ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ
ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΕΦΑΡΜΟΣΜΕΝΩΝ
ΜΑΘΗΜΑΤΙΚΩΝ
ΚΑΙ ΦΥΣΙΚΩΝ ΕΠΙΣΤΗΜΩΝ

ΣΧΟΛΗ ΜΗΧΑΝΟΛΟΓΩΝ
ΜΗΧΑΝΙΚΩΝ

ΕΚΕΦΕ «ΔΗΜΟΚΡΙΤΟΣ»

ΙΝΣΤΙΤΟΥΤΟ ΝΑΝΟΕΠΙΣΤΗΜΗΣ
ΚΑΙ ΝΑΝΟΤΕΧΝΟΛΟΓΙΑΣ

ΙΝΣΤΙΤΟΥΤΟ ΠΥΡΗΝΙΚΗΣ ΚΑΙ
ΣΩΜΑΤΙΔΙΑΚΗΣ ΦΥΣΙΚΗΣ

Διατμηματικό Πρόγραμμα Μεταπτυχιακών Σπουδών

«Φυσική και Τεχνολογικές Εφαρμογές»

Quantitative relations between Bell non locality and Quantum Key Distribution

ΜΕΤΑΠΤΥΧΙΑΚΗ ΔΙΠΛΩΜΑΤΙΚΗ ΕΡΓΑΣΙΑ

της Ηρώς Παπαδοπούλου

Ερευνητικοί επιβλέποντες:
Ελένη Διαμαντή
Ivan Šupić

Ακαδημαϊκος επιβλέπων
Γιώργος Βαρελογιάννης

Αθήνα, Μάρτιος 2025

Quantitative relations between Bell nonlocality and quantum key distribution

Supervisors:

Eleni Diamanti
Ivan Šupić

Co-Supervisor:

Georgios Varelogiannis

Author:

Iro Papadopoulou

Master thesis
Physics and Technological Applications

National Technical University of Athens
School of Applied Mathematics and Physical Science

NCSR Demokritos

LIP6 - Sorbonne Université

2023/2024

Dedicated to all the wonderful people of the QI team of Lip6.

Abstract

This thesis investigates the quantitative relationships between Bell nonlocality—a hallmark of quantum entanglement—and the security potential within device-independent quantum key distribution (DI-QKD). DI-QKD is a protocol in quantum cryptography that enables secure communication without trusting the underlying devices, making it reliant solely on the principles of quantum mechanics. The study begins by establishing foundational concepts, including quantum entanglement, Bell's theorem, and the critical role of nonlocal correlations in ensuring secure key distribution. A major focus is placed on understanding how varying degrees of Bell inequality violations affect DI-QKD, particularly examining whether minimal nonlocality levels suffice for cryptographic security. By exploring methods for quantifying nonlocality and introducing novel interpretations, the thesis demonstrates that even small amounts of nonlocality can be sufficient for secure key generation. Additionally, a new metric for nonlocality is proposed, potentially enhancing the precision of security assessments in DI-QKD. This work thus provides insights into the entanglement requirements of secure quantum communication, expanding the theoretical framework of DI-QKD and its applicability to real-world cryptographic protocols.

Contents

1 Introduction

1.1 Entanglement

1.1.1 Entanglement of pure states

Quantum physics is characterised by unique properties that separate it from classical physics. One of them is **entanglement**. Quantum entanglement is one of the most distinctive features of quantum theory. It was first described by Einstein, Podolsky, and Rosen in 1935 [Ein] and later by Schrödinger, who introduced the term "entanglement". The presence of entangled states arises from the superposition principle and the structure of the state space in multipartite systems. Entanglement is a very valuable resource for many applications of quantum information and computation, such as quantum state teleportation [Hug+21] and quantum key distribution [Wol]. A composite system is in an entangled state if its overall state cannot be represented as a tensor product of individual states corresponding to its subsystems.

A composite quantum system of n qubits can be described by a state $|\psi_n\rangle$, which corresponds to a unit-norm vector in a Hilbert space, that has a form of a tensor product of n single system Hilbert spaces. In some cases, this state can be written in the form:

$$|\psi_n\rangle = |q_1\rangle \otimes |q_2\rangle \otimes ... \otimes |q_n\rangle \,.$$

Then, the state $|\psi_n\rangle$ is called **separable**. However, sometimes the state of the composite system cannot be written as the tensor product of its component systems. Then, we call the state $|\psi_n\rangle$ **entangled**.

For example, the pure bipartite state $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle)$ is separable, since it can be written as:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |01\rangle) = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |0\rangle \otimes |1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle \otimes (|0\rangle + |1\rangle))$$

On the other hand, the state $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle$ is entangled, because it cannot be written as a tensor product of the component states. As a result, measurement outcomes on the entangled subsystems lead to correlations, that cannot be observed in classical physics.

