation 22 gives rise to the expression for CHSH inequality (as seen in Equation 1).

For $\alpha \leqslant 0$, the resultant expression leads to a trivial scenario, meaning that a classical strategy will be able to achieve the maximum possible value. In other words, it will be an inequality with no quantum violation.

2.1.1 *Definition of inequality*

In this subsection, we introduce a family of inequalities that we term α – CHSH. The inequalities belonging to this group are of the form:

$$I_\alpha = \alpha\cdot\langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_0\rangle - \langle A_1B_1\rangle \leqslant |1-\alpha| + 2. \tag{22}$$

The expression for the inequality in Equation 22 resembles the expression for CHSH inequality, the only difference being the coefficient for the correlator $\langle A_0B_0\rangle$. In order to restrict the analyses to only non-trivial scenarios for the expression in Equation 22, for now, we enforce that $\alpha > 0$. By non-trivial scenarios we mean scenarios wherein quantum violations are encountered. We shall see later in subsection

Section 2.1.2, the minimum value of α, for which the inequality is not trivial, is strictly larger than 0.

As already seen in case of CHSH inequality in Equation 18, we once again introduce four real unit vectors x_1, x_2, y_1 and y_2 such that we can establish a relation between the full correlations of the α–CHSH inequality and scalar products of these unit vectors. As per this relation, the correlators can be expressed in form of the following scalar products:

$$\begin{aligned} \langle A_0 B_0 \rangle &= x_1 \cdot y_1; \ \langle A_0 B_1 \rangle = x_1 \cdot y_2; \\ \langle A_1 B_0 \rangle &= x_2 \cdot y_1; \ \langle A_1 B_1 \rangle = x_2 \cdot y_2. \end{aligned} \tag{23}$$

We will require the above equation in determining the bound on α and computing values of the correlators when the quantum upper bound is reached by the inequality expression. In the following subsection, we derive the quantum bound of the $\alpha - \text{CHSH}$ expression. This quantum bound is the maximum value for the $\alpha - \text{CHSH}$ expression that can be attained by quantum correlations.

2.1.2 *Derivation of quantum bound*

The optimal solutions of the primal and dual problems specified in [Weh06] can be used to find the desired expression for the quantum bound of an $\alpha - \text{CHSH}$ inequality. The dual problem, which is a Semi-Definite Programming (SDP) problem is given by:

$$\begin{aligned} &\text{minimize} \ \ \text{Tr}(\text{diag}(\lambda)) \\ \text{subject to} \ \ &-\frac{1}{2} W + \text{diag}(\lambda) \succeq 0. \end{aligned} \tag{24}$$

Here, $\text{diag}(\lambda)$ is a diagonal matrix with the elements of the vector $\lambda = (\lambda_1, \lambda_2, \lambda_3, \lambda_4)$ along the diagonal. For the scenario of $\alpha - \text{CHSH}$ inequalities, we take the matrix W to be:

The top-right and bottom-left 2×2 submatrices of the matrix W make up the coefficients of the correlators on $\alpha - \text{CHSH}$ inequality.

$$W = \begin{pmatrix} 0 & 0 & \alpha & 1 \\ 0 & 0 & 1 & -1 \\ \alpha & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \end{pmatrix}. \tag{25}$$

The optimal value for the dual problem is attained when at least one of the non-negative eigenvalues of $-\frac{1}{2} W + \text{diag}(W)$ is 0. This condition is satisfied by making the following choices for the elements of λ:

$$\begin{aligned} \lambda_1 = \lambda_3 &= \alpha \cdot \sqrt{\frac{(\alpha+1)}{4\alpha}}; \\ \lambda_2 = \lambda_4 &= \sqrt{\frac{(\alpha+1)}{4\alpha}}. \end{aligned} \tag{26}$$

Since the quantum bound for $\alpha - \text{CHSH}$ inequality is, $S_\alpha = \text{Tr}(\text{diag}(\lambda))$, and from Equation 26 we have that:

$$S_\alpha \leqslant \sum_{i=1}^{4} \lambda_i = \sqrt{\frac{(\alpha+1)^3}{\alpha}}. \tag{27}$$

Now, we make use of the primal problem mentioned in [Weho6], which is given by:

$$\begin{aligned} &\text{maximize} \ \ \frac{1}{2}\cdot \mathrm{Tr}(GW) \\ \text{s.t.} \ \ &G \succeq 0; \ \ \text{and} \ \ G_{ii} = 1 \ \ \forall\, i. \end{aligned} \tag{28}$$

Here, W is taken same as in Equation 25 and G is the Gram matrix given by:

Unit vectors x_1, x_2, y_1 and y_2 have been defined in Section 2.1.1.

$$G = \begin{pmatrix} x_1\cdot x_1 & x_2\cdot x_1 & y_1\cdot x_1 & y_2\cdot x_1 \\ x_1\cdot x_2 & x_2\cdot x_2 & y_1\cdot x_2 & y_2\cdot x_2 \\ x_1\cdot y_1 & x_2\cdot y_1 & y_1\cdot y_1 & y_2\cdot y_1 \\ x_1\cdot y_2 & x_2\cdot y_2 & y_1\cdot y_2 & y_2\cdot y_2 \end{pmatrix}. \tag{29}$$

Due to the definition of the vectors x_1, x_2, y_1 and y_2, the diagonal elements of G are all equal to 1. Furthermore, if we set:

$$\begin{aligned} x_1\cdot y_2 = x_2\cdot y_1 = -x_2\cdot y_2 &= \sqrt{\frac{(\alpha+1)}{4\alpha}}; \\ x_1\cdot y_1 = 3\Big(\sqrt{\frac{(\alpha+1)}{4\alpha}}\Big) - 4\Big(\sqrt{\frac{(\alpha+1)}{4\alpha}}\Big)^3 &; \\ x_1\cdot x_2 = y_1\cdot y_2 &= \frac{(\alpha-1)}{2\alpha}, \end{aligned} \tag{30}$$

then the matrix G is a Gram matrix that not only satisfies the constraints of the primal problem but for the values defined in Equation 30, the objective function of the primal problem even results in the optimal solution that satisfies the following relation:

$$S_\alpha \geqslant \frac{1}{2}\cdot \mathrm{Tr}(GW) = \sqrt{\frac{(\alpha+1)^3}{\alpha}}. \tag{31}$$

Clearly, the feasible points leading to optimal primal and dual solutions, satisfy both - the duality and the strong duality conditions. The optimal solutions for the primal and dual problems are equal (as can be seen from Equation 27 and Equation 31). Thus, the quantum bound for the expression of α−CHSH inequalities is $S_\alpha = \sqrt{\frac{(\alpha+1)^3}{\alpha}}$.

Also, the relation between the variables λ, G and the constant matrix W at optimality satisfy the relation defined in Equation 20.

Now, the value of the correlators in the inequality expression ranges from −1 to 1. Consequently, the values of the scalar products $x_1\cdot y_1$, $x_1\cdot y_2$, $x_2\cdot y_1$ and $x_2\cdot y_2$ (as defined in Equation 23) must also range from −1 to 1. Taking this into consideration and from Equation 30, and the assumption that $\alpha > 0$, we have that:

Fixing the range of $[-1, 1]$ for just $x_1\cdot y_1$ automatically ensures, that all other scalar products follow this rule.

$$\begin{aligned} &\sqrt{\frac{(\alpha+1)}{4\alpha}} \leqslant 1. \\ &\implies \alpha \geqslant \frac{1}{3}. \end{aligned} \tag{32}$$

Thus, for the constraint on α, specified by the above equation, the maximum value achievable by the expression of α−CHSH inequality using quantum correlations is $S_\alpha = \sqrt{\frac{(\alpha+1)^3}{\alpha}}$.

Furthermore, the relation between the correlators $\langle A_x B_y \rangle$ at the quantum bound is given by the relation between the scalar products in Equation 30. Recall Equation 23, which gives the relations between the correlators and the scalar products. In Section 3.2.2 we will describe an optimum quantum strategy in terms of the operators, namely, A_0, A_1, B_0, B_1.

Interestingly, for $0 < \alpha < \frac{1}{3}$, the classical value and the quantum value of an $\alpha - \text{CHSH}$ inequality expression are equal, and so no quantum advantage is witnessed in that case.

2.2 $\alpha\beta - \text{CHSH}$ INEQUALITIES

Let us now move on to the next group of inequalities and prove the following claim:

Claim: For $\alpha > 0$, $\beta > 0$ and $\frac{|\alpha-\beta|}{\alpha\beta} \leqslant 2$, the maximum value achievable by expressions of the $\alpha\beta - \text{CHSH}$ inequalities, using quantum correlations is given by,

$$S_{\alpha\beta} = (\alpha + \beta) \cdot \sqrt{\frac{(1 + \alpha\beta)}{\alpha\beta}}. \tag{33}$$

2.2.1 *Definition of inequality*

Note: Substituting $\alpha = \beta = 1$ in Equation 34 gives rise to the expression for CHSH inequality. Substituting $\beta = 1$ in Equation 34 gives rise to the expression for $\alpha - \text{CHSH}$ inequality, given by Equation 22.

In this subsection, we introduce a family of inequalities that we term $\alpha\beta - \text{CHSH}$. The inequalities belonging to this group are of the form:

$$I_{\alpha\beta} = \alpha \cdot \langle A_0 B_0 \rangle + \beta \cdot \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle \leqslant |\alpha - \beta| + 2. \tag{34}$$

Expression $I_{\alpha\beta}$ resembles the expression for CHSH inequality (i.e. I_{CHSH} in Equation 1), the only difference being the coefficients for the correlators $\langle A_0 B_0 \rangle$ and $\langle A_0 B_1 \rangle$. As we did for α–CHSH inequalities, in order to consider only the non-trivial possibilities of the inequality group in Equation 34, for now, we enforce that $\alpha > 0$ and $\beta > 0$. It should be noted that if $\alpha < 0$ and $\beta < 0$, then the resultant scenarios are non-trivial as well. But by virtue of similarity among the positive and negative valued α and β, we will focus only on the case where $\alpha > 0$ and $\beta > 0$. We shall see later in Section 2.2.2, an additional condition that must be satisfied by the parameters α and β to ensure some quantum advantage.

We will continue using the same definition for x_1, x_2, y_1 and y_2 as in Section 2.1.1. In the following subsection, we derive the expression for the maximum value achievable by expressions of $\alpha\beta - \text{CHSH}$ inequalities, using quantum correlations.

2.2.2 *Derivation of quantum bound*

The proof for quantum bound of αβ − CHSH inequalities follows the same steps as the proof for the maximal quantum bound of α − CHSH inequalities (see Section 2.1.2). The key difference here, however, is in the matrix W to solve the dual problem given by Equation 25. For the scenario of αβ − CHSH inequalities, we take the matrix W to be:

$$W = \begin{pmatrix} 0 & 0 & \alpha & \beta \\ 0 & 0 & 1 & -1 \\ \alpha & 1 & 0 & 0 \\ \beta & -1 & 0 & 0 \end{pmatrix}. \tag{35}$$

Then, the optimal value of the dual problem is attained when:

$$\begin{aligned} \lambda_1 &= \frac{(\alpha+\beta)}{2}\sqrt{\frac{\alpha\beta}{(1+\alpha\beta)}}; \\ \lambda_2 &= \frac{(\alpha+\beta)}{2}\sqrt{\frac{1}{\alpha\beta(1+\alpha\beta)}}; \\ \lambda_3 &= \frac{1}{2}\sqrt{\frac{\alpha(1+\alpha\beta)}{\beta}}; \\ \lambda_4 &= \frac{1}{2}\sqrt{\frac{\beta(1+\alpha\beta)}{\alpha}}. \end{aligned} \tag{36}$$

For these values of elements of the vector λ, $S_{\alpha\beta} \leqslant \mathrm{Tr}(\mathtt{diag}(\lambda))$. And consequently, we have that:

$$S_{\alpha\beta} \leqslant \sum_{i=1}^{4} \lambda_i = (\alpha+\beta)\sqrt{\frac{(1+\alpha\beta)}{\alpha\beta}}. \tag{37}$$

Next, we make use of the primal problem given by Equation 28. The specifications for the matrices G and W are given by Equation 29 and Equation 35, respectively. Then for the optimal solution of the primal problem, the following relations hold:

$$\begin{aligned} x_2 \cdot y_1 &= \frac{\sqrt{(1-x_1\cdot y_1)(1+x_1\cdot y_2)}+\sqrt{(1+x_1\cdot y_1)(1-x_1\cdot y_2)}}{2}; \\ \alpha^2 - \alpha^2\cdot(x_1\cdot y_1)^2 &= \beta^2 - \beta^2\cdot(x_1\cdot y_2)^2; \\ \implies x_2\cdot y_1 = -x_2\cdot y_2 &= \frac{(\alpha+\beta)}{2}\sqrt{\frac{1}{\alpha\beta(1+\alpha\beta)}}; \\ \implies x_1\cdot y_1 = \frac{(\alpha-\beta+2\alpha^2\beta)}{2\alpha\sqrt{\alpha\beta(1+\alpha\beta)}};&\quad x_1\cdot y_2 = \frac{(\beta-\alpha+2\alpha\beta^2)}{2\beta\sqrt{\alpha\beta(1+\alpha\beta)}}; \\ x_1\cdot x_2 = (x_1\cdot y_1)(x_2\cdot y_1) - \sqrt{(1-(x_1\cdot y_1)^2)(1-(x_2\cdot y_1)^2)}&; \\ y_1\cdot y_2 = (x_1\cdot y_1)(x_1\cdot y_2) - \sqrt{(1-(x_1\cdot y_1)^2)(1-(x_1\cdot y_2)^2)}&. \end{aligned} \tag{38}$$

Substituting β = 1 in Equation 37 leads to the expression derived in Equation 27. Substituting α = β in Equation 37 leads to the expression mentioned for a maximally entangled state in Equation 11 of [AMP12]. Same kind of expression has also been derived in [NSPS14].

Recall from Equation 23 how the scalar products (of the form $x_i \cdot y_j$) in the equations alongside map to the correlators of the form $\langle A_x B_y \rangle$ in the expression for the αβ−CHSH inequality.

The optimal solution for the primal problem with the above mentioned values of scalar products sets the following bound:

$$S_{\alpha\beta} \geqslant \frac{1}{2} \cdot \mathrm{Tr}(GW) = (\alpha+\beta)\sqrt{\frac{(1+\alpha\beta)}{\alpha\beta}}. \tag{39}$$

The feasible points of the primal and dual problems dictate that $S_{\alpha\beta} \geqslant (\alpha+\beta)\sqrt{\frac{(1+\alpha\beta)}{\alpha\beta}}$ and $S_{\alpha\beta} \leqslant (\alpha+\beta)\sqrt{\frac{(1+\alpha\beta)}{\alpha\beta}}$, respectively. Thus, the duality and strong duality conditions are satisfied and the quantum bound of $\alpha\beta-$CHSH inequalities is: $S_{\alpha\beta} = (\alpha+\beta)\sqrt{\frac{(1+\alpha\beta)}{\alpha\beta}}$.

As in the case of $\alpha-$CHSH inequalities, the relation specified by Equation 20 holds even for the $\alpha\beta-$CHSH inequalities. Finally, we need to ensure that the scalar products defined for the optimal scenario are within the permissible limits. Accordingly, from Equation 38, we have that:

Ensuring that $x_2 \cdot y1 \leqslant 1$ automatically helps ensure that the same constraint is imposed on the other scalar products.

$$\begin{aligned} \frac{(\alpha+\beta)}{2}\sqrt{\frac{1}{\alpha\beta(1+\alpha\beta)}} &\leqslant 1; \\ \implies \frac{|\alpha-\beta|}{\alpha\beta} &\leqslant 2. \end{aligned} \tag{40}$$

Just like the $\alpha-$CHSH inequalities, the classical value is equal to the quantum value for combinations of α and β outside the set domain.

Thus, for $\alpha > 0$, $\beta > 0$ and $\frac{|\alpha-\beta|}{\alpha\beta} \leqslant 2$, the maximum value achievable by expressions of the $\alpha\beta-$CHSH inequalities is $S_{\alpha\beta} = (\alpha+\beta)\cdot\sqrt{\frac{(1+\alpha\beta)}{\alpha\beta}}$. The relation between correlators $\langle A_x B_y\rangle$ at optimality are given by Equation 38. Tracing back the relation between the scalar products and the correlators $\langle A_x B_y\rangle$ from Equation 23, we get a relation between these correlators for the optimum quantum strategy.

This concludes the requisite description for bipartite inequalities with two inputs per party. Following sections of this chapter provide similar description for bipartite inequalities with three possible measurements for each party.

2.3 $\alpha-$MagicSquare INEQUALITIES

In this section, let us first introduce the MagicSquare inequality and define the generic expression for the family of Bell inequality expressions that we name $\alpha-$MagicSquare. Our main claim pertaining to this class of inequalities is as follows:

Claim: For $\alpha \geqslant 0$, the optimum quantum value of an $\alpha-$MagicSquare expression is:

$$S'_\alpha = (\alpha+5). \tag{41}$$

Just like the earlier subsections in this chapter, let us resort to the dual and primal problems at our disposal to prove the above mentioned claim.

2.3.1 *Definition of inequality*

Consider the following Bell inequality:

$$\begin{aligned}\langle A_0B_0\rangle - \langle A_0B_1\rangle + \langle A_0B_2\rangle - \langle A_1B_0\rangle + \langle A_1B_1\rangle \\ + \langle A_1B_2\rangle + \langle A_2B_0\rangle + \langle A_2B_1\rangle - \langle A_2B_2\rangle \leqslant 5.\end{aligned} \tag{42}$$

Additionally, let us consider a 3×3 matrix whose element in a cell (i, j) is equal to the coefficient of the correlator $\langle A_iB_j\rangle$. Then for the aforementioned inequality, the sum of each row and column of this matrix turns out to be equal to 0. Such a matrix is very similar to a magic square from recreational mathematics. A magic square is a square grid that comprises of distinct positive integers such that the sum of each row, column and diagonal is equal to a constant (magic) value [Sch94]. We will hereafter call this inequality as the MagicSquare inequality.

Putting $\alpha = 1$ in Equation 43 results in the expression for the MagicSquare inequality. This expression with a classical bound of 5, a quantum bound of 6 and a no-signallinig bound of 9, has an interesting symmetry. For instance, swapping the coefficients of $\langle A_0B_1\rangle$ and $\langle A_1B_0\rangle$ with $\langle A_0B_2\rangle$ and $\langle A_2B_0\rangle$ (or $\langle A_1B_2\rangle$ and $\langle A_2B_1\rangle$) results in the same bounds.

Now, let the expression for a Bell inequality be given by:

$$\begin{aligned}I'_\alpha = \langle A_0B_0\rangle - \alpha\cdot\langle A_0B_1\rangle + \langle A_0B_2\rangle - \langle A_1B_0\rangle + \\ \langle A_1B_1\rangle + \langle A_1B_2\rangle + \langle A_2B_0\rangle + \langle A_2B_1\rangle - \langle A_2B_2\rangle \leqslant \alpha + 4.\end{aligned} \tag{43}$$

We attribute the inequality whose expression is given by I'_α as an $\alpha -$ MagicSquare inequality; and at $\alpha = 1$, we attribute the inequality as simply the MagicSquare inequality. Now, since we would like to consider only the non-trivial possibilities, we set α to be positive. Note that, the inequalities introduced here are not equivalent to the Peres-Mermin inequality [Mer90; Per90].

Now, using Tsirelson's theorem, the expectation values of the correlations are equivalent to the following scalar products of the unit vectors x_1, x_2, x_3, y_1, y_2 or y_3:

$$\begin{aligned}&\langle A_0B_0\rangle = x_1\cdot y_1;\ \ \langle A_0B_1\rangle = x_1\cdot y_2;\ \ \langle A_0B_2\rangle = x_1\cdot y_3;\\ &\langle A_1B_0\rangle = x_2\cdot y_1;\ \ \langle A_1B_1\rangle = x_2\cdot y_2;\ \ \langle A_1B_2\rangle = x_2\cdot y_3;\\ &\langle A_2B_0\rangle = x_3\cdot y_1;\ \ \langle A_2B_1\rangle = x_3\cdot y_2;\ \ \langle A_2B_2\rangle = x_3\cdot y_3.\end{aligned} \tag{44}$$

Let us now derive the expression for the quantum bound.

2.3.2 *Derivation of quantum bound*

For the derivation, consider the dual problem in Equation 24. Now, for $\alpha -$ MagicSquare inequalities, λ is a vector with six elements and the matrix W is chosen as:

$$W = \begin{pmatrix} 0 & 0 & 0 & 1 & -\alpha & 1 \\ 0 & 0 & 0 & -1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & -1 \\ 1 & -1 & 1 & 0 & 0 & 0 \\ -\alpha & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & -1 & 0 & 0 & 0 \end{pmatrix}. \tag{45}$$

Now, if we take:

$$\begin{aligned} \lambda_1 = \lambda_5 &= \frac{(\alpha+1)}{2}; \\ \lambda_2 = \lambda_3 = \lambda_4 &= \lambda_6 = 1, \end{aligned} \tag{46}$$

then, not only is the matrix $-\frac{1}{2}W + \mathrm{diag}(\lambda)$ (in the constraint) positive semi-definite, but even the objective function of the dual problem attains the minimum value. This choice of feasible points gives rise to the following bound on the quantum bound S'_α:

$$S'_\alpha \leqslant \sum_{i=1}^{6} \lambda_i = (\alpha+5). \tag{47}$$

Now let us consider the primal problem specified by Equation 28. The value for matrix W is given in Equation 45 and Gram matrix G is given by:

$$G = \begin{pmatrix} x_1\cdot x_1 & x_2\cdot x_1 & x_3\cdot x_1 & y_1\cdot x_1 & y_2\cdot x_1 & y_3\cdot x_1 \\ x_1\cdot x_2 & x_2\cdot x_2 & x_3\cdot x_2 & y_1\cdot x_2 & y_2\cdot x_2 & y_3\cdot x_2 \\ x_1\cdot x_3 & x_2\cdot x_3 & x_3\cdot x_3 & y_1\cdot x_3 & y_2\cdot x_3 & y_3\cdot x_3 \\ x_1\cdot y_1 & x_2\cdot y_1 & x_3\cdot y_1 & y_1\cdot y_1 & y_2\cdot y_1 & y_3\cdot y_1 \\ x_1\cdot y_2 & x_2\cdot y_2 & x_3\cdot y_2 & y_1\cdot y_2 & y_2\cdot y_2 & y_3\cdot y_2 \\ x_1\cdot y_3 & x_2\cdot y_3 & x_3\cdot y_3 & y_1\cdot y_3 & y_2\cdot y_3 & y_3\cdot y_3 \end{pmatrix}. \tag{48}$$

Unit vectors $x_1, x_2, x_3, y_1, y_2, y_3$ have been defined in Section 2.3.1.

Then the values for the scalar products in matrix G that guarantee that $G \succeq 0$ and that the objective function of the primal problem attains the maximum value, are given below:

$$\begin{aligned} x_1\cdot y_2 = x_2\cdot y_1 = x_3\cdot y_3 &= -1; \\ x_1\cdot y_1 = x_1\cdot y_3 = x_2\cdot y_2 = x_2\cdot y_3 = x_3\cdot y_1 = x_3\cdot y_2 &= \frac{1}{2}; \\ x_1\cdot x_2 = x_1\cdot x_3 = x_2\cdot x_3 = y_1\cdot y_2 = y_1\cdot y_3 = y_2\cdot y_3 &= -\frac{1}{2}. \end{aligned} \tag{49}$$

Consequently, using the feasible solutions of the primal problem, we can say that:

$$S'_\alpha \geqslant \frac{1}{2}\mathrm{Tr}(GW) = (\alpha+5). \tag{50}$$

Since using the primal problem, $S'_\alpha \geqslant (\alpha+5)$ and using the dual problem, $S'_\alpha \leqslant (\alpha+5)$, we can say that indeed, $S'_\alpha = (\alpha+5)$. This common optimal solution, therefore, gives the expression for the quantum bound for α–MagicSquare expressions.

Interestingly, the expression $S'_\alpha = (\alpha+5)$ also gives the quantum upper bound for the expression of $\alpha - \mathrm{MagicSquare}$ inequality at $\alpha = 0$. Thus, the claim made at the beginning of this section holds true.

Since, all the scalar product values in Equation 49 are within the permissible limits of -1 to 1, there is no additional constraint that needs

to be enforced on the parameter α. Combining Equation 44 and Equation 49, we get the relation that must hold true among the correlators $\langle A_x B_y \rangle$ when the quantum bound is attained. In addition to this, it is important to note that at optimality, the following relation between the parameters λ and G and matrix W of SDP problems holds true:

$$\lambda_i = \frac{1}{2} \cdot \sum_{j=1}^{6} G_{ij} W_{ji} \quad \forall\, i. \tag{51}$$

To conclude the section, it can be observed that the generic expression for the quantum bound of $\alpha - MagicSquare$ expressions is $(\alpha + 5)$. This holds true for all $\alpha \geqslant 0$.

2.4 $\alpha^2 - MagicSquare$ INEQUALITIES

We now prove the following claim for another variant of the MagicSquare inequality (Equation 42):

Claim: For $\alpha \geqslant \frac{1}{3}$, the quantum bound that the expression of a $\alpha^2 - MagicSquare$ inequality can take is of the form:

$$S'_{\alpha^2} = 2 \cdot (\alpha + 2). \tag{52}$$

2.4.1 *Definition of inequality*

Under the name of $\alpha^2 - MagicSquare$, we denote a group of Bell inequalities of the form:

$$\begin{aligned} I'_{\alpha^2} = \langle A_0 B_0 \rangle - \alpha \cdot \langle A_0 B_1 \rangle + \langle A_0 B_2 \rangle - \alpha \cdot \langle A_1 B_0 \rangle + \\ \langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_0 \rangle + \langle A_2 B_1 \rangle - \langle A_2 B_2 \rangle \leqslant 2\alpha + 3. \end{aligned} \tag{53}$$

Carrying forth the same definition for scalar products of the unit vectors $x_1, x_2, x_3, y_1, y_2, y_3$ as in Equation 44 in Section 2.3.1, we now compute an expression giving the maximum quantum bound for the expression represented by I'_{α^2}.

Substituting $\alpha = 1$ in Equation 53 results in the expression for the MagicSquare inequality (Equation 42).

2.4.2 *Derivation of quantum bound*

Once again, we make use of the dual problem in Equation 24, where $\lambda = (\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5, \lambda_6)$. Now, for $\alpha^2 - MagicSquare$ inequalities, the matrix W is:

$$W = \begin{pmatrix} 0 & 0 & 0 & 1 & -\alpha & 1 \\ 0 & 0 & 0 & -\alpha & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & -1 \\ 1 & -\alpha & 1 & 0 & 0 & 0 \\ -\alpha & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & -1 & 0 & 0 & 0 \end{pmatrix}. \tag{54}$$

For values of $0 < \alpha < \frac{1}{3}$ there does exist some quantum advantage and the quantum bound is greater than the classical bound. However, in the present work, we will not be deriving any analytical expressions for $\alpha^2 -$ MagicSquare with α in that range. For $\alpha < 0$, α^2–MagicSquare inequalities have no quantum advantage.

For $\alpha \geqslant \frac{1}{3}$, Equation 55 gives the choice of the elements of λ that help satisfy the constraint of the dual problem and ensure that the objective function attains the optimal value.

$$\begin{aligned} \lambda_1 = \lambda_2 = \lambda_4 = \lambda_5 = \frac{(\alpha+1)}{2}; \\ \lambda_3 = \lambda_6 = 1, \end{aligned} \tag{55}$$

By solving the dual problem we have the following bound on the quantum value S'_{α^2}:

$$S'_{\alpha^2} \leqslant \sum_{i=1}^{6} \lambda_i = 2 \cdot (\alpha + 2). \tag{56}$$

For $\alpha \geqslant \frac{1}{3}$, it can be seen that for W given by Equation 54 and G given by Equation 48 and Equation 49, optimal solution for the primal problem is encountered. Consequently, we have that:

$$S'_{\alpha^2} \geqslant \frac{1}{2} \mathrm{Tr}(GW) = 2 \cdot (\alpha + 2). \tag{57}$$

Since the feasible points given by Equation 56 and Equation 57 satisfy the duality and strong duality conditions, the quantum bound for α^2–MagicSquare inequalities is given by: $S'_{\alpha^2} = 2 \cdot (\alpha + 2)$.

Thus, the claim in Equation 52 holds true. Also, to state explicitly, the value of correlators $\langle A_x B_y \rangle$ for attaining the quantum bound should be of the form:

$$\begin{aligned} \langle A_0 B_1 \rangle = \langle A_1 B_0 \rangle = \langle A_2 B_2 \rangle = -1; \\ \langle A_0 B_0 \rangle = \langle A_0 B_2 \rangle = \langle A_1 B_1 \rangle = \langle A_1 B_2 \rangle = \langle A_2 B_0 \rangle = \langle A_2 B_1 \rangle = \frac{1}{2}. \end{aligned} \tag{58}$$

In the next section, the final family of Bell inequalities is introduced and analyzed.

2.5 $\alpha^3 -$ MagicSquare INEQUALITIES

Let us now look at the proof for the following claim:

Claim: For $\alpha \geqslant \frac{1}{2}$, the quantum bound of $\alpha^3 -$ MagicSquare Bell inequality expressions can be stated as:

$$S'_{\alpha^3} = 3 \cdot (\alpha + 1). \tag{59}$$

2.5.1 *Definition of inequality*

Considering positive values for α, we define $\alpha^3 -$ MagicSquare to be a group of Bell inequalities given by:

$$\begin{aligned} I'_{\alpha^3} = \langle A_0 B_0 \rangle - \alpha \cdot \langle A_0 B_1 \rangle + \langle A_0 B_2 \rangle - \alpha \cdot \langle A_1 B_0 \rangle + \\ \langle A_1 B_1 \rangle + \langle A_1 B_2 \rangle + \langle A_2 B_0 \rangle + \langle A_2 B_1 \rangle - \alpha \cdot \langle A_2 B_2 \rangle \leqslant 3 \cdot \alpha + 2. \end{aligned} \tag{60}$$

2.5.2 *Derivation of quantum bound*

We use the same approach as in Section 2.4.2, the only differences being slight modifications to the matrix W and vector λ. We take:

$$W = \begin{pmatrix} 0 & 0 & 0 & 1 & -\alpha & 1 \\ 0 & 0 & 0 & -\alpha & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & -\alpha \\ 1 & -\alpha & 1 & 0 & 0 & 0 \\ -\alpha & 1 & 1 & 0 & 0 & 0 \\ 1 & 1 & -\alpha & 0 & 0 & 0 \end{pmatrix}. \tag{61}$$

$$\text{And} \quad \lambda_i = \frac{(\alpha+1)}{2} \quad \forall \ i.$$

Indeed, for this choice of vector λ and the constraint that $\alpha \geqslant \frac{1}{2}$, the dual problem constraints are satisfied. Consequently, we have that:

$$S'_{\alpha^3} \leqslant \sum_{i=1}^{6} \lambda_i = 3 \cdot (\alpha+1). \tag{62}$$

Now, to solve the primal problem, as specified in Equation 28, we take the matrix G to be the matrix in Equation 48. Once again, by choosing the values of the scalar products in G to be the ones in Equation 49, we get the solution for the primal problem. And consequently, we have that:

$$S'_{\alpha^3} \geqslant \frac{1}{2} \mathrm{Tr}(GW) = 3 \cdot (\alpha+1). \tag{63}$$

Since the feasible optimal solutions to the primal and dual problems have the same value, the optimal strategy leads to the quantum bound of this common value, that is $S'_{\alpha^3} = 3 \cdot (\alpha+1)$.

Thus, for $\alpha > \frac{1}{2}$, the quantum bound is $3 \cdot (\alpha+1)$. Also, since the optimal quantum strategy is the same as the optimal strategies for α–MagicSquare and α^2–MagicSquare inequalities, the values of the correlators $\langle A_x B_y \rangle$ at optimality are as mentioned in Equation 58.

The results derived in this chapter shall be used in the following chapter for the key-rate analyses in the asymptotic and finite regimes.

3

DIQKD USING THE INEQUALITIES ANALYZED

Before delving into the finite key regime, it is important to discuss some results pertaining to the asymptotic key regime and to establish constructs that, apart from being relevant to the asymptotic regime, are primarily useful for the analyses in the finite regime.

Section 3.1 shows that with the $\alpha - \text{CHSH}$ inequalities (defined in Section 2.1), it is possible to achieve marginally higher rate and marginally greater noise tolerance for certain values of α, as compared to the rate and noise tolerance achieved using the lower bound on the min-entropy using the CHSH inequality.

Section 3.2 transitions from the use of min-entropy to the use of von Neumann entropy, which, as described in Section 1.4, helps achieve significantly better noise tolerance. For this scenario, we derive a bound on the von Neumann entropy and show that the tightness of this bound is dependent on how high the value of the ratio of an inequality's quantum bound to its classical bound is. The overall bound is tight only in case of the CHSH inequality. And therefore, among the inequalities that we are considering in this chapter, the best results, in terms of all three parameters of our interest (i.e. rate, noise tolerance and minimum number of rounds required), are yielded by CHSH inequality.

3.1 CONSIDERING BOUND ON THE MIN-ENTROPY

In this section, we compare the use of $\alpha - \text{CHSH}$ inequality versus the use of CHSH inequality in a scenario that employs the use of min-entropy to compute the key rate. The approach used is the one presented in the paper by Masanes *et al.* [MPA11]. For both these inequalities, the maximal violation using quantum correlations is achieved using the maximally entangled state. And so, we fix the state under consideration to be the Bell state $|\phi^+\rangle = \frac{(|00\rangle+|11\rangle)}{\sqrt{2}}$. So for a depolarizing noise model and the visibility of the Bell state given by ν, the state ρ can be expressed as:

$$\rho = \nu \cdot |\phi^+\rangle\langle\phi^+| + (1-\nu) \cdot \frac{\mathbb{I}}{4}. \tag{64}$$

Now, from Section 1.4, we can recall how Bob has an extra choice of observable B_2 for the error correction phase. For this error correction procedure, it is important to ensure that the need for transmission of information is as little as possible. This requires as perfect correlation as can be achieved among Alice and Bob's outcomes. Now, for the inequalities under consideration, it is possible to fix B_2 for Alice's choice of A_0, such that their outcomes in the error correction phase

Section 3.2.2.1 gives an elaborate description on the measurements that ensure that this requirement of perfect correlations is satisfied by $\alpha-$CHSH while attaining the maximum quantum value.

can be perfectly correlated. Considering A_0 to be σ_z, we can thereby fix B_2 to also be σ_z. For the state ρ defined in Equation 64, we have seen in Section 1.4 that the error correction term facilitating minimum leakage of information is of the form $H(A \mid B) = h\left(\frac{1-\nu}{2}\right)$.

Now, for both, α–CHSH as well as CHSH, the equation below gives the expression for the computation of the key rate, as a function of the visibility, ν, of the state ρ:

$$\text{rate} \geqslant H_{\min}(A \mid E) - h\left(\frac{1-\nu}{2}\right). \tag{65}$$

In Equation 65, $H_{\min}(A \mid E)$ is the min-entropy and h denotes the binary Shannon entropy. As seen in Section 1.4, the min-entropy relates to Eve's guessing probability as: $H_{\min}(A \mid E) = -\log_2(p_{\text{guess}})$. An upper bound on this guessing probability can be computed using the QETLAB [Joho3] package's NPAHierarchy module.

Now, the min-entropy, $H_{\min}(A \mid E)$, for $\alpha-$CHSH, for $\cos^2\left(\frac{\pi}{8}\right) < \alpha < 1$, is higher than the min-entropy for the CHSH inequality. Since the error correction term (i.e. the second term in Equation 65) will be the same for both the inequalities, the overall lower bound on the rate curve will be better for α–CHSH. Although this improvement is very marginal and at most of the order of half a percent, it is at least evident that while considering the min-entropy scenario, CHSH is not the best alternative. Figure 4 gives a comparison of $\alpha-$CHSH and CHSH inequality in the asymptotic key regime whilst considering the min-entropy to bound the corresponding rate curves. For a detailed derivation of Equation 65, we redirect the readers to Section 1.4.

It is, however, evident from the plots in Figure 4 that the von Neu-

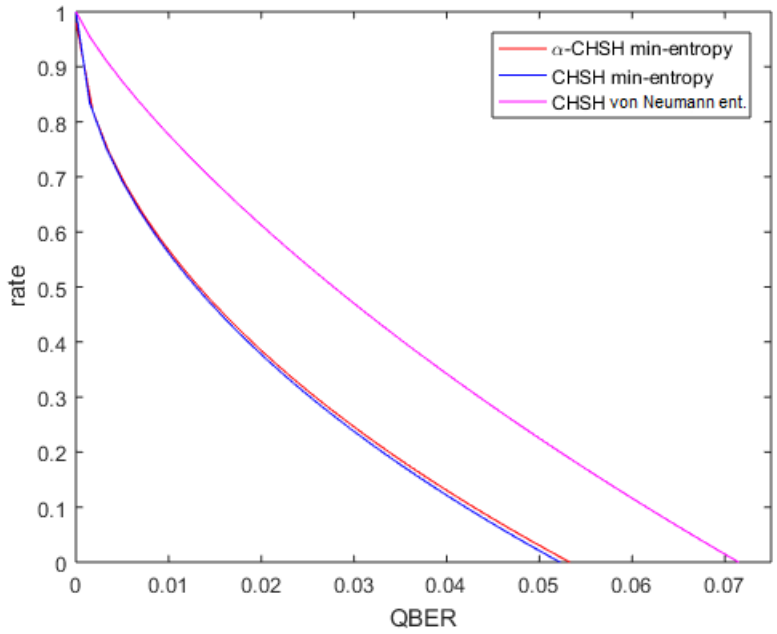


Figure 4: Rate vs visibility plot for the scenario involving $\alpha-$CHSH for $\alpha = \left(\frac{\pi}{8}\right)$ and $\alpha = 1$.

mann entropy for the CHSH inequality is significantly higher than the min-entropy for α–CHSH inequality. Note that for all these scenarios, the error correction term has the same value. It is therefore, a

good motivation to derive a bound on the conditional von Neumann entropy for α—CHSH inequalities and to compare it with the von Neumann entropy for CHSH inequality. So, let us now focus on finding a bound on the von Neumann entropy for the α—CHSH inequality, and subsequently for other inequalities that have been introduced earlier (in Chapter 2). Our attempt to derive such a bound on the von Neumann entropy for inequalities other than CHSH is new.

3.2 BOUNDING THE VON NEUMANN ENTROPY

For the CHSH inequality, a tight bound on the key rate is given by the conditional von Neumann entropy. Unlike min-entropy, von Neumann entropy cannot be easily computed by numerical methods, such as SDP. It needs to be derived using other techniques. So far, such a derivation has been performed only for the CHSH inequality [Pir+09]. In this section, we shall attempt to extend the proof presented in [Pir+09] and derive our own bound on the von Neumann entropy, and in turn, bound the key rate.

In [Pir+09], Pironio *et al.* give the proof for the derivation of the Holevo quantity, χ, between Eve and Bob. This Holevo quantity can be defined as:

$$\chi = H(A) - H(A \mid E). \tag{66}$$

From Section 1.4, we already know that:

$$\mathrm{rate} \geqslant H(A \mid E) - EC. \tag{67}$$

The Holevo quantity can, thus, be used to define the key rate as:

$$\mathrm{rate} \geqslant H(A) - \chi - h(\mathrm{QBER}). \tag{68}$$

As already seen in the previous section, $\mathrm{QBER} = \frac{(1-v)}{2}$ *and is the Quantum Bit Error Rate (QBER) which helps gauge the noise tolerance.*

As per the proof in [Pir+09], for the CHSH inequality, the value of χ is upper bound in the following manner:

$$\chi \leqslant h\Big(\frac{1 + \sqrt{(\frac{g}{2})^2 - 1}}{2}\Big). \tag{69}$$

In the above equation, g denotes the quantum violation value achieved for the CHSH inequality.

For the inequalities that we will be considering in this chapter, the third term in the lower bound for the rate (Equation 68), which characterizes the error correction term, is equal to the binary entropy of QBER.

Intuitively, a tight bound on the Holevo quantity would imply a tight bound on $H(A \mid E)$ and thereby, an overall tight bound on the rate.

While proving the upper bound for the Holevo quantity, the authors of [Pir+09] take into account various considerations. In the following

subsections, we first list out all these considerations. Next, ensuring that these considerations are adhered to, and using the relations between correlators at optimality, we derive a generic upper bound for the Holevo quantity for all the families of inequalities described in Chapter 2. Additionally, a set of measurement operators, leading to the optimal quantum bound and satisfaction of all the considerations, is given for each of those families of inequalities. Finally, we focus on how the rates trend for different families of inequalities and have a look at their respective noise tolerances as well.

3.2.1 *Considerations regarding set-up*

$|\phi^+\rangle = \frac{(|00\rangle+|11\rangle)}{\sqrt{2}}$, $|\phi^-\rangle = \frac{(|00\rangle-|11\rangle)}{\sqrt{2}}$, $|\psi^+\rangle = \frac{(|01\rangle+|10\rangle)}{\sqrt{2}}$ and $|\psi^-\rangle = \frac{(|01\rangle-|10\rangle)}{\sqrt{2}}$ *are the four Bell pair states that are orthogonal to each other. They define the two-qubit Bell basis.*

In order to derive the Holevo quantity for the families of Bell inequalities in the same way as the Holevo quantity is derived for the CHSH inequality, certain considerations need to be taken into account. These are listed as follows:

- Let us assume that the state under consideration can be reduced to the Bell diagonal state of two qubits. This means that for the Bell basis ordered as $\{|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle, |\psi^-\rangle\}$, the state ρ_λ can be given by:

$$\rho_\lambda = \begin{pmatrix} \lambda_{\phi^+} & 0 & 0 & 0 \\ 0 & \lambda_{\phi^-} & 0 & 0 \\ 0 & 0 & \lambda_{\psi^+} & 0 \\ 0 & 0 & 0 & \lambda_{\psi^-} \end{pmatrix}. \tag{70}$$

  where the eigenvalues are chosen in such a way that: $\lambda_{\phi^+} \geqslant \lambda_{\psi^-}$ and $\lambda_{\phi^-} \geqslant \lambda_{\psi^+}$.

  If one restricts the subspace of the system to dimension $d = 2$, then it is general enough to look at states of the form Equation 70 [Reno8; Pir+09]. Now, for Bell inequalities with two inputs and two outcomes per party it is enough to consider the analysis of systems of dimension 2. For inequalities with three inputs and two outputs per party, we will take this assumption of $d = 2$ into account for the ease of the derivation. However, for the inequalities with three inputs, we restrict the setup to a subspace of dimension $d = 2$.

- In the paper [Pir+09], it is assumed that, the measurement operators are restricted to be in the XZ plane. A detailed proof for this consideration can be found in the lemma presented in [Mas06]. Among the families of inequalities introduced in Chapter 2, this assumption of restricting the system to a subspace of dimension 2 is general enough to cover all possible arbitrary measurements for inequalities with two inputs, two outputs per party. On the other hand, for inequalities with multiple inputs and two outputs per party, this restriction on the subspace dimension is still an assumption. A more detailed description of

the choice of operators to achieve maximum quantum value can be found in the following subsection.

3.2.2 *Prospective setup for optimality*

For each family of inequalities introduced in Chapter 2, we now consult the relations defined between the correlators when these inequalities achieve the maximum quantum value. These have been mentioned under the subsection of optimum quantum strategy for each group of inequalities. We also take into account the requirements set forth in Section 3.2.1. Additionally, it is assumed that Alice and Bob's operators, in general, are of the form:

$$\begin{aligned} A_0 &= \cos\mu_1 \cdot \sigma_z + \sin\mu_1 \cdot \sigma_x; \quad A_1 = \cos\mu_2 \cdot \sigma_z + \sin\mu_2 \cdot \sigma_x; \\ B_0 &= \cos\mu_3 \cdot \sigma_z + \sin\mu_3 \cdot \sigma_x; \quad B_1 = \cos\mu_4 \cdot \sigma_z + \sin\mu_4 \cdot \sigma_x. \end{aligned} \tag{71}$$

It is important to recollect that for inequalities with two inputs per party defined in Chapter 2, it is general enough to consider that the operators are in the XZ plane. For inequalities with three inputs per party considered in this chapter, in order to derive bound on Holevo quantity in the same way as in [Pir+09], we assume that the operators lie in the XZ plane.

Accordingly, the optimal measurement operators for the different families of inequality that help them achieve their respective maximum quantum values for the state $|\phi^+\rangle\langle\phi^+|$ are presented below.

3.2.2.1 $\alpha-$CHSH *inequalities*

For the expressions of the $\alpha-$CHSH inequalities, if we take the measurement operators to be of the form given by Equation 71, and if we take into account the relations established in Equation 30, then the set of values for the four angles (i.e. μ_1 to μ_4) at optimality is given by:

$$\begin{aligned} \mu_2 = \cos^{-1}\left(3\cdot\sqrt{\frac{(\alpha+1)}{4\alpha}} - 4\cdot\left(\sqrt{\frac{(\alpha+1)}{4\alpha}}\right)^3\right) + \cos^{-1}\left(\sqrt{\frac{(\alpha+1)}{4\alpha}}\right); \\ \mu_3 = \cos^{-1}\left(3\cdot\sqrt{\frac{(\alpha+1)}{4\alpha}} - 4\cdot\left(\sqrt{\frac{(\alpha+1)}{4\alpha}}\right)^3\right); \\ \mu_1 = 0; \quad \mu_4 = -\cos^{-1}\left(\sqrt{\frac{(\alpha+1)}{4\alpha}}\right). \end{aligned} \tag{72}$$

3.2.2.2 $\alpha\beta-$CHSH *inequalities*

In case of expressions from the $\alpha\beta-$CHSH group of inequalities, we take into account the relations established in Equation 38. Now, the values for the four angles of Equation 71 at optimality can be stated as:

$$\begin{aligned} \mu_2 = \cos^{-1}\left(\frac{(\alpha-\beta+2\alpha^2\beta)}{2\alpha\sqrt{\alpha\beta(1+\alpha\beta)}}\right) + \cos^{-1}\left(\frac{(\alpha+\beta)}{2}\sqrt{\frac{1}{\alpha\beta(1+\alpha\beta)}}\right); \\ \mu_1 = 0; \quad \mu_3 = \cos^{-1}\left(\frac{(\alpha-\beta+2\alpha^2\beta)}{2\alpha\sqrt{\alpha\beta(1+\alpha\beta)}}\right); \\ \mu_4 = -\cos^{-1}\left(\frac{(\beta-\alpha+2\alpha\beta^2)}{2\beta\sqrt{\alpha\beta(1+\alpha\beta)}}\right). \end{aligned} \tag{73}$$

3.2.2.3 *Variants of the* MagicSquare *inequality*

To recall, we denote the MagicSquare inequality by:

$$\begin{aligned}\langle A_0B_0\rangle - \langle A_0B_1\rangle + \langle A_0B_2\rangle - \langle A_1B_0\rangle + \langle A_1B_1\rangle \\ + \langle A_1B_2\rangle + \langle A_2B_0\rangle + \langle A_2B_1\rangle - \langle A_2B_2\rangle \leqslant 5.\end{aligned} \tag{74}$$

As we have seen in the previous chapter, at a point when the maximum quantum violation is attained by this inequality, the value of the correlators is given as:

$$\begin{aligned}\langle A_0B_1\rangle = \langle A_1B_0\rangle = \langle A_2B_2\rangle = -1; \\ \langle A_0B_0\rangle = \langle A_0B_2\rangle = \langle A_1B_1\rangle = \langle A_1B_2\rangle = \langle A_2B_0\rangle = \langle A_2B_1\rangle = \frac{1}{2}.\end{aligned} \tag{75}$$

And in fact, it has been observed that for the defined domains of $(\alpha \geqslant 0)$, $(\alpha \geqslant \frac{1}{2})$ and $(\alpha \geqslant \frac{1}{2})$ for $\alpha - \mathrm{MagicSquare}$, $\alpha^2 - \mathrm{MagicSquare}$ and $\alpha^3 - \mathrm{MagicSquare}$ inequalities, respectively, the values of the correlators at optimality are the same as the ones mentioned in Equation 75. Thus, we establish the set of measurement operations that work at optimality for all these inequalities alike. These measurements are given by:

$$\begin{aligned}A_0 = \sigma_z; \;\; B_0 = \cos\left(\frac{\pi}{3}\right)\sigma_z + \sin\left(\frac{\pi}{3}\right)\sigma_x; \\ A_1 = \cos\left(\frac{2\pi}{3}\right)\sigma_z - \sin\left(\frac{2\pi}{3}\right)\sigma_x; \;\; B_1 = -\sigma_z; \\ A_2 = \cos\left(\frac{2\pi}{3}\right)\sigma_z + \sin\left(\frac{2\pi}{3}\right)\sigma_x; \;\; B_2 = \cos\left(\frac{\pi}{3}\right)\sigma_z - \sin\left(\frac{\pi}{3}\right)\sigma_x.\end{aligned} \tag{76}$$

Notice how it is possible to attain the optimal quantum strategy for the three input variants of the MagicSquare inequalities even after restricting the operators to be in the XZ plane.

3.2.2.4 *Chained inequalities*

As discussed in Section 1.4, chained inequalities [BC90] have been used in the asymptotic key regime while considering the min-entropy to define the key rate. The general form of expression of these inequalities with m inputs per party is given as:

$$\sum_{i=1}^{n}\langle A_iB_i\rangle + \sum_{i=1}^{n-1}\langle A_{i+1}B_i\rangle - \langle A_1B_m\rangle \leqslant 2m-2. \tag{77}$$

Let us explore the implications of using the chained inequality in the asymptotic regime (and later, in the finite regime) by directly bounding the von Neumann entropy. These bipartite Bell inequalities, with m inputs and 2 outputs per party, have a classical bound of the form $(2m-2)$ and quantum bound of the form $2m \cdot \cos\left(\frac{\pi}{2m}\right)$ [Weh06]. The Chained inequality for 3 inputs per party is given by:

Chained inequality with $m = 2$ is equivalent to the CHSH inequality.

$$\langle A_0B_0\rangle + \langle A_0B_1\rangle + \langle A_1B_1\rangle + \langle A_1B_2\rangle + \langle A_2B_2\rangle - \langle A_0B_2\rangle \leqslant 4. \tag{78}$$

When the number of inputs is $m = 3$, it is possible to achieve the optimal strategy with the restriction of Section 3.2.1. A possibility of measurement operators at optimality, for the maximally entangled state $|\phi^+\rangle$, is given by:

Notice how it is possible to attain the optimal quantum strategy for the three input variant of the Chained inequality even after restricting the operators to be in the XZ plane.

$$\begin{aligned} A_0 = \sigma_z; \quad B_0 = \cos\left(\frac{\pi}{6}\right)\sigma_z + \sin\left(\frac{\pi}{6}\right)\sigma_x; \\ A_1 = \cos\left(\frac{\pi}{3}\right)\sigma_z + \sin\left(\frac{\pi}{3}\right)\sigma_x; \quad B_1 = \sigma_x; \\ A_2 = \cos\left(\frac{2\pi}{3}\right)\sigma_z + \sin\left(\frac{2\pi}{3}\right)\sigma_x; \quad B_2 = \cos\left(\frac{5\pi}{6}\right)\sigma_z + \sin\left(\frac{5\pi}{6}\right)\sigma_x. \end{aligned} \tag{79}$$

Having established in detail the various conditions and settings for optimality, let us now look at a generalized derivation of the Holevo quantity for the inequalities in question.

3.2.3 *A new lower bound for the von Neumann entropy*

Section 3.2.1 gives a gist of requirements considering which we can proceed with the derivation of the bound on the von Neumann entropy. One of the considerations is that of restricting the subspace to dimension 2. As mentioned earlier and shown in [Pir+09], this assumption is general enough to cover all possible arbitrary measurements for inequalities with two inputs per party. On the other hand, for inequalities with multiple inputs per party, this restriction on the subspace dimension is still an assumption.

In addition to this, the description in Section 3.2.2 gives an optimal strategy for each group of inequalities under consideration. Taking these strategies into account, Alice's outcomes are random, and each of the two possibilities are equally probable. Thus, we have that $H(A) = h\left(\frac{1}{2}\right) = 1$. The definition in Equation 66 equation thereby simplifies to:

$$\begin{aligned} \chi &= 1 - H(A \mid E); \\ \implies H(A \mid E) &= 1 - \chi; \\ \implies \text{rate} &\geqslant 1 - \chi - h(\text{QBER}). \end{aligned} \tag{80}$$

Thus, for the inequalities under consideration, the conditional von Neumann entropy can be expressed as a function of the Holevo quantity χ as: $H(A \mid E) = 1 - \chi$. Therefore, choosing an upper bound on the Holevo quantity can set a bound on the von Neumann entropy. Now, as per Lemma 6 of [Pir+09], for Bell diagonal state of the form of ρ_λ in Equation 70, we have that:

$$\begin{aligned} \chi \leqslant h\left(\frac{1+\sqrt{2R^2-1}}{2}\right) \quad \forall \quad R^2 > \frac{1}{2}; \\ \text{And} \quad \chi \leqslant 1 \quad \forall \quad R^2 \leqslant \frac{1}{2}. \end{aligned} \tag{81}$$

Here, $R^2 = (\lambda_{\phi^+} - \lambda_{\psi^-})^2 + (\lambda_{\phi^-} - \lambda_{\psi^+})^2$.

Now, for the state ρ_λ (as defined in Equation 70), we need to establish a relation between the maximum quantum value, S_λ, attainable using a particular Bell inequality, and the parameter R. In that regard, we present the following claim and the corresponding proof for the claim follows.

Claim: Let $\mathbb{C}$ be the classical bound of a particular two-outcome Bell inequality expression, with only full correlations, that is maximally violated by a maximally entangled two-qubit state. Then for the state ρ_λ and the maximum quantum violation for the state given by S_λ, we have the following lower bound on the von Neumann entropy:

$$H(A \mid E) \geqslant 1 - h\Big(\frac{1+\sqrt{(\frac{S_\lambda}{\mathbb{C}})^2 - 1}}{2}\Big). \tag{82}$$

Proof. Let us first prove this claim for $\alpha - \text{CHSH}$ inequalities. For that, let the measurement operators be of the form described in Equation 71. Then, for a combination of values of λ_{ϕ^+}, λ_{ϕ^-}, λ_{ψ^+}, λ_{ψ^-}, the quantum value of applying the $\alpha - \text{CHSH}$ inequality, with arbitrary measurements in XZ plane, on the state ρ_λ is given by:

It is intuitive to see that $\text{Tr}(\langle A_0 B_0\rangle \cdot |\phi^+\rangle\langle\phi^+|) = \cos(\mu_1 - \mu_3)$. Likewise, the other terms in Equation 83 emerge and the expression for S_λ is thus formulated.

$$\begin{aligned} S_\lambda = (\lambda_{\phi^+} - \lambda_{\psi^-}) \cdot (\alpha \cdot \cos(\mu_1 - \mu_3) + \cos(\mu_1 - \mu_4) + \cos(\mu_2 - \mu_3) \\ - \cos(\mu_2 - \mu_4)) + (\lambda_{\phi^-} - \lambda_{\psi^+}) \cdot (\alpha \cdot \cos(\mu_1 + \mu_3) \\ + \cos(\mu_1 + \mu_4) + \cos(\mu_2 + \mu_3) - \cos(\mu_2 + \mu_4)). \end{aligned} \tag{83}$$

It is quite trivial to notice that taking $\lambda_{\phi^+} = \lambda_{\phi^-} = \lambda_{\psi^+} = \lambda_{\psi^-} = \frac{1}{4}$ results in the maximally mixed state for ρ_λ, and the value of S_λ is, evidently, equal to 0. Also, it should be noted that as per the condition imposed on these eigenvalues in Equation 70, both $(\lambda_{\phi^+} - \lambda_{\psi^-}) \geqslant 0$ and $(\lambda_{\phi^-} - \lambda_{\psi^+}) \geqslant 0$ hold true.

Now, barring the case where the eigenvalues of ρ_λ are equal to each other, (i.e. $\lambda_{\phi^+} = \lambda_{\phi^-} = \lambda_{\psi^+} = \lambda_{\psi^-} = \frac{1}{4}$), if we consider the other possibilities of the values of these eigenvalues, and the fact that $R^2 = (\lambda_{\phi^+} - \lambda_{\psi^-})^2 + (\lambda_{\phi^-} - \lambda_{\psi^+})^2$, we can define some θ such that $(\lambda_{\phi^+} - \lambda_{\psi^-}) = |R| \cdot \cos\theta$ and consequently, $(\lambda_{\phi^-} - \lambda_{\psi^+}) = |R| \cdot \sin\theta$. Then for θ ranging from 0 to $\frac{\pi}{4}$ radians, all the different combinations of eigenvalues can be covered. With this trigonometric substitution, Equation 83 now becomes:

Since $(\lambda_{\phi^+} - \lambda_{\psi^-}) \geqslant 0$ and $(\lambda_{\phi^-} - \lambda_{\psi^+}) \geqslant 0$ hold true, θ can range from 0 to $\frac{\pi}{2}$ only. For $\frac{\pi}{4} < \theta \leqslant \frac{\pi}{2}$, we simply plug in $-\mu_3$ and $-\mu_4$, instead of μ_3 and μ_4 in Equation 84.

$$\begin{aligned} S_\lambda = |R| \cdot \cos\theta \cdot (\alpha \cdot \cos(\mu_1 - \mu_3) + \cos(\mu_1 - \mu_4) + \cos(\mu_2 - \mu_3) \\ - \cos(\mu_2 - \mu_4)) + |R| \cdot \sin\theta \cdot (\alpha \cdot \cos(\mu_1 + \mu_3) \\ + \cos(\mu_1 + \mu_4) + \cos(\mu_2 + \mu_3) - \cos(\mu_2 + \mu_4)). \end{aligned} \tag{84}$$

Now, as θ increases from 0 to $\frac{\pi}{4}$, the maximum value that S_λ can obtain starts increasing. This has been verified numerically. At $\theta = 0$, the term bearing $\sin\theta$ vanishes; and S_λ is merely given by:

$$S_\lambda = |R| \cdot (\alpha \cdot \cos(\mu_1 - \mu_3) + \cos(\mu_1 - \mu_4) + \cos(\mu_2 - \mu_3) - \cos(\mu_2 - \mu_4)).$$

(85)

Now, since $(\alpha \cdot \cos(\mu_1 - \mu_3) + \cos(\mu_1 - \mu_4) + \cos(\mu_2 - \mu_3) - \cos(\mu_2 - \mu_4))$ denotes the expression resulting from applying quantum correlations of the $\alpha -$ CHSH inequality to the $|\phi^+\rangle$ state, the maximum value that it can procure is quantum bound of the inequality (which we are denoting by $\mathbb{Q}$). Thus, we have that, at $\theta = 0$:

$$S_\lambda \geqslant \mathbb{Q} \cdot |R|. \tag{86}$$

Next, for $\theta = \frac{\pi}{4}$, the expression in Equation 84 will modify to:

$$\begin{aligned} S_\lambda = \sqrt{2} \cdot |R| \cdot (\alpha \cdot \cos\mu_1 \cdot \cos\mu_3 + \cos\mu_1 \cdot \cos\mu_4 \\ + \cos\mu_2 \cdot \cos\mu_3 - \cos\mu_2 \cdot \cos\mu_4). \end{aligned} \tag{87}$$

Equation 87 arises from the fact that $\cos(A-B) + \cos(A+B) = 2 \cdot \cos A \cdot \cos B$.

It is interesting to note that the maximum value of $(\alpha \cdot \cos\mu_1 \cdot \cos\mu_3 + \cos\mu_1 \cdot \cos\mu_4 + \cos\mu_2 \cdot \cos\mu_3 - \cos\mu_2 \cdot \cos\mu_4)$ is in fact, equal to the classical bound of the α—CHSH inequality. This has been verified numerically. And in fact, the maximum value for this expression is attained by applying the commuting operators that help attain the classical bound. And since we are denoting this classical bound by $\mathbb{C}$, we have that:

$$\sqrt{2} \cdot \mathbb{C} \cdot |R| \geqslant S_\lambda. \tag{88}$$

Combining Equation 86 and Equation 88, we have that:

$$\sqrt{2} \cdot \mathbb{C} \cdot |R| \geqslant S_\lambda \geqslant \mathbb{Q} \cdot R. \tag{89}$$

Also, from the bound on χ in Equation 81 and the relation established in the above equation, we have that, for $R^2 \geqslant \frac{1}{2}$:

$$h\Big(\frac{1+\sqrt{(\frac{S_\lambda}{\mathbb{C}})^2 - 1}}{2}\Big) \geqslant \chi \geqslant h\Big(\frac{1+\sqrt{2(\frac{S_\lambda}{\mathbb{Q}})^2 - 1}}{2}\Big). \tag{90}$$

Since, for the inequalities under our consideration, $H(A \mid E) = 1 - \chi$, the claim in Equation 82 follows from Equation 90. □

3.2.4 *Transitioning from* S_λ *to* g

For the derivation of the bound on the von Neumann entropy in the previous subsection, we have assumed the system to be confined to a subspace of dimension 2. Also, S_λ is the maximum violation that can be attained using quantum correlations in this subspace. In this subsection, we extend the convexity argument used in [Pir+09] to extend the scope of the derived bound from being a function of S_λ to being a function of the violation g considering the overall space, for all the inequalities under consideration. For each subspace i of dimension 2, let $F(S_{\lambda i})$ denote the von Neumann entropy of that subspace. Thus, we have that:

$$F(S_{\lambda i}) = H(A \mid E)_i \geqslant 1 - h\Big(\frac{1+\sqrt{(\frac{S_\lambda}{\mathbb{C}})^2 - 1}}{2}\Big). \tag{91}$$

Now, owing to the concavity of the monotonically decreasing function F, the overall von Neumann entropy satisfies:

$$H(A \mid E) = \sum_i p_i \cdot F(S_{\lambda_i}) \leqslant F(\sum_i p_i \cdot S_{\lambda_i}). \tag{92}$$

And since we can express the violation g as: $g = \sum_i p_i \cdot \{S_\lambda\}_i$, we have that:

$$H(A \mid E) \leqslant F(g). \tag{93}$$

in this manner, the assumption of reduction of the state shared by Alice and Bob to a Bell diagonal state and the assumption of their measurement operations being in the XZ plane only can be generalized to arbitrary measurements and dimension for Bell inequalities with full correlations and two inputs, two outcomes per party. For Bell inequalities with three inputs per party, these assumptions are, however, assumptions after all, which help in easily extending the same proof for the derivation of the von Neumann entropy from the two inputs case to the three inputs case.

Now, for an arbitrary state ρ with the depolarising noise model (recall Equation 64), the quantum value can be expressed in terms of $Q \cdot v$. Consequently, from Equation 90 we can say that:

$$\begin{aligned} h\Big(\frac{1+\sqrt{(\frac{Q}{C}\cdot v)^2-1}}{2}\Big) \geqslant \chi \geqslant h\Big(\frac{1+\sqrt{2v^2-1}}{2}\Big). \\ \implies 1-h\Big(\frac{1+\sqrt{(\frac{Q}{C}\cdot v)^2-1}}{2}\Big) \leqslant H(A \mid E) \leqslant 1-h\Big(\frac{1+\sqrt{2v^2-1}}{2}\Big). \end{aligned} \tag{94}$$

In the following sections of this chapter, we will see the implications of the bounds defined on the von Neumann entropy to study the key rate curves in the asymptotic and finite key regimes.

3.3 KEY RATE ANALYSES IN THE ASYMPTOTIC KEY REGIME

In this section, using the constructs established in the previous sections of this chapter, results of key rate analyses in the asymptotic regime are discussed.

Firstly, for the bounds derived on the Holevo quantity in Equation 94, it is important to notice that in case of CHSH inequality, the upper and lower bounds coincide. So the bound on the Holevo quantity is tight. However, for the other inequalities that we have considered in this chapter, certain gap starts emerging between the upper and lower bounds that we have defined for the Holevo quantity. More specifically, this gap depends on the value of the ratio $\frac{Q}{C}$. The higher the value of this ratio, the lesser is the gap between the upper and lower bounds that have been defined for the Holevo quantity.

As such, from the equation for the key rate that has been mentioned in Equation 65 and from the bound that we defined in Equation 90, the lower bound on the rate in the asymptotic regime can be derived to be:

$$\text{rate} \geqslant 1 - h\Big(\frac{1+\sqrt{(\frac{Q}{C}\cdot\nu)^2-1}}{2}\Big) - h\Big(\frac{1-\nu}{2}\Big). \tag{95}$$

It is important to notice that the bound that we have defined gets loose, and hence worse, as the value of the ratio $\frac{Q}{C}$ starts straying away from $\sqrt{2}$ towards 1. It is, therefore, important to inspect the ratio of $\frac{Q}{C}$ for the different inequalities that we have analyzed so far. Table 2 lists down the different families of inequalities and specifies the corresponding expressions for ratio $\frac{Q}{C}$.

Substituting $\beta = 1$ in the $\alpha\beta-$CHSH inequality gives rise to the $\alpha-$CHSH group of inequalities; and therefore it has not been mentioned explicitly in the table.

Table 2: Table specifying the $\frac{Q}{C}$ expressions for different families of inequalities.

#	Family of inequalities	$\frac{Q}{C}$
1.	$\alpha\beta-$CHSH	$\frac{(\alpha+\beta)}{\lvert\alpha-\beta\rvert+2}\cdot\sqrt{\frac{1+\alpha\beta}{\alpha\beta}}$
2.	$\alpha-$MagicSquare	$\frac{\alpha+5}{\alpha+4}$
3.	α^2-MagicSquare	$\frac{2\alpha+4}{2\alpha+3}$
4.	α^3-MagicSquare	$\frac{3\alpha+3}{3\alpha+2}$
5.	Chained inequality (with m inputs per party)	$\frac{2m\cdot\cos(\pi/2m)}{2m-2}$

In case of the $\alpha\beta-$CHSH inequalities, the ratio $\frac{Q}{C}$ attains the highest value of $\sqrt{2}$ at $\alpha = \beta = 1$, which is the case of CHSH inequality, after all. It is important to notice how the expression for $\frac{Q}{C}$ is symmetric in α and β, which in turn ensures the occurrence of the maximum at a point where $\alpha = \beta$. In short, among the $\alpha-$CHSH and $\alpha\beta-$CHSH group of inequalities, the only inequality with a tight bound on the Holevo quantity (as a function of the violation) is the CHSH inequality. As the values of the parameters α and/or β deviate from 1, the value of $\frac{Q}{C}$ starts falling from $\sqrt{2}$ and the overall bounds on the rate curve start becoming loose.

Among the variants of the MagicSquare inequality, namely, the $\alpha-$MagicSquare, α^2-MagicSquare and α^3-MagicSquare inequalities, for the permissible range of values of α (as can be found in Table 1), the highest value that $\frac{Q}{C}$ achieves is $\frac{6}{5} = 1.2$ (which is low compared to $\sqrt{2} \approx 1.4142$) for the inequality arising by putting $\alpha = 0$ in the generic framework for $\alpha-$MagicSquare inequalities.

Finally, in case of Chained inequalities, the value of $\frac{Q}{C}$ starts dropping from $\sqrt{2}$ as the number of inputs, m, increases. To give a quantitative representation of this decline, we present the plot for the value of $\frac{Q}{C}$ versus the number of inputs per party for the Chained inequality in Figure 5. Thus, among the Chained inequalities as well, the best choice is the inequality for $m = 2$, which is, in fact, the CHSH inequality. Taking into consideration that the noise tolerance is defined

in terms of the Quantum Bit Error Rate, QBER $= \frac{1-v}{2}$, we use our bounds on the von Neumann entropy for the inequalities in question to see how the rate curves behave for different values of $\frac{Q}{C}$. As can be seen in Figure 6, with a drop in the value of $\frac{Q}{C}$, there is a drop in the maximum rate achievable and the noise tolerance.

As can be seen in Figure 6, for $\frac{Q}{C} < \sqrt{2}$, it is evident that the lower bound on the rate cannot attain the value 1; and even the noise tolerance will deteriorate. It might even happen that the rate curve obtained for a particular inequality using the min-entropy bound might turn out to be better than the rate curve obtained by using the loose von Neumann entropy bound (from Equation 94).

To wrap up the analyses in the asymptotic regime, we present the

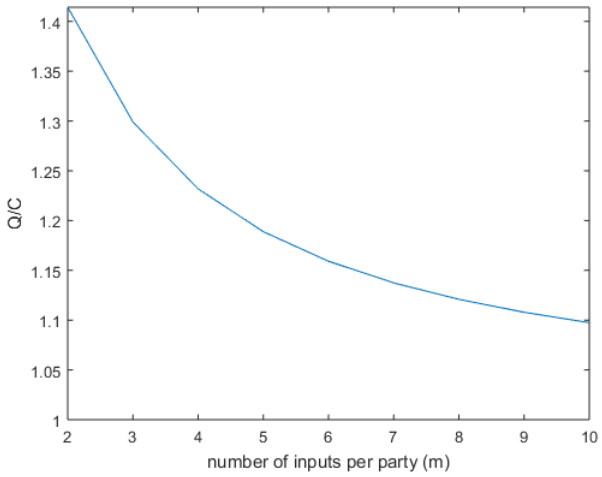


Figure 5: $\frac{Q}{C}$ versus number of inputs (m) plot for the Chained inequality for m ranging from 2 to 10.

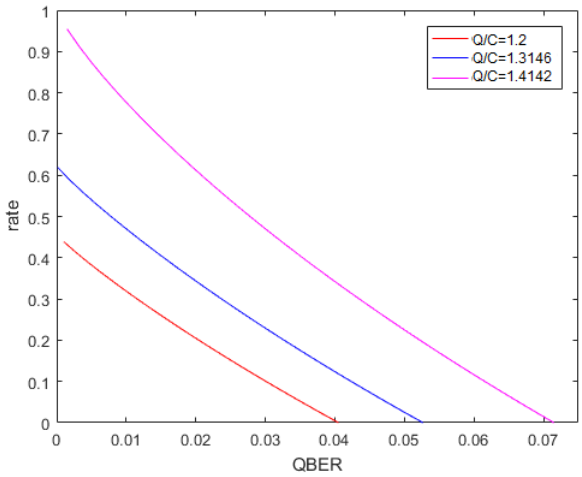


Figure 6: Rate versus noise tolerance using the bounds defined for von Neumann entropy for different values of $\frac{Q}{C}$.

Note that for the α–CHSH inequality at $\alpha = \cos\left(\frac{\pi}{8}\right)$, $\frac{Q}{C} \approx 1.3372$.

rate curve for a particular inequality from the group of α–CHSH in Figure 7. It can be seen that for very low value of QBER, surely min-entropy turns out to be a better alternative to bound the rate curve for the α–CHSH inequality, at $\alpha = \cos\left(\frac{\pi}{8}\right)$. However, for high noise regime, the bound that we have derived for the von Neumann entropy turns out to be the better alternative over min-entropy, both in terms of maximum rate achievable and noise tolerance. This improvement, however, is not enough to outperform the maximum rate and

noise tolerance values attainable by using CHSH inequality and the associated tight von Neumann entropy bound.

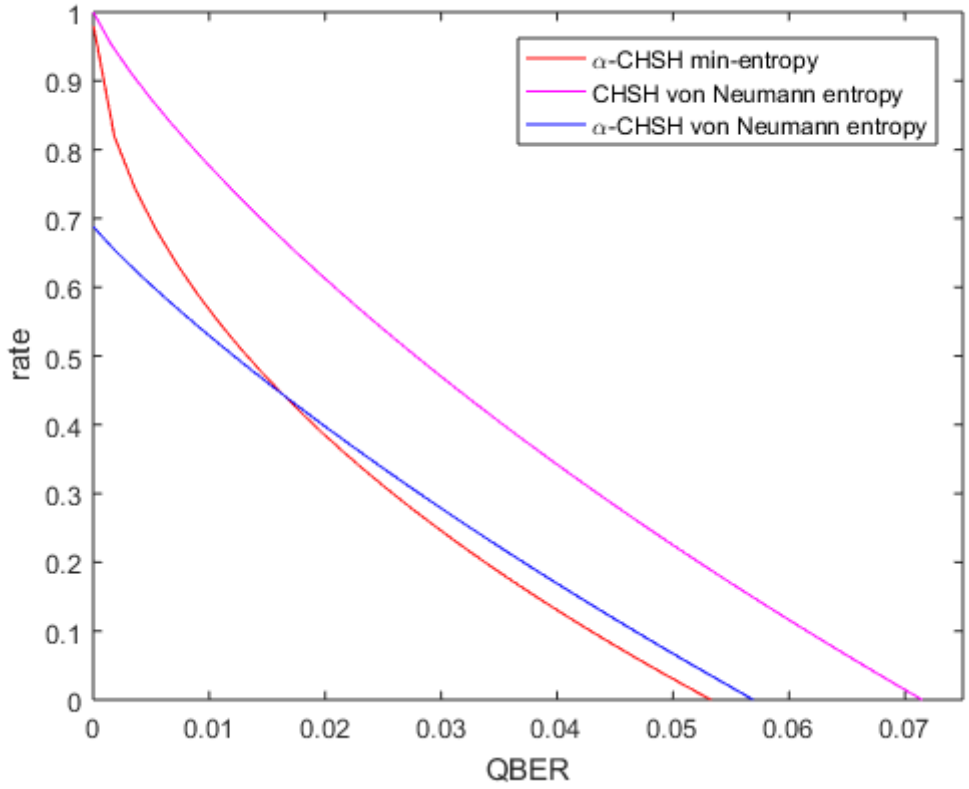


Figure 7: Rate versus QBER plot comparisons of α—CHSH inequality, at $\alpha = \cos(\pi/8)$ (red curve shows the rate curve bound by min-entropy, blue curve shows the rate curve bound by von Neumann entropy) with CHSH inequality (by using only its von Neumann entropy).

Apart from the key rate analyses done so far, we would like to look at yet another lower bound for $H(A \mid E)$ which has been derived in [KR14]. Since this bound is applicable only for inequalities with two outcomes per party, we can use it to compare it with the von Neumann bound that we have derived for the inequalities considered in this chapter. As per the derivation by Kim and Ruskai in [KR14], it can be said that

We would like to thank Ernest Tan from ETH Zurich for pointing out the result in [KR14] to us.

$$H(A \mid E) \geqslant 2 - 2^{(1 - H_{min}(A \mid E))}. \tag{96}$$

Now, plugging this into the overall lower bound on the rate, which is given by:

$$rate \geqslant H(A \mid E) - h\Big(\frac{1-\nu}{2}\Big), \tag{97}$$

it can be seen that this other bound on $H(A \mid E)$ is clearly better than the min-entropy bound. Additionally, the bound in Equation 96 does better than the bound that we have defined on the von Neumann entropy for inequalities with a $\frac{Q}{C}$ ratio that is much lesser than $\sqrt{2}$. We show this through the plots in Figure 8, wherein we choose an

inequality that we have already used to plot results before, i.e. the α–CHSH for $\alpha = \cos\left(\frac{\pi}{8}\right)$. However, as the $\frac{Q}{C}$ ratio for a Bell inequality, with two-outcomes per party, starts approaching $\sqrt{2}$, the bound that we have defined on the von Neumann entropy turns out to give better rate and noise tolerance in the high noise regime. To show this, we once again pick the α–CHSH inequality, but this time with $\alpha = 0.98$. The relevant plots can be seen in Figure 9.

Let us now focus once again only on the bound derived on the von Neumann entropy, but this time in the finite key regime.

3.4 KEY RATE ANALYSES IN THE FINITE KEY REGIME

As already mentioned in Section 1.5, recall that the key rate analysis that we are taking into account is in lines with the original entropy accumulation theorem that has been specified in the main text of [AFRV16].

Key rate analysis in a truly Device Independent sense was first performed and reported in [AFRV16]. In this section, we first introduce the parts of the protocol from [AFRV16] that will be modified with the application of each of the different groups of Bell inequalities. Next, the analysis in finite regime is performed in the sense as to what implications these modifications hold.

Firstly, let us recall the expression for the rate curve from Equation 13, which is based on equation 7 and 24 of [AFRV16]:

$$\begin{aligned} &\text{rate} \geqslant f[\eta] - \text{leak} - \gamma \cdot f_1(d) + \mathcal{O}\Big(\frac{1}{\sqrt{n}}\Big); \\ &\text{where} \quad f[\eta] = \eta - \frac{k}{\sqrt{n}}\Big(f_2(d)) + \| \nabla\eta \|\Big). \end{aligned} \tag{98}$$

Since in this chapter we are considering only the Bell inequalities with two outcomes per party, the value of d is, naturally, equal to 2.

In the above equation, k denotes a value that is very close to 2; and f_1 and f_2 are functions of the number of outcomes d per party. Also, $\| \nabla\eta \|$ denotes the first derivative of η with respect to p, which is the probability of getting correlated outcomes. Recall from Section 1.5 that η in the above equation is very much related to the conditional entropy $H(A \mid E)$.

For the inequalities that have been considered in this chapter, the function η can be expressed in terms of the bound that we have derived and presented in Equation 95.

$$\begin{aligned} \eta &= 1 - h\Big(\frac{1 + \sqrt{(\frac{Q}{C} \cdot \nu)^2 - 1}}{2}\Big). \\ &= 1 - h\Big(\frac{1 + \sqrt{(\frac{S_\lambda}{C})^2 - 1}}{2}\Big). \end{aligned} \tag{99}$$

Now, the part that shall contribute towards a change in the key rates with a change in choice of inequalities includes the definition of the expression for η. Among the α–CHSH, $\alpha\beta$–CHSH, α–MagicSquare, α^2–MagicSquare, α^3–MagicSquare and Chained inequalities, the highest value for η is attained for the CHSH inequality. So the maximum rate achievable, noise tolerance and least number of rounds required

for all other inequalities in these groups will not be any better than those for the CHSH inequality. To give a quantitative view of this, we present as an example the comparative plots of an α—CHSH inequality and CHSH inequality in Figure 10.

So far, we have inspected the use of such two-outcome Bell inequalities in asymptotic as well as finite regimes that are maximally violated by a maximally entangled two-qubit state. In the next chapter, we look at a class of two-outcome Bell inequalities whose inequality expressions are violated maximally by non-maximally entangled two-qubit states.

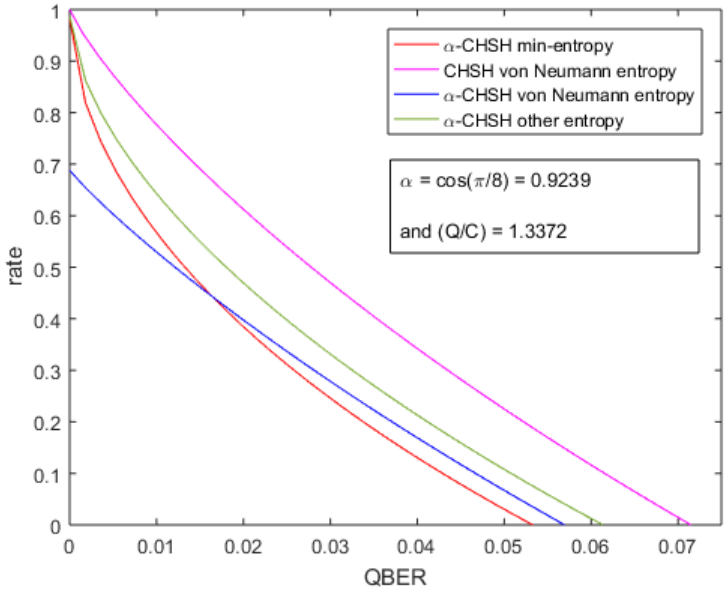


Figure 8: Rate versus QBER plot comparisons of α—CHSH inequality, at $\alpha = \cos\left(\frac{\pi}{8}\right)$ (red curve shows the rate curve bound by min-entropy, blue curve shows the rate curve bound by von Neumann entropy, and green curve shows the rate curve bound by the entropy in Equation 96).

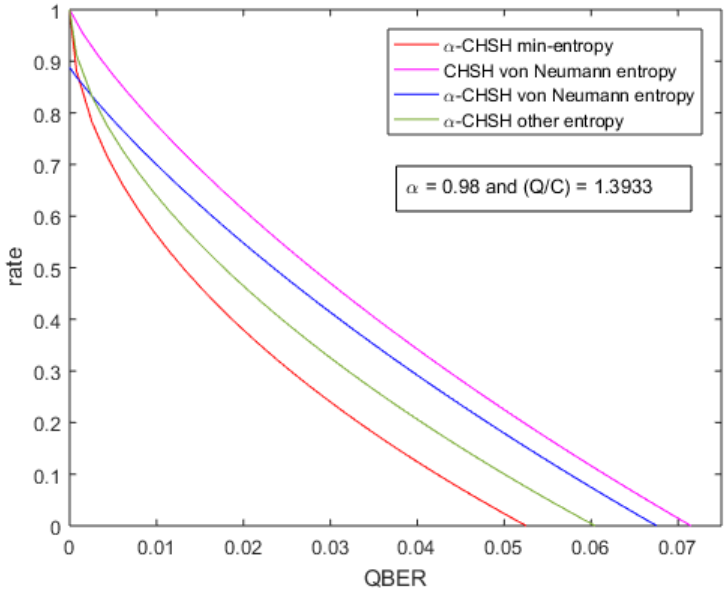


Figure 9: Rate versus QBER plot comparisons of α—CHSH inequality, at $\alpha = 0.98$ (red curve shows the rate curve bound by min-entropy, blue curve shows the rate curve bound by von Neumann entropy, and green curve shows the rate curve bound by the entropy in Equation 96).

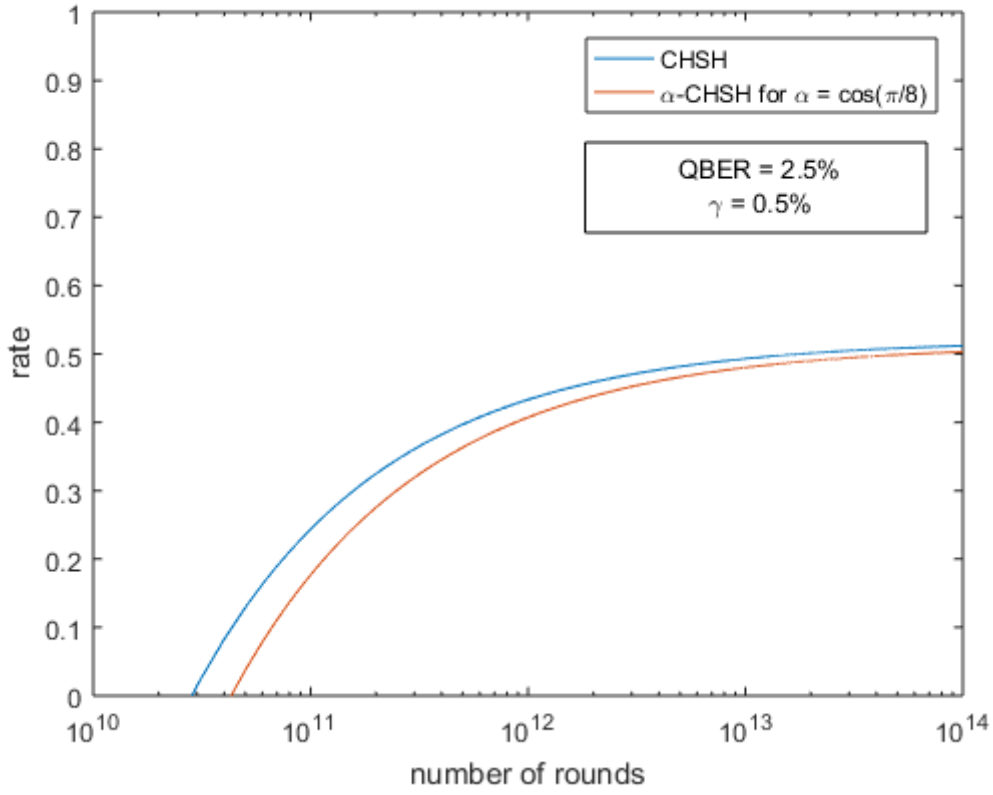


Figure 10: Comparison between Rate and minimum rounds required by using the derived von Neumann entropy for CHSH and for $\alpha - \text{CHSH}$ at $\alpha = \cos\left(\frac{\pi}{8}\right) = 0.9239$ for a fixed QBER and proportion of test rounds, γ.

4

DIQKD USING TILTED INEQUALITIES

Chapter 3 presents the key rate analyses of DIQKD using two- outcome Bell inequalities that are maximally violated by the maximally entangled two-qubit state. While considering inequalities with two outcomes per party, it is possible to achieve the maximal quantum violation using the maximally entangled state because the expression for these inequalities involves only full correlators (i.e. terms like $\langle A_x B_y \rangle$), and no single marginals. In this chapter, we will make use of a class of Bell inequalities that, once again, have two outcomes per party, but additionally, the inequality expression comprises of a marginal as well. In literature, these inequalities are called the tilted inequalities [BP15]. The work in [AMP12] conjectures that these inequalities can be used for optimal key rate generation in DIQKD by using almost-local correlations in the scenario involving the almost separable state. In this chapter we elaborate further upon that argument and show that the scenario involving the use of almost-local correlations brings along with it a heavy penalty from the error correction phase. This penalty from the error correction term is so large that the key cannot be achieved by arbitrarily separable states.

The first section gives a general description of the class of inequalities under consideration. In the next section the rate curves are computed and a detailed explanation is provided on why these inequalities are not a good alternative for achieving optimal key rates in DIQKD.

4.1 GENERAL DESCRIPTION OF TILTED INEQUALITIES

The general form of the expression of tilted inequalities, as introduced in [AMP12], is given as follows:

$$I_{\text{tilted}} : \alpha \cdot \langle A_1 \rangle + \beta \cdot \langle A_0 B_0 \rangle + \beta \cdot \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle; \quad \text{where } \alpha \geqslant 0; \ \& \ \beta \geqslant 1. \tag{100}$$

The scenarios with $\alpha < 0$ and/or $\beta < 1$ are equivalent to the ones described in Equation 100 with appropriate shuffling in the measurement and operation settings.

From the point of view of parameters of our interest, namely, maximum key rates attainable, noise tolerance and least number of rounds required, setting β to be equal to 1 imparts some sort of symmetry and thus, turns out to be a better case than the cases where $\beta > 1$. Therefore, we shall fix the parameter β in Equation 100 to be 1. Thus, the expression for this restricted class of inequalities becomes:

$$I_{\text{tilted}} : \alpha \cdot \langle A_1 \rangle + \langle A_0 B_0 \rangle + \langle A_0 B_1 \rangle + \langle A_1 B_0 \rangle - \langle A_1 B_1 \rangle; \quad \text{where } \alpha \geqslant 0. \tag{101}$$

Also, we have seen in case of $\alpha\beta-$CHSH inequalities of how the optimal choice for DIQKD is, in fact, the scenario with $\alpha = \beta = 1$.

A striking feature of the tilted inequalities is that with the inclusion of the single marginal $\langle A_0 \rangle$, the inequality is able to achieve a min-entropy of 1 for a partially entangled state. At this point, Eve can

guess Alice's outcome with a probability of only $\frac{1}{2}$, which is the least value that the guessing probability can procure for binary outcomes. The amount of entanglement in a state that facilitates complete randomness depends on the coefficient α of the single marginal. The classical bound of the expression in Equation 101 is equal to $2 + \alpha$. Now, the inclusion of the single marginal in the expression for the inequality helps ensure that the maximum quantum violation be attained by a non-maximally entangled state. Specifically, it is possible to define some angle θ as a function of α, such that the state $\cos\theta\,|00\rangle + \sin\theta\,|11\rangle$ maximally violates the inequality. The relation between this angle θ and the coefficient α can be stated as:

$$\alpha = \frac{2}{\sqrt{1 + 2\tan^2 2\theta}}. \tag{102}$$

Also, the maximum quantum value that can be achieved by the expression in Equation 101 is equal to $\sqrt{8 + 2\alpha^2}$. The optimal setting of operators to attain this maximal value is given as:

$$\begin{aligned} A_0 = \sigma_x;\ A_1 = \sigma_z; \\ B_0 = \cos\mu\,\sigma_z + \sin\mu\,\sigma_x; \\ B_1 = \cos\mu\,\sigma_z - \sin\mu\,\sigma_x; \\ \text{where } \tan\mu = \sin 2\theta; \\ \text{and } \sigma_z,\ \sigma_x \text{ are Pauli Z and X matrices respectively.} \end{aligned} \tag{103}$$

In the next section we will put forth the implications of the setting described in this section, and in turn, the results obtained by exploring the use of tilted inequalities for DIQKD.

4.2 DIQKD USING TILTED INEQUALITIES

As seen in earlier chapters, the lower bound on the rate in the asymptotic regime is given by:

$$\text{rate} \geqslant H(A \mid E) - EC. \tag{104}$$

Eve's guessing probability, given by p_{guess} in the equation alongside can be computed using the NPAHierarchy script in the QETLAB package [Joh03].

The first conditional entropy (i.e. the one specifying the entropy of Alice's state conditioned on Eve's knowledge) is bounded by the min-entropy in the following manner:

$$H(A \mid E) \geqslant H_{min}(A \mid E) = -\log_2(p_{guess}). \tag{105}$$

Bob's choice of measuring in the X-basis during error correction (for Alice's fixed measurement in the X-basis) will result in optimal error correction term for such a case.

The next term quantifies the amount of information to be communicated from Alice to Bob as part of error correction. Now, irrespective of the value of α, the optimal choices for the operators A_0 and A_1 in this case are always σ_x and σ_z, respectively. The operator A_0 is fixed for Alice as the same as what she uses for the inequality (i.e. σ_x). This fixed operator that she has projects her state onto the X-basis when she measures it for the error correction phase. In such a case, as Bob is free to choose a basis for error correction, he will pick the X-basis as well. The main goal for them is to keep the amount of error correction information to be sent as minimal as possible. And Bob fixing

his operator B_2 to σ_x helps ensure that there's maximum correlation between Alice and Bob's outcomes during the error correction phase. Considering that for $|\psi_\alpha\rangle = \cos\theta\,|00\rangle + \sin\theta\,|11\rangle$, Alice and Bob share the following two-qubit state:

$$\rho_\alpha = \nu \cdot |\psi_\alpha\rangle\langle\psi_\alpha| + \frac{(1-\nu)}{4} \cdot \mathbb{I}, \tag{106}$$

where ν denotes the visibility of the state $|\psi\rangle$, the expression for the error correction term becomes:

$$EC = H(A \mid B) = h\Big(\frac{1 - \nu \cdot \sin 2\theta}{2}\Big). \tag{107}$$

'h' in the equation alongside denotes the binary entropy function.

It is important to note that this expression for the error correction term has been arrived upon by optimizing over all possible measurements that Bob can have.

In the equation right above (i.e. Equation 107), it is intuitive that when $\theta = \frac{\pi}{4}$ (i.e. in case of the maximally entangled state and CHSH inequality), the value of the error correction term is optimal. However, as the value of θ moves towards 0 (or even towards $\frac{\pi}{2}$ for that matter), the error correction term increases; and this is quite undesirable for the overall expression for key rates. Just to give a quantitative perspective on the value of the error correction term for different values of θ, we present the plots for different values of θ (corresponding to different values of the coefficient α in the inequality) in Figure 11.

For the CHSH inequality, Bob can choose B_2 such that the error correction is the one corresponding to $\theta = \frac{\pi}{4}$ in Equation 107.

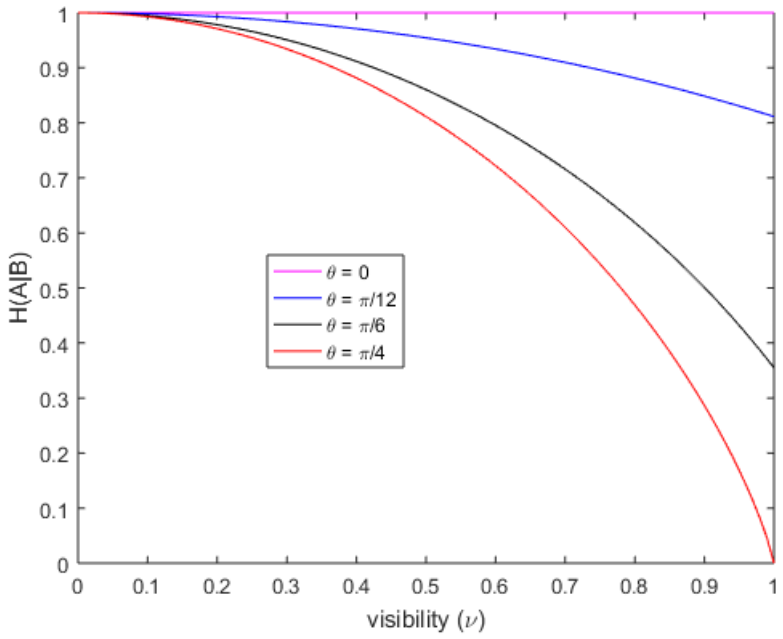


Figure 11: Error correction values for different values of θ as a function of the visibility, ν, of the state ρ mentioned in Equation 106.

Now, as $\alpha \to 2$, the state that leads to optimal violation tends to an almost-separable state. Indeed, at this point the value of the conditional entropy term, $H(A \mid E)$, in Equation 104 will be quite high,

but the value of the second term, EC, in the same same equation will also be quite high for almost all values of the visibility, v, for the state ρ mentioned in Equation 106. Therefore, all the advantage procured from a low guessing probability for Eve will be overshadowed by a lot of error correction information to be sent from Alice to Bob.

The range of values of α considered is $[0, 2]$. This is because for this range, θ ranges from 0 to $\frac{\pi}{4}$. For other range of θ, the scenario will be similar, with only the role of cosine and sine ratios in defining the state, $|\psi\rangle = \cos\theta\,|00\rangle + \sin\theta\,|11\rangle$, to be interchanged.

We browse through different values of α and compute the rates for different values of v. Later we compare the rate achievable using the tilted inequality with the rate achievable using the CHSH inequality (with the min-entropy and in another scenario with von Neumann entropy to bound the rate curve) for the best ρ_α, that was chosen for the tilted inequality. It is found that for $v > 0.99$, there is a certain range of values of α for which the maximum rate achieved by using the min-entropy bound on the rate for the tilted inequality is more than the maximum rate achieved by using the min-entropy bound on the rate for the CHSH inequality. However, the maximum rate achieved by using the von Neumann entropy bound on the rate for the CHSH inequality, is the highest, no matter what the visibility of the state be. For $v = 0.998$, Figure 12 shows such plots of the maximum rate achievable versus the value of θ corresponding to the value of α in the tilted inequality. However, with a slight increase in the value of the visibility, a drastic improvement can be observed in the rate for the tilted inequality. In Figure 13 we show the plots for maximum rate achievable at $v = 1$. For this maximum value of visibility, the rates achieved by tilted inequality are as good as the rates for CHSH inequality that are bound by the von Neumann entropy. However, it must be noted that for the overall range of values of θ (and therefore, even α) and the range of values of v, the rate achieved by using the von Neumann entropy bound of CHSH inequality is still the best.

Notice how the maximum rate attainable in Figure 12 doesn't reach 1. This is owing to the fact that v has been fixed to be 0.998.

Using an approach similar to the one used to compute the maximum rates achievable, we just check numerically the maximum noise that can be tolerated by the different tilted inequalities. It turns out that the maximum noise tolerable by the tilted inequalities is poorer than even the maximum noise tolerable by CHSH inequality (while just considering the min-entropy to bound its rate curve).

Now, these analyses pertaining to the rate and noise tolerance have been performed in the asymptotic regime. But it should be intuitive that since none of the tilted inequalities outperform the use of CHSH inequality (with the von Neumann entropy to bound the rate curve), in terms of either the rate or the noise tolerance, the tilted inequalities cannot perform better than CHSH on account of any of the three parameters (namely rate, noise tolerance and minimum number of rounds required) in the finite regime.

From the results presented in the current as well as the previous chapter, it becomes clear that in order to outperform the CHSH inequality in at least one of the three parameters (i.e. rate, noise tolerance and minimum number of rounds required), it is important that the rate

curve for a particular inequality not only has a high value for the conditional entropy ($H(A \mid E)$), but also has a low value for the error correction term. This means that Eve's guessing probability should be as low as possible; and at the same time, Alice and Bob's optimal states and measurements should facilitate as much closeness to perfect (anti-)correlation as possible.

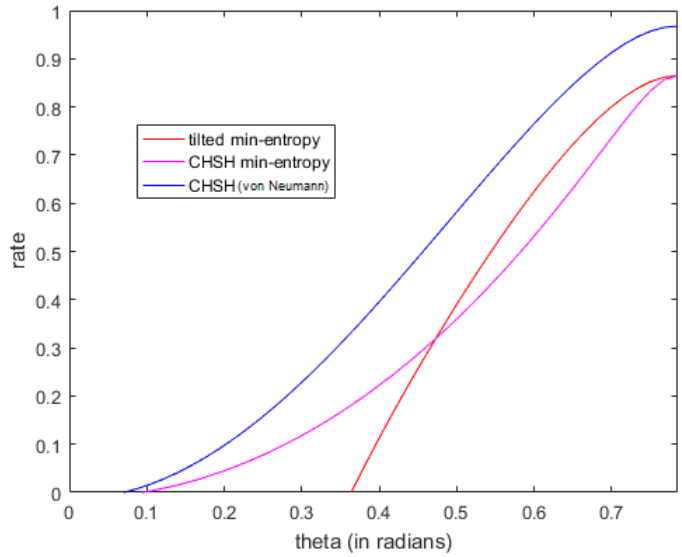


Figure 12: Rate vs θ plots for $\nu = 0.998$.

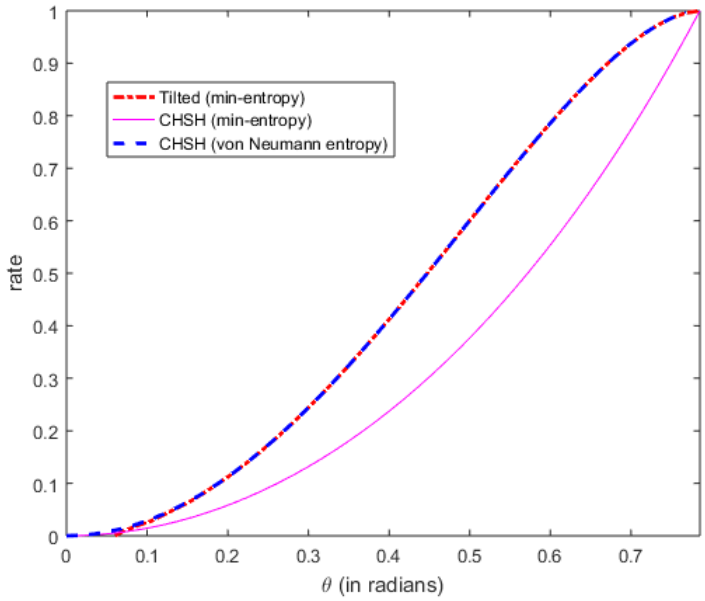


Figure 13: Rate vs θ plots for $\nu = 1$.

5

MOVING TO THREE-OUTCOME BELL INEQUALITIES

Having explored the use of Bell inequalities with two outcomes, we now focus on the use of Bell inequalities with more than two outcomes per party. Specifically, the use of three-outcome inequalities in the finite key regime is studied in this chapter. The main motivation to study the use of three-outcome inequalities lies in the fact that for such inequalities information sent in each round is in form of trits, as opposed to bits. We want to see if the advantage of better noise tolerance and key rates with an increase in the number of outcomes per party, holds for DIQKD or not. Such an advantage has already been shown to hold in case of standard QKD [SS10].

The first inequality under consideration is the CGLMP-3 inequality [Col+02]. This is a two-input and three-output inequality that achieves maximal quantum violation for a non-maximally entangled three-dimensional state. Next, we consider the three outcome Bell inequality that has been tailored to achieve maximal quantum violation using the maximally entangled two qutrit state [Sal+17], namely $\frac{1}{\sqrt{3}} \cdot (|00\rangle + |11\rangle + |22\rangle)$.

This tailored Bell inequality is a variant of the CGLMP inequality; the difference being in the coefficients of the probability terms in the expression of CGLMP inequality. These coefficients are formulated in such a way as to achieve the maximum violation using the maximally entangled state.

To define the key rate curves while using each of these inequalities, we bound the min-entropy of Alice's state conditioned on Eve's knowledge. This min-entropy is basically the logarithm (with base = 2) of the inverse of Eve's guessing probability. Therefore, for better key rates, it is desirable to have lower guessing probability. Out of the two inequalities considered in this chapter, it is observed that CGLMP-3 inequality with three outcomes has a significantly low guessing probability. In fact, this guessing probability leads to a min-entropy that is higher than the min-entropy for CHSH inequality. However, since the maximal violation for this inequality is not achieved by the maximally entangled state, the error correction term arising for this inequality is non-zero even when the state shared by Alice and Bob is the one leading to maximal violation. As such, the overall key rate analyses for these inequalities suggest that their usage does not offer any better noise tolerance. The overall rate achieved for significantly low values of noise, however, is one parameter where these multi-outcome inequalities offer an advantage. This is mainly because the raw key sent in each round now is in qudits, which amounts to $\log_2 d$ bits for a $d-$dimensional system. In the finite key regime, this has been found to hold true for CGLMP-3 and tailored-CGLMP-3 inequalities. Consequently, the requirement of the minimum number of rounds for these inequalities is lower than the requirement for CHSH inequality in the low noise regime and for lower proportion of test rounds.

In the following sections we present the key rate analyses with the use of CGLMP-3 and tailored-CGLMP-3 inequalities in the asymptotic as well as the finite key regimes.

5.1 DIQKD USING THE CGLMP INEQUALITY

In this section, first the CGLMP-3 inequality is described and the settings that help attain maximal quantum violation are specified. In the next subsection, we explore the use of CGLMP-3 in the asymptotic key regime and the final subsection deals with the use of CGLMP-3 inequality in the finite key regime.

5.1.1 *General description of CGLMP-3 inequality*

Here, the variable A_i (B_i) stands for Alice's (Bob's) outcome for an input i.

The CGLMP-3 inequality for three outcomes per party is given by:

$$\begin{aligned} \alpha \cdot [P(A_0 = B_0) + P(A_1 = B_1) + P(B_1 = A_0) + \\ P(B_0 = A_1 + 1)] - \beta \cdot [P(A_0 = B_0 - 1) + P(A_1 = B_1 - 1) \\ + P(B_1 = A_0 - 1) + P(B_0 = A_1)] \leqslant 2; \\ \text{where } \alpha = \beta = 1. \end{aligned} \tag{108}$$

Let the expression of the above mentioned inequality be denoted by I_{CGLMP}. As shown in [Aci+02; Che+06], the maximal quantum violation attained by applying this inequality to the maximally entangled two-qutrit state, $\frac{1}{\sqrt{3}}(|00\rangle + |11\rangle + |22\rangle)$, is equal to $\left(\frac{8}{3\sqrt{3}} + \frac{4}{3}\right) \approx 2.8729$. The optimal setting for this state dictates that Alice and Bob perform the following operations:

Here, $\iota = \sqrt{-1}$ and $\omega = e^{\iota \cdot \frac{2\pi}{3}}$. In fact, ω is one of the three cube roots of unity.

- For the inputs 0 and 1, respectively, Alice applies the operators that are eigenvectors of the following unitaries:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -\omega^2 & 0 \\ 0 & 0 & \omega \end{pmatrix}. \tag{109}$$

  For the inputs 0 and 1, respectively, Bob applies the operators that are eigenvectors of the following unitaries:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \iota\omega & 0 \\ 0 & 0 & -\omega^2 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & \iota\omega^2 & 0 \\ 0 & 0 & -\omega \end{pmatrix}. \tag{110}$$

Here, $U_{FT}^{\dagger}$ denotes the complex conjugate transpose of U_{FT}.

- Next, Alice applies a dicrete Quantum Fourier transform, U_{FT} and Bob applies $U_{FT}^{\dagger}$.
- Finally, they both measure in the computational basis (i.e. the generalized Z basis).

Now, as mentioned in [Aci+02], the maximum value attainable by this inequality using quantum correlations is, in fact, equal to $1+\sqrt{\frac{11}{3}} \approx 2.9149$. The state that helps achieve the quantum bound is given by $\rho = |\psi\rangle\langle\psi|$, where

$$|\psi\rangle = \sqrt{\frac{2}{11-\sqrt{33}}} \cdot \left(|00\rangle + \frac{\sqrt{11}-\sqrt{3}}{2} \cdot |11\rangle + |22\rangle\right). \tag{111}$$

Naturally, this state is a non-maximally entangled one. Also, performing a Fourier transform on the unitaries in Equation 110 means that Alice's operator A_0, which is initially in the generalized Z-basis, is projected onto a different basis after applying U_{FT}. This basis is characterized by the eigenvectors of:

Note that the clock and shift matrix in Equation 112 is a non-hermitian generalization of Pauli matrix in dimension $d = 3$.

$$A_0 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}. \tag{112}$$

Now, for the error-correction phase, Bob must measure in the basis that gives maximal correlation for the choice of unitary A_0. Here, Bob's basis is given by the eigenvectors of the unitary B_2 that he would apply during the error correction phase. Such a choice of A_0 and B_3, will modify the optimal choice of other unitaries, as well as the choice of the optimal state $\rho = |\psi\rangle\langle\psi|$. Using numerical methods, we have been able to compute an optimal quantum strategy involving A_0, A_1, B_0 and B_1 for the test rounds, and A_0 and B_2 for the key generation and error correction phase. As per this strategy, we fix the unitary A_0 to be

This is owing to the fact that the X and Z-bases are orthogonal to each other and each is an equal superposition of the other's basis states.

$$A_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}. \tag{113}$$

After fixing this, we compute the corresponding changes in the other three operators A_1, B_0, B_1 and B_2. We also compute the two-qutrit state for attaining maximum violation. This state is:

$$\begin{aligned} |\psi_{CGLMP}\rangle = \mu \cdot |00\rangle + \delta\iota \cdot |01\rangle + \delta \cdot |02\rangle \\ -\delta\iota \cdot |10\rangle + \mu \cdot |11\rangle + \delta\iota \cdot |12\rangle \\ +\delta \cdot |20\rangle - \delta\iota \cdot |21\rangle + \mu \cdot |22\rangle; \\ \text{where } \mu \approx 0.5742,\ \delta \approx 0.0427 \text{ and } \iota = \sqrt{-1}. \end{aligned} \tag{114}$$

For the choice of this non-maximally entangled state $|\psi_{CGLMP}\rangle$, and A_0 as mentioned in Equation 113, it is possible to attain the maximal value of $1+\sqrt{\frac{11}{3}}$. Thus, we have seen that the CGLMP-3 inequality is maximally violated for a non-maximally entangled two-qutrit state. We shall use the results established in this subsection to derive the rate curves in the asymptotic and finite key regimes.

5.1.2 *CGLMP-3 inequality in the asymptotic key regime*

To recall, for a generic Bell inequality, the lower bound on the key rate in the asymptotic regime (as seen in Equation 4 and Equation 5) is given by:

Here, $H_{min}(A \mid E)$ is the min-entropy and EC denotes the error correction term.

$$\text{rate} \geqslant H_{min}(A \mid E) - EC. \tag{115}$$

The min-entropy in the above equation can be computed by estimating Eve's guessing probability about Alice's state, in the following way:

$$H_{min}(A \mid E) = -\log_2(p_{guess}). \tag{116}$$

Recall that the problem specified by Equation 117 can be solved using the NPA Hierarchy function in the QETLAB package [Joh03].

The guessing probability as a function of the violation g can be computed from the following SDP problem:

$$\begin{aligned} &\text{maximize } p_{guess} = P(A_0 = 0) \\ &\text{subject to } I_{CGLMP} = g; \\ &\text{and probability distributions } P(A_0) \text{ and} \\ &\text{the distribtuion in } I_{CGLMP} \text{ follow NPA Hierarchy constraints.} \end{aligned} \tag{117}$$

Note that, I_{CGLMP} denotes the expression of the CGLMP-3 inequality and the violation g ranges from the classical bound of 2 to the quantum bound of $1 + \sqrt{\frac{11}{3}}$.

The conditional entropy in Equation 118 denotes the entropy of Alice's outcome on the knowledge of Bob's outcome for their respective inputs for key generation.

Additionally, for the error correction phase, we take into consideration Alice and Bob's outcomes for the inputs used during the key generation rounds. Therefore, the error correction term EC in Equation 115 can be specified by:

$$EC = H(A_0|B_2). \tag{118}$$

Let us consider that the two-qutrit state distributed among Alice and Bob is of the form:

$$\rho = \nu \cdot |\psi_{CGLMP}\rangle\langle\psi_{CGLMP}| + (1-\nu)\frac{\mathbb{I}}{9}, \tag{119}$$

where ν denotes the visibility of the state $|\psi_{CGLMP}\rangle$ as specified in Equation 114. Then, the value of the error-correction term in Equation 119 becomes:

$$\begin{aligned} EC = -3 \times \Big[&\Big(\mu^2\nu + \frac{(1-\nu)}{9}\Big)\log_2\Big(3 \cdot \Big(\mu^2\nu + \frac{(1-\nu)}{9}\Big)\Big) \\ &+2 \cdot \Big(\delta^2\nu + \frac{(1-\nu)}{9}\Big)\log_2\Big(3 \cdot \Big(\delta^2\nu + \frac{(1-\nu)}{9}\Big)\Big)\Big]; \\ &\text{where } \mu \approx 0.5742,\ \delta \approx 0.0427. \end{aligned} \tag{120}$$

It is extremely important to note that the scenario involved herein is still device independent. For a different choice of quantum strategy to be applied on I_{CGLMP}, there would still be a unitary B_2

that would result in maximal correlations during the error correction phase. Also, the non-maximally entangled state helping in achieving maximal value can be expressed in form of the depolarising noise model involving any arbitrary state being shared by Alice and Bob. Consequently, the error correction term would turn out to be the one in Equation 120. Considering the results established in this subsection (i.e. Equation 115 to Equation 120), we plot the key rate curve for the CGLMP inequality with 3 outcomes in the asymptotic key regime in Figure 14. It should be noted that for each inequality here, we consider the corresponding bipartite states that yield the quantum bound. Therefore, for CGLMP-3 inequality, the state under consideration is the arbitrary state mentioned in Equation 119. For CHSH inequality, the state is the arbitrary state in Equation 64. The min-entropy term

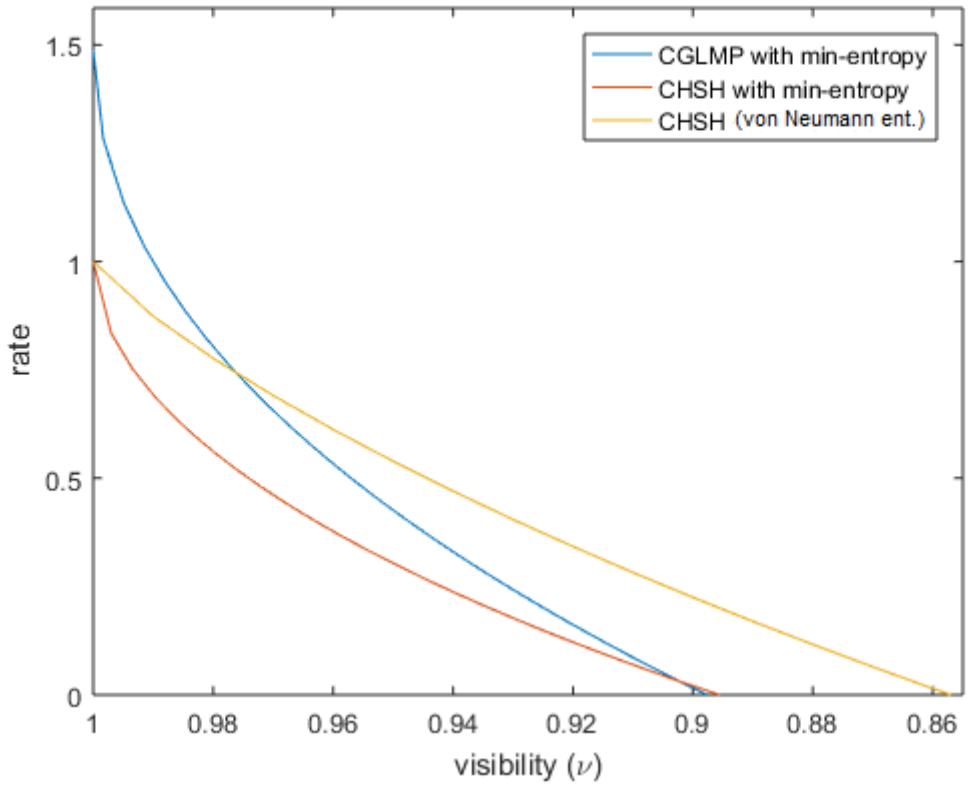


Figure 14: Comparison of rate curves using CGLMP ($d = 3$) (while considering min-entropy to bound the rate curve) and CHSH inequalities (while considering min-entropy as well as von Neumann entropy to bound the respective rate curves).

for the CGLMP-3 inequality achieves the maximum value of $\log_2 3$ at $\nu = 1$. The Y-axis in the figure above goes from 0 to $\log_2 3$; and thus, for the non-maximally entangled state that we are considering, it can be seen that even at 100% visibility of the state, there will be some error correction value subtracted from the min-entropy term. Nevertheless, for $\nu \geqslant 0.97$ the rate achieved using CGLMP inequality, with three outcomes, is better than the optimal rate for CHSH inequality. This is owing to the fact that in case of CGLMP-3 inequality here, the information transmitted is in form of trits (as opposed to bits, in

This advantage is observed thanks to the fact that in case of CGLMP-3, in every round, a trit of information is sent, as opposed to bits.

case of Bell inequalities with two outcomes per party). This notion has already been established before, in a slightly different context [HP13].

The noise tolerance, on the other hand is a parameter for which CGLMP-3 does worse than even the scenario where min-entropy is used to bound the rate curve for CHSH inequality. As can be seen in Figure 14, the noise tolerance offered by CGLMP-3 is lesser than the noise tolerance offered by CHSH inequality (considering min-entropy). As such, CGLMP-3 produces some key for a bipartite state with v, of the order of 0.899. This is significantly worse compared to the tolerance of as low as $v = 0.858$, in case of CHSH inequality. It is extremely important to recollect that for CHSH inequality we are considering a two-qubit state being shared amon Alice and Bob; whereas for CGLMP-3 inequality, we are considering a two-qutrit state being shared among them.

5.1.3 *CGLMP-3 in the finite key regime*

Firstly let us recall the expression for the rate in the finite regime from Equation 98.

$$\begin{aligned} &\text{rate} \geqslant f[\eta] - \text{leak} - \gamma \cdot f_1(d) + \mathcal{O}\Big(\frac{1}{\sqrt{n}}\Big); \\ &\text{where} \quad f[\eta] = \eta - \frac{k}{\sqrt{n}}\Big(f_2(d)) + \| \nabla\eta \|\Big). \end{aligned} \tag{121}$$

Note that this bound on the key rate is based on equation 7 in the paper [AFRV16]. Now, here, since we are looking at an inequality with three outcomes per party, the value of d will change and accordingly, the value of the functions f_1 and f_2 will also change. To study the implications of the use of CGLMP-3 inequality in the finite key regime, we bound the von Neumann entropy used to define the key rate for the CHSH inequality in [AFRV16] by the min-entropy for the CGLMP-3 inequality. The other major and significant change in the rate curve will be in the leak term where the error correction term for the maximally entangled two-qubit state is replaced by the error correction defined in Equation 120. Also, since the third term in the above equation (the one involving γ and f_1) is constant in the number of rounds n, the change in that term also turns out to be significant. The subsequent plots for CGLMP-3 in the finite regime are showcased in Figure 15 and Figure 16. From the plots of rate curves in the asymptotic regime it is evident that the advantage, if any, can be witnessed only in the low noise regime. We therefore showcase the rate curves for the visibility $v = 0.99$ of the two-qutrit state, given by Equation 114. For the purpose of compare and contrast, we present the plots for CHSH in the finite key regime for the same choice of value of v of the two-qubit state given by Equation 8.

It should be noted already that the noise tolerance offered by CGLMP-3 is much less compared to the noise tolerance offered by CHSH inequality. In terms of the rate and minimum number of rounds re-

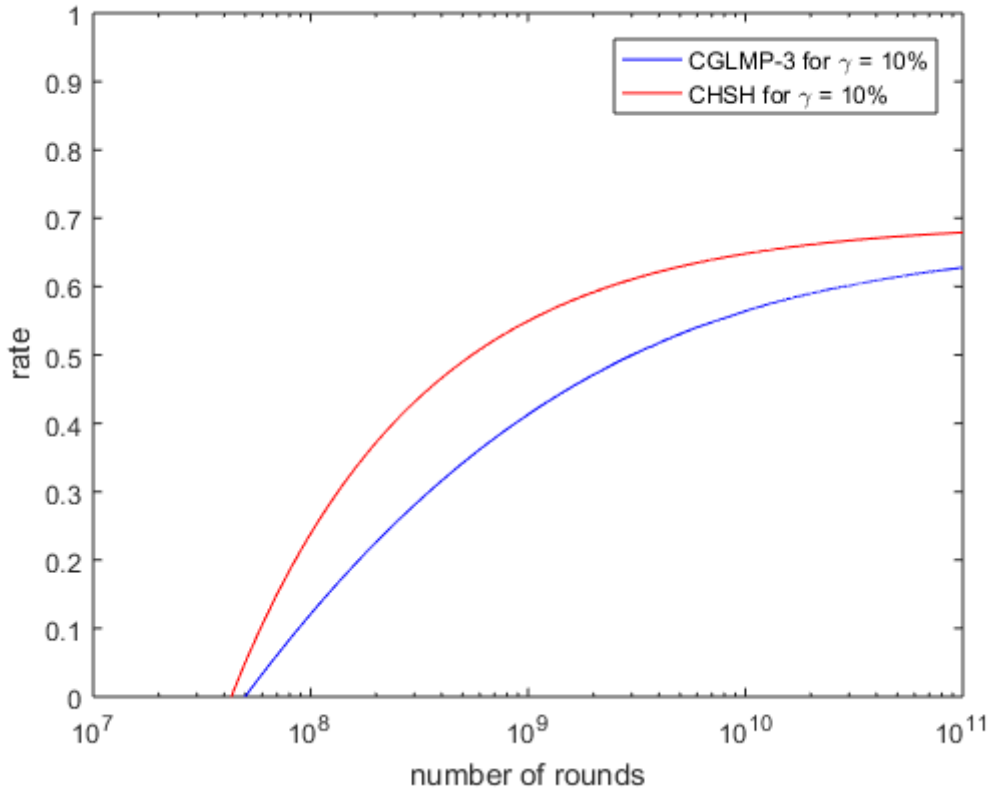


Figure 15: Comparison of rate curves for CGLMP-3 inequality (with min-entropy bound) and CHSH inequality (with von Neumann entropy bound) in the finite key regime. The proportion of test rounds is $\gamma = 10\%$ and the visibility has been set to $\nu = 0.99$.

quired, it can be observed from the plots in Figure 15 that for $\gamma = 10\%$, even in the low noise regime, the rate for CGLMP-3 is lesser than the rate for CHSH for lower number of rounds. Also, the requirement of minimum number of rounds is lesser in case of CHSH compared to CGLMP-3.

If we use a smaller fraction of rounds for testing, say $\gamma = 5\%$, then there is slight advantage observed in terms of the minimum number of rounds required for CGLMP-3 compared to the value of the same parameters for $\gamma = 5\%$. This can be seen in the plots in Figure 16. It is also evident that for lower values of n, the plot for CGLMP-3 at $\gamma = 5\%$ offers no advantage, for any parameter, over the plot for CHSH at $\gamma = 10\%$. While, we are free to choose a value of γ that gives the best results, in practice, carrying out the Bell's experiment for test rounds can be a costly affair. So if a smaller value for γ is of interest, then CGLMP-3 offers better rates and requires lesser number of rounds than CHSH in the low noise scenario. Nevertheless, looking at the overall picture and considerinng the lower values of n, CHSH is still the better alternative in terms of noise tolerance, rates and minimum number of rounds required.

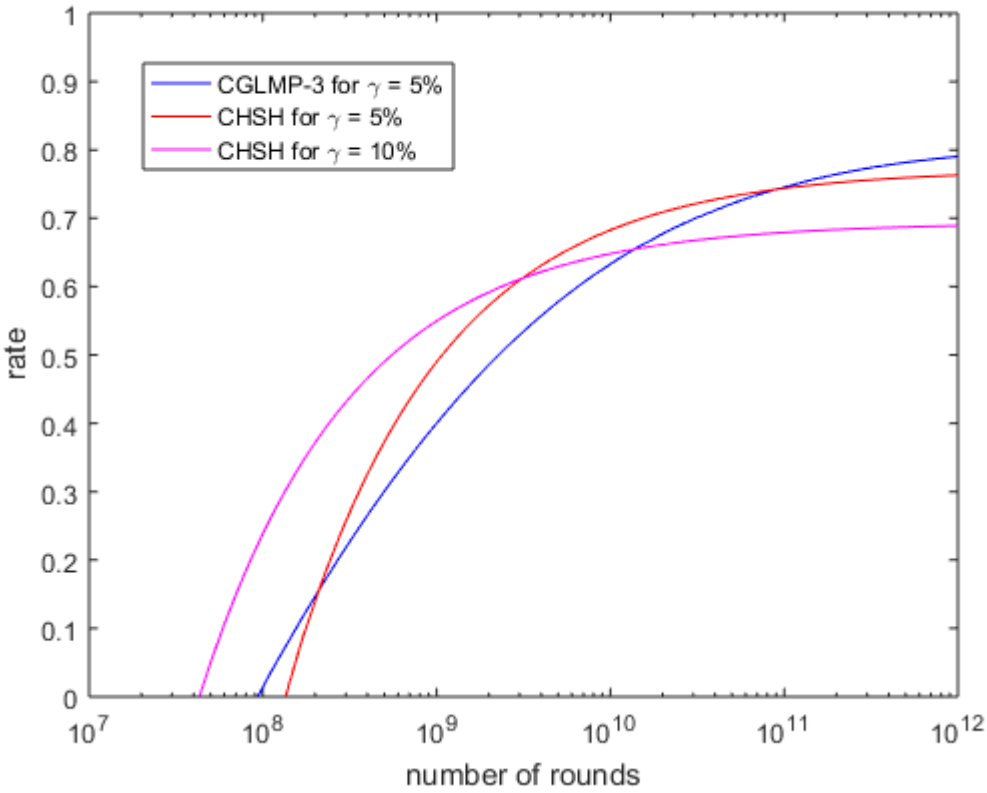


Figure 16: Comparison of rate curves for CGLMP-3 inequality (with min-entropy) and CHSH inequality (with von Neumann entropy) in the finite key regime. The proportion of test rounds is $\gamma = 5\%$ for CGLMP-3; and for CHSH curves for $\gamma = 5\%$ and $\gamma = 10\%$ are shown.

5.2 DIQKD USING THE TAILORED-CGLMP-3 INEQUALITY

In this section we explore the implications arising from the use of a three-outcome Bell inequality that has been tailored so as to achieve the maximum quantum value for the maximally entangled two-qutrit state. The generic, multi-output (d-output) and multi-input (m-input) form of this inequality has been introduced and studied in [Sal+17]. For ease of notation, we shall call the two-input, three-output scenario of this inequality as tailored-CGLMP-3 inequality.

5.2.1 *General description of tailored-CGLMP-3 inequality*

The tailored-CGLMP-3 inequality can be stated as follows:

$$\begin{aligned} \alpha \cdot [P(A_0 = B_0) + P(A_1 = B_1) + P(B_1 = A_0) + \\ P(B_0 = A_1 + 1)] - \beta \cdot [P(A_0 = B_0 - 1) + P(A_1 = B_1 - 1) \\ + P(B_1 = A_0 - 1) + P(B_0 = A_1)] \leqslant \frac{3 \cdot \cot(\pi/12) - 1}{2} - 2; \\ \text{where } \alpha = \frac{1}{6} \cdot \left[\cot\left(\frac{\pi}{12}\right) - \cot\left(\frac{5\pi}{12}\right)\right] \ \& \ \beta = \frac{1}{6} \cdot \left[1 + \cot\left(\frac{5\pi}{12}\right)\right]. \end{aligned} \tag{122}$$

We denote the expression of the above inequality by $I_{tailored-CGLMP}$. The classical bound of the expression for tailored-CGLMP-3 is equal to $\frac{3\cdot\cot(\pi/12)-1}{2} - 2 \approx 3.0981$; and the quantum bound of the same expression is 4 [Sal+17]. The operators applied to achieve the maximum quantum value are the same as in case of CGLMP-3 (specified in Equation 109 and Equation 110). The key advantage here, however, is the fact that the state that is facilitating the achievement of the maximal violation is the maximally entangled two-qutrit state:

Note that the only difference between the expressions of CGLMP-3 (Equation 108) and tailored-CGLMP-3 inequalities is in the values of the coefficients α and β. These coefficients in Equation 122 are tuned in such a way that the inequality is maximally violated by the maximally entangled state.

$$|\psi\rangle = \frac{1}{\sqrt{3}} \cdot \Big(|00\rangle + |11\rangle + |22\rangle\Big). \tag{123}$$

For the error correction phase, the choice of bases for Alice and Bob should be such that there is maximal correlation. This causes the amount of error correction information, which is to be sent across, to be the least. Now, even though the operator A_0 (as specified in Equation 112) is in the generalized X-basis, since the inequality maximally violates the maximally entangled state, during error correction, Bob can choose a unitary B_2 such that information leaked during the error correction phase is as little as possible. In the following subsections we present the results of the rate curves for the use of tailored-CGLMP-3 inequality in the asymptotic and finite key regimes, respectively.

5.2.2 *Tailored-CGLMP-3 in the asymptotic key regime*

The equation for the rate curve for this scenario is going to be the same as the one put forth in Equation 115. Additionally, the relations mentioned in Equation 116 and Equation 118 hold in this case as well. By replacing the probabilities in I_{CGLMP} with the probabilities in $I_{tailored-CGLMP}$, the SDP problem specified in Equation 117 can be used to formulate the problem to be solved.

Now, for the depolarizing noise model considered in Equation 119, where the state $|\psi\rangle$ is given by Equation 123, the error correction term is given by:

$$EC = -\Big(\frac{1+2v}{3}\Big)\log_2\Big(\frac{1+2v}{3}\Big) - 2\cdot\Big(\frac{1-v}{3}\Big)\log_2\Big(\frac{1-v}{3}\Big). \tag{124}$$

Since the qutrit state in consideration this time is the maximally entangled state, at $v = 1$, the visibility of the state is 100% and there will be maximal correlation in Alice and Bob's outcomes; therefore, no error correction information will have to be sent from Bob to Alice. By substituting $v = 1$ in Equation 124 we can see that indeed, the error correction term becomes 0.

Consequently, the rate curve in the asymptotic key regime is as plotted in Figure 17.

As can be seen, the noise tolerance offered by the use of tailored-CGLMP-3 inequality is even worse than noise tolerance offered by the use of CGLMP-3 inequality.

The advantage, that the use of this inequality to bound the rate curve has, is in terms of the maximum rate attainable. Since there is no need for error correction when the state shared between Alice and Bob is the pure, maximally entangled two-qutrit state, the maximum value

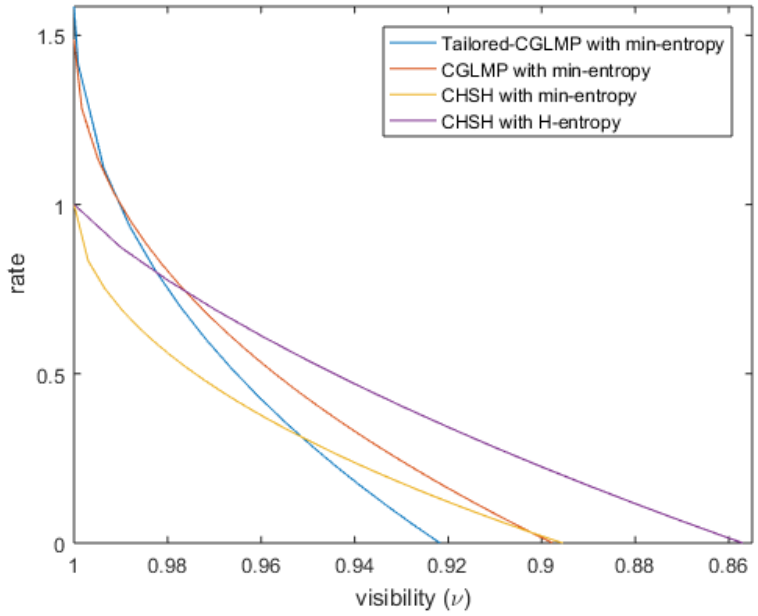


Figure 17: Comparison of rate curves using tailored-CGLMP-3, CGLMP-3 inequalities (while considering min-entropy to bound the rate curve) and CHSH inequalities (while considering min-entropy as well as von Neumann entropy to bound the respective rate curves).

For Figure 17, it is important to note that for each of three inequalities considered here, the respective states yielding the quantum bound are considered while defining the bipartite state with depolarizing noise model.

that the key rate can reach in the asymptotic regime is $\log_2 3$. However, it should be noted that the range of value of visibility for which the rate attained is better than the rate attained by considering CHSH, is merely $[0.98, 1]$.

5.2.3 *Tailored-CGLMP-3 in the finite key regime*

An approach similar to the one described for CGLMP-3 inequality in Section 5.1.3 is used to analyze the use of tailored-CGLMP-3 inequality in the finite key regime. Figure 18 showcases the resultant rate curves for the visibility ν fixed at 0.99.

The unequal coefficients for the probabilities in the expression for tailored-CGLMP-3 breaks the otherwise existing symmetry in the expression for CGLMP inequality. This, in turn, increases Eve's guessing probability and results in a shorter range of low noise regime with rates better than CHSH.

As far as the rates are concerned, for small values of n, and for high values of visibility of the state (given by Equation 119 and Equation 123), meaning for $\nu \geqslant 0.98$, the rate attained is higher than the rate attained by using CHSH inequality. Also, in this low noise regime, the minimum number of rounds required is the least for tailored-CGLMP-3 among CHSH, CGLMP-3 and tailored-CGLMP-3 inequalities.

It can be observed from the plots in Figure 18 that for larger values of n, the rates achieved using tailored-CGLMP-3 inequality are not higher than the rates achieved using CHSH inequality. Recall that these plots are for $\nu = 0.99$; and from the rate curves in the asymptotic regime (Figure 17) it is clear that the rates for tailored-CGLMP-3 inequality should plateau to a higher value than the rates for CHSH

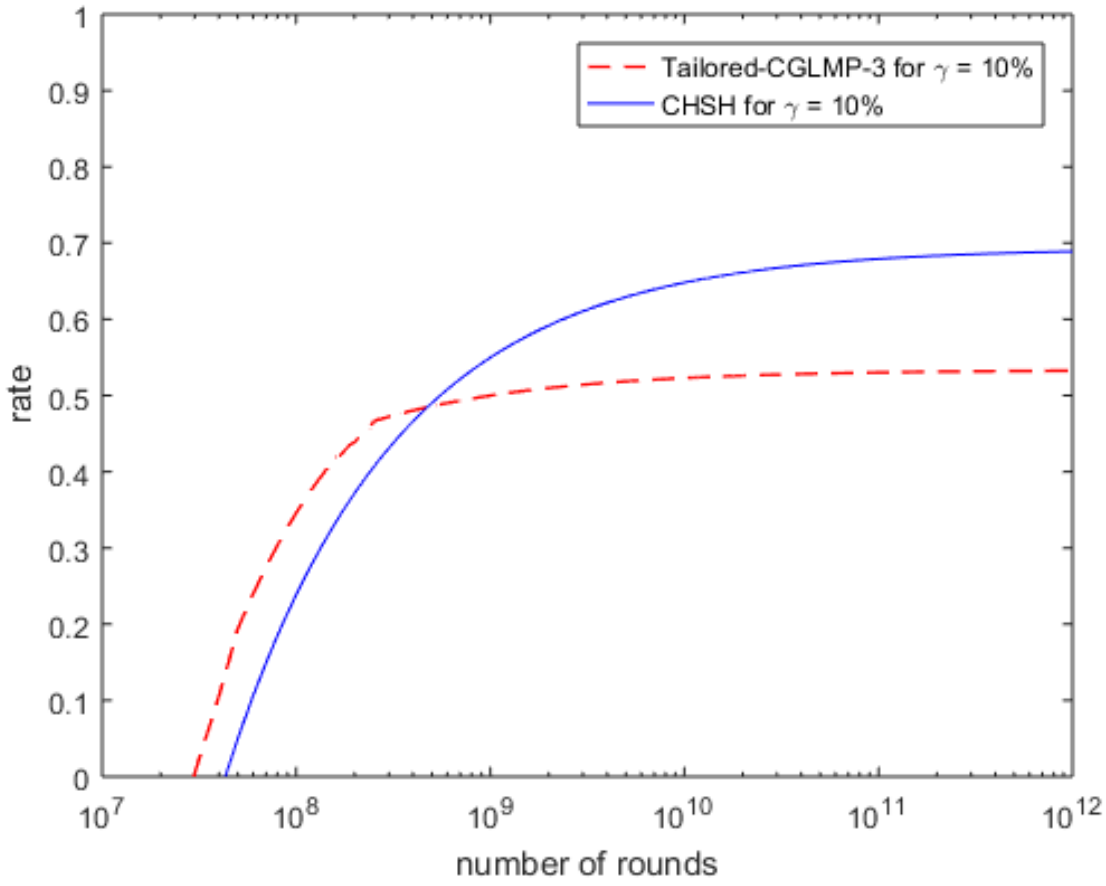


Figure 18: Comparison of rate curves for tailored-CGLMP-3 inequality (with min-entropy) and CHSH inequality (with von Neumann entropy) in the finite key regime. The proportion of test rounds is $\gamma = 10\%$, and the visibility is $\nu = 0.99$.

inequality for greater number of rounds. This observation is due to the significance of the fraction of test rounds (γ) in setting the lower bound on the rate curve in the finite regime. In figure Figure 19, we can see that tailored-CGLMP-3 evidently achieves better rate as well as has a lower requirement of minimum number of rounds, as compared to CHSH inequality. For these plots, the value of ν has been kept 0.99 and the fraction of test rounds is $\gamma = 0.1\%$.

Finally, the lowest value of visibility for which there is some positive key rate using the tailored-CGLMP-3 inequality is $\nu \approx 0.92$. Thus, the overall noise tolerance of this inequality is relatively poor compared to the scenarios involving the use of CGLMP-3 or CHSH inequality.

This concludes, the analyses using inequalities with three outcomes per party to perform device independent quantum key distribution. For the two inequalities studied, increasing the number of outcomes per party has not been advantageous in achieving better noise tolerance than CHSH. However, the tailored-CGLMP-3 inequality offers

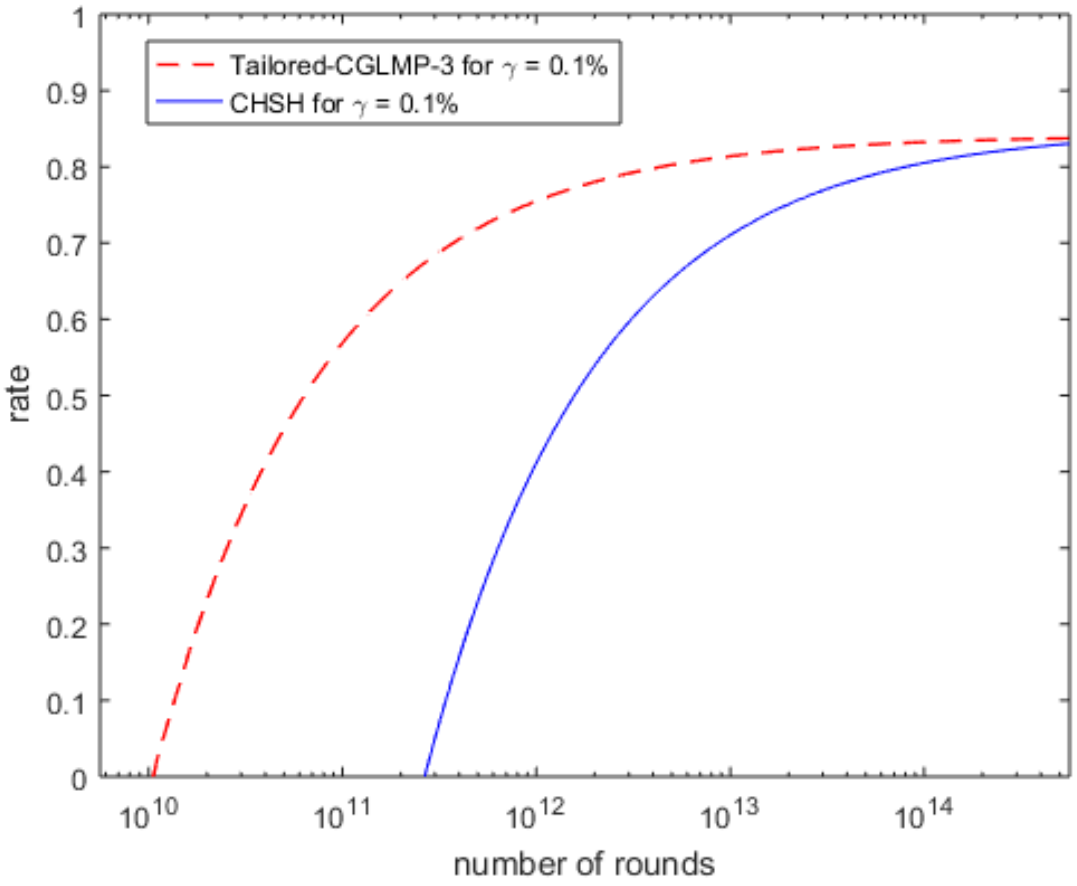


Figure 19: Comparison of rate curves for tailored-CGLMP-3 inequality (with min-entropy) and CHSH inequality (with von Neumann entropy) in the finite key regime. The proportion of test rounds is $\gamma = 0.1\%$, and the visibility is $\nu = 0.99$.

better rates and requires lesser number of rounds for key generation compared to CHSH in the low noise regime. In the following chapter, which is the concluding chapter, all the results are summarized. Also, some potential future scope is discussed.

6

CONCLUSION AND DISCUSSION

6.1 SUMMARY OF RESULTS

Use of different Bell inequalities in a DIQKD setting results in different key rate analyses. We have focused on the parameters of rate achievable, noise tolerance and minimum number of rounds required to study the suitability of applying a particular inequality in the finite key regime. In this chapter, the key results encountered so far are summarized. We end this final chapter by posing a couple open questions.

Firstly, various groups of two-outcome, bipartite Bell inequalities have been analyzed. These groups of inequalities, namely, $\alpha-$CHSH, $\alpha\beta-$CHSH, α^3-CHSH, $\alpha-$MagicSquare, α^2-MagicSquare, α^3- MagicSquare and Chained inequalities are inequalities that attain the quantum bound using the maximally entangled state. To verify this, we have derived the generic quantum bound for these groups (except for Chained inequalities, which have already been studied extensively [BC90; Weh06]), and then specified the set-up for Alice and Bob to achieve the proven quantum bound. Next, using the recipe to derive the bound on von Neumann entropy for CHSH inequality, as in [Pir+09], we have derived generic bounds on the von Neumann entropy as a function of the violation of these groups of inequalities. For inequalities with three inputs per party, the bound assumes the restriction of the system to a subspace of dimension $d = 2$. Based on the bounds that are derived, it is evident that the bound is only tight in case of CHSH inequality. In addition to this, as the ratio of the quantum bound, $\mathbb{Q}$, of an inequality to its classical bound, $\mathbb{C}$, starts waning, the bound on the von Neumann entropy starts getting loose. This affects the rate curves and renders poor results in terms of all three parameters of interest compared to CHSH inequality. And while the derived von Neumann entropy bound does offer an advantage over the min-entropy bound, especially in the high noise regime, it should also be noted that below a certain value for the ratio $\frac{\mathbb{Q}}{\mathbb{C}}$ the bound on von Neumann entropy is so low that it is better to just consider min-entropy to bound the rate curve.

Next, we look at the tilted inequalities, which are two-outcome bipartite inequalities that attain the maximum violation when using a non-maximally entangled state. For these inequalities, we use the rate curve bound by the min-entropy and find that for non-maximally entangled states, the value of the min-entropy is quite high; and as we move towards an almost separable state, the value of min-entropy for tilted inequality surpasses the von Neumann entropy value of CHSH inequality. Owing to this, it was conjectured that high key rates can be achieved for the almost-separable states. However, it is quintessen-

tial to recall that the expression for the key rate also has an error correction term. We show that for the tilted inequality, as we move from the maximally entangled state towards the separable state, the amount of information to be communicated during the error correction phase keeps increasing, thereby increasing the penalty on the error correction term in the expression for rate. Thus, the potential advantage that the tilted inequality could have offered in terms of optimal rates is also lost. However, this improvement is not enough, and for all the states CHSH is still the better option. Also, in terms of noise tolerance, tilted inequalities cannot do better than CHSH inequality. These results clearly suggest that even in terms of minimum number of rounds required, tilted inequalities are incapable of outperforming the CHSH inequality.

Finally, we switch from bipartite inequalities having two outcomes per party to bipartite inequalities having three outcomes per party. In this regard, we study and apply CGLMP-3 inequality and tailored-CGLMP-3, with the rate curves bound by the corresponding min-entropy. In the finite regime, both these inequalities perform worse compared to CHSH (with von Neumann entropy bound) on account of the parameter of noise tolerance. However, as far as the rates and minimum number of rounds are concerned, the tailored-CGLMP-3 inequality turns out to be the best choice among CHSH, CGLMP-3 and tailored-CGLMP-3 inequalities in the low noise regime. For a high noise scenario, CHSH inequality is yet again the best choice for attaining high rates and having a lower requirement of minimum rounds.

Noise tolerance is one parameter for which no improvement has been procured in the value compared to the noise tolerance of 7.1% offered by CHSH inequality. We now take a brief look at a Bell inequality with three-outcomes per party. Next, we put forth two open questions, one that arises as a result of the derivations performed in Chapter 3 and the other directly relevant to DIQKD in the finite key regime.

6.2 OPEN QUESTIONS

6.2.1 *Bell inequality with a higher $\frac{Q}{C}$ ratio than CHSH?*

For the inequalities inspected in Chapter 3 for their use in DIQKD, it was observed that the highest value of the ratio $\frac{Q}{C}$ is $\sqrt{2}$, which occurs for CHSH inequality. So is there a two-outcome, bipartite Bell inequality that is not only maximally violated by a maximally entangled state, but also has $\frac{Q}{C} > \sqrt{2}$? Or, is there a way to prove that for such Bell inequalities, the maximum value of $\frac{Q}{C}$ is $\sqrt{2}$? While the answer to this may not have direct applications immediately, but it still is an interesting riddle to solve!

6.2.2 *A potential von Neumann entropy bound for CHSH-3 inequality?*

To recall, the rate in asymptotic regime has the following lower bound:

$$\text{rate} \geqslant H(A \mid E) - EC. \tag{125}$$

For CHSH inequality, while using min-entropy to bound the rate curve, we have that:

$$H(A \mid E) = -\log_2\Big(\frac{1+\sqrt{2-2\cdot\nu^2}}{2}\Big). \tag{126}$$

And while using von Neumann entropy to bound the rate curve for CHSH inequality, the following holds:

$$H(A \mid E) = 1 - h\Big(\frac{1+\sqrt{2\cdot\nu^2-1}}{2}\Big). \tag{127}$$

Recollect that for $\rho = \nu\cdot|\phi^+\rangle\langle\phi^+| + \frac{(1-\nu)}{4}\cdot\mathbb{I}$, the parameter ν in Equation 126 and Equation 127, denotes the visibility and 'h' in Equation 127 denotes the binary entropy function.

To quantitatively see how von Neumann entropy is better than min-entropy in binding the rate curve, the corresponding plots are showcased in Figure 20.

Extending the approach used in [Pir+09], the bounds derived in

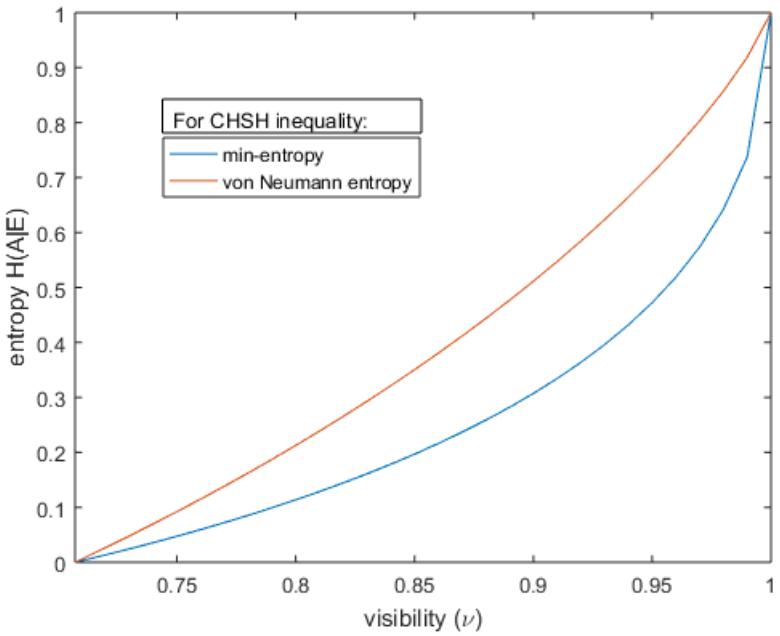


Figure 20: Plots of the quantity $H(A \mid E)$ versus the visibility ν, for the CHSH inequality.

Chapter 3 on the von Neumann entropy achieve an improvement over the min-entropy for the inequalities considered. However, this bound is not a tight bound. It becomes a good motivation to derive a bound on von Neumann entropy for other inequalities which is tight, just like the tight bound on the von Neumann entropy for CHSH inequality.

To lay a foundation in the direction of this motivation, we briefly look at a Bell inequality that is analogous to the CHSH inequality but in a field 3 subspace instead of a field 2 subspace. We shall denote this inequality as CHSH-3 inequality.

Applying the CHSH inequality, with inputs x, y and outcomes a, b for Alice and Bob respectively, is equivalent to playing a game and allocating a score of $+1$ when $a \oplus b = x \times y$ and a score of 0 otherwise. This was the case for a field 2 scenario, with two possible input options and two possible output options. Now, let us extrapolate the same premise of the game to a field 3 scenario with three input and three output options each (i.e. a, b, x, y each can take values from either 0, 1 or 2). For this scenario, if we allocate the scores of $+1$ for $a \oplus_3 b = x \times_3 y$, and 0, otherwise, then the expression for the game that arises thereby is the expression for the CHSH-3 inequality. In general, CHSH-d inequalities have been studied in depth [LLD+09; RAM16; BS15] for d possible inputs and outcomes per party.

Note that the subscript 3 denotes the application of $\mathrm{modulo}3$ *after performing the addition or multiplication operation.*

Now, since CHSH-3 inequality is quite analogous to CHSH inequality, the question we pose is: is it possible to derive a bound on the von Neumann entropy for CHSH-3 inequality which is significantly higher than the corresponding min-entropy for it? Consequently, is it possible to surpass the noise tolerance threshold that CHSH inequality has already set?

BIBLIOGRAPHY

[AMP12] Antonio Acín, Serge Massar, and Stefano Pironio. "Randomness versus nonlocality and entanglement." In: *Physical review letters* 108.10 (2012), p. 100402.

[Aci+02] Antonio Acin, Thomas Durt, Nicolas Gisin, and José I Latorre. "Quantum nonlocality in two three-level systems." In: *Physical Review A* 65.5 (2002), p. 052325.

[AFRV16] Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick. "Simple and tight device-independent security proofs." In: *arXiv preprint arXiv:1607.01797* (2016).

[BP15] Cédric Bamps and Stefano Pironio. "Sum-of-squares decompositions for a family of Clauser-Horne-Shimony-Holt-like inequalities and their application to self-testing." In: *Physical Review A* 91.5 (2015), p. 052111.

[BHK05] Jonathan Barrett, Lucien Hardy, and Adrian Kent. "No signaling and quantum key distribution." In: *Physical review letters* 95.1 (2005), p. 010503.

[BS15] Mohammad Bavarian and Peter W Shor. "Information causality, Szemerédi-Trotter and algebraic variants of CHSH." In: *Proceedings of the 2015 Conference on Innovations in Theoretical Computer Science*. ACM. 2015, pp. 123–132.

[Ben84] Charles H Bennett. "Quantum cryptography: Public key distribution and coin tossing." In: *Proc. IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*. 1984, pp. 175–179.

[BB14] Charles H Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing." In: *Theor. Comput. Sci.* 560.P1 (2014), pp. 7–11.

[BC90] Samuel L Braunstein and Carlton M Caves. "Wringing out better Bell inequalities." In: *Annals of Physics* 202.1 (1990), pp. 22–56.

[Che+06] Jing-Ling Chen, Chunfeng Wu, Leong Chuan Kwek, Choo Hiap Oh, and Mo-Lin Ge. "Violating Bell inequalities maximally for two d-dimensional systems." In: *Physical Review A* 74.3 (2006), p. 032106.

[Cir80] Boris S Cirel'son. "Quantum generalizations of Bell's inequality." In: *Letters in Mathematical Physics* 4.2 (1980), pp. 93–100.

[Cla+69] John F Clauser, Michael A Horne, Abner Shimony, and Richard A Holt. "Proposed experiment to test local hidden-variable theories." In: *Physical review letters* 23.15 (1969), p. 880.

[Col+02] Daniel Collins, Nicolas Gisin, Noah Linden, Serge Massar, and Sandu Popescu. "Bell inequalities for arbitrarily high-dimensional systems." In: *Physical review letters* 88.4 (2002), p. 040404.

[Dha+11] Chirag Dhara, Lluis Masanes, Stefano Pironio, and Antonio Acín. "Security of device-independent quantum key distribution protocols." In: *Conference on Quantum Computation, Communication, and Cryptography*. Springer. 2011, pp. 13–22.

[DFR16] Frederic Dupuis, Omar Fawzi, and Renato Renner. "Entropy accumulation." In: *arXiv preprint arXiv:1607.01796* (2016).

[Eke91] Artur K Ekert. "Quantum cryptography based on Bell's theorem." In: *Physical review letters* 67.6 (1991), p. 661.

[HP13] Marcus Huber and Marcin Pawłowski. "Weak randomness in device-independent quantum key distribution and the advantage of using high-dimensional entanglement." In: *Physical Review A* 88.3 (2013), p. 032309.

[Joh03] Nathaniel Johnston. "Introducing QETLAB: A MATLAB toolbox for quantum entanglement." In: *Quantum* 3 (2003), pp. 193–202.

[KR14] Isaac Kim and Mary Beth Ruskai. "Bounds on the concavity of quantum entropy." In: *Journal of Mathematical Physics* 55.9 (2014), p. 092201.

[LLD+09] Yeong-Cherng Liang, Chu-Wee Lim, Dong-Ling Deng, et al. "Reexamination of a multisetting Bell inequality for qudits." In: *Physical Review A* 80.5 (2009), p. 052116.

[Mas06] Lluís Masanes. "Asymptotic violation of Bell inequalities and distillability." In: *Physical review letters* 97.5 (2006), p. 050503.

[MPA11] Lluís Masanes, Stefano Pironio, and Antonio Acín. "Secure device-independent quantum key distribution with causally independent measurement devices." In: *Nature communications* 2 (2011), p. 238.

[Mer90] N David Mermin. "Extreme quantum entanglement in a superposition of macroscopically distinct states." In: *Physical Review Letters* 65.15 (1990), p. 1838.

[NPA08] Miguel Navascués, Stefano Pironio, and Antonio Acín. "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations." In: *New Journal of Physics* 10.7 (2008), p. 073013.

[Nec91] James Nechvatal. *Public-key cryptography*. Tech. rep. NATIONAL COMPUTER SYSTEMS LAB GAITHERSBURG MD, 1991.

[NSPS14] Olmo Nieto-Silleras, Stefano Pironio, and Jonathan Silman. "Using complete measurement statistics for optimal device-independent randomness evaluation." In: *New Journal of Physics* 16.1 (2014), p. 013035.

[Per90] Asher Peres. "Incompatible results of quantum measurements." In: *Physics Letters A* 151.3-4 (1990), pp. 107–108.

[Pir+09] Stefano Pironio, Antonio Acin, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. "Device-independent quantum key distribution secure against collective attacks." In: *New Journal of Physics* 11.4 (2009), p. 045021.

[Pir+10] Stefano Pironio, Antonio Acín, Serge Massar, A Boyer de La Giroday, Dzmitry N Matsukevich, Peter Maunz, Steven Olmschenk, David Hayes, Le Luo, T Andrew Manning, et al. "Random numbers certified by Bell's theorem." In: *Nature* 464.7291 (2010), p. 1021.

[RAM16] Ravishankar Ramanathan, Remigiusz Augusiak, and Gláucia Murta. "Generalized XOR games with d outcomes and the task of nonlocal computation." In: *Physical Review A* 93.2 (2016), p. 022333.

[Ren08] Renato Renner. "Security of quantum key distribution." In: *International Journal of Quantum Information* 6.01 (2008), pp. 1–127.

[Sal+17] Alexia Salavrakos, Remigiusz Augusiak, Jordi Tura, Peter Wittek, Antonio Acín, and Stefano Pironio. "Bell Inequalities Tailored to Maximally Entangled States." In: *Physical review letters* 119.4 (2017), p. 040402.

[Sch94] Steven Schwartzman. *The words of mathematics: An etymological dictionary of mathematical terms used in English*. MAA, 1994.

[SS10] Lana Sheridan and Valerio Scarani. "Security proof for quantum key distribution using qudit systems." In: *Physical Review A* 82.3 (2010), p. 030301.

[VV14] Umesh Vazirani and Thomas Vidick. "Fully device-independent quantum key distribution." In: *Physical review letters* 113.14 (2014), p. 140501.

[Weh06] Stephanie Wehner. "Tsirelson bounds for generalized clauser-horne-shimony-holt inequalities." In: *Physical Review A* 73.2 (2006), p. 022110.

SOME OF THE EASTER EGGS IN THIS DOCUMENT

Shadow block on the title page

The shadow block on the title page of this thesis is inspired from the shadow block on the cover page of the amazing book – *Gödel, Escher, Bach: an Eternal Golden Braid* – by Douglas Hofstadter. In the shadow block diagram I have tried to amalgamate ideas from two very different fields that I find very fascinating.

First of, it aims to herald the metaphysical notion of *Anekantvada* or many-sidedness. Indeed, there can be many subjective views pertaining to an idea. And these views may vary based on the variations in the perspective of the observer(s).

Secondly, since the thesis deals with quantum information theory, it can be interesting to streamline the main theme of the diagram in this direction. The block suspended in the diagram has been chosen to be such that based on the point of view (analogous to the choice of basis for measurement), one can encounter the corresponding shadow (analogous to the resultant outcome of the measurement). The three shadows aim to showcase the representations of three of the six cardinal states in a Bloch sphere. While it may be clear that the shadows on the walls stand for the $|0\rangle$ and the $|+\rangle$ states, the shadow on the floor is supposed to denote the $|+i\rangle$ state, which is orthogonal to both $|0\rangle$ and $|+\rangle$. If you viewed the shadow on the floor as 'I', then it is easy to see the analogy between this shadow representation and $|+i\rangle$. If however, you viewed the shadow on the floor as 'H', then notice how the Hadamard gate transforms the state along the Y-basis into the other state along the Y-basis (i.e. Hadamard basis transforms $|+i\rangle$ to $|-i\rangle$, and vice versa).

Emphasized words in the acknowledgements

Look closely, and you will find that the emphasized words in the acknowledgements combine together to form the phrase *Device Indepenedent Quantum Key Distribution*!

COLOPHON

This document was typeset using the typographical look-and-feel `classicthesis` developed by André Miede. The style was inspired by Robert Bringhurst's seminal book on typography "*The Elements of Typographic Style*". `classicthesis` is available for both LaTeX and LyX:

https://bitbucket.org/amiede/classicthesis/