1.1.2 Entanglement of mixed states

We can generalise the above for mixed states, which can be seen as a statistical ensembles of pure states. If a mixed state $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ acting on a Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2 \otimes ... \otimes \mathcal{H}_N$ can be written as:

$$\rho = \sum_\lambda p_\lambda {\rho_1}^\lambda \otimes {\rho_2}^\lambda \otimes ... \otimes {\rho_N}^\lambda \qquad\qquad \sum_\lambda p_\lambda = 1$$

then it is **separable**. If not, then it is **entangled**.

1.1.3 Quantifying entanglement

To quantify entanglement means to measure the amount or degree of entanglement present in a quantum state. In other words, to assign measurable, numerical values to the amount of entanglement in a quantum system. This allows us to indicate how strong the entanglement in a system is, as well as to compare entangled quantum states. Unlike classical correlations,

entanglement does not have a single, universal measure; instead, various entanglement measures are used depending on the system's context, the nature of the entanglement, and the application. Here are some widely-used methods and concepts for quantifying entanglement:

- Entanglement of formation [Woo]: This measure quantifies the amount of "resource" needed to create a particular entangled state, specifically referring to the minimum number of Bell pairs required to produce the state through local operations and classical communication (LOCC).
- Distillable entanglement [Rai] : This measure represents the amount of pure entanglement that can be extracted from a mixed entangled state through LOCC. It's useful for understanding how much "usable" entanglement can be harnessed from a given quantum state.
- Negativity [Qua] : This measure is used mostly for mixed states, and it shows how "non-positive" the partial transpose of a state's density matrix is. For separable states partial transpose always creates a positive matrix, thus negative partial transpose indicates entanglement. If the partial transpose of a bipartite density matrix has negative eigenvalues, the state is entangled, and the sum of the absolute values of these negative eigenvalues defines the negativity.

It is important to note that there are many measures of entanglement, however they are not all equivalent. That means that it is possible to have two different measures of entanglement that give contradictory results in certain cases.

1.1.4 Monogamy of entanglement

A very important property of entanglement, used in quantum cryptography, is the **monogamy of entanglement**; If two systems are maximally entangled with each other, then they cannot be entangled with any other system.

In other words: If two qubits A and B are maximally quantumly correlated, they cannot be correlated at all with a third qubit C. This property is purely quantum: in the classical world, if A and B bits are perfectly correlated, then there is no constraint on correlations between bits A and C. We can also state this backward: In order for two qubits A and B to be maximally entangled, they must not be entangled with any third qubit C whatsoever. Even if A and B are not maximally entangled, the degree of entanglement between them constrains the degree to which either can be entangled with C.

1.2 Bell Non-locality

1.2.1 Bell experiment

Entanglement was first introduced as a challenge to the completeness of quantum theory. The famous EPR paper [Ein] presented an entangled state that suggested either a violation of the Heisenberg uncertainty principle or the need for faster-than-light information transmission. To resolve this paradox, Einstein, Podolsky, and Rosen proposed "hidden variables" that would provide specific values for measurement outcomes, completing the theory.

Thirty years later, John Bell examined models that assume local hidden variables, where measurement outcomes are both predetermined (reality) and unaffected by events at distant locations (locality). Bell's theorem [Bel] demonstrated that such models impose limits on

correlations in measurement outcomes, formalized in Bell inequalities. Importantly, Bell showed that quantum mechanics violates these inequalities, revealing that no local hidden variable theory can replicate quantum correlations.

In a Bell experiment, two or more spatially separated parties—typically called Alice and Bob—perform measurements on a shared entangled state and record their outcomes. Each party has a set of possible measurement choices, denoted by $x \in \{0, \cdot, n_A - 1\}$ for Alice and $y \in \{0, \cdot, n_B - 1\}$ for Bob. The measurement outcomes are represented as $a \in \{0, \cdot, m_A - 1\}$ for Alice and $b \in \{0, \cdot, m_B - 1\}$ for Bob. The results of a Bell test are summarized in the set of joint probabilities $P = \{p(a, b|x, y)\}$, known as the behavior, which characterizes the experiment. These probabilities are used to calculate the Bell expression $I = \sum_{a,b,x,y} \beta_{a,b,x,y} p(a, b|x, y)$, which is then compared to the Bell inequality bound $I \leq \beta_L$, where β_L represents the classical bound for theories compatible with local hidden variable models.

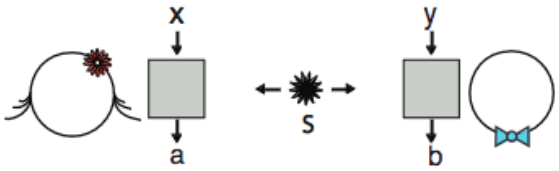

Figure 1: Bell experiment

Alice and Bob can violate Bell inequalities by performing measurements $\{M_{a|x}\}$ and $\{N_{b|y}\}$, respectively, on their shared entangled state ρ_{AB}. The probability of obtaining the outcomes (a, b) for measurement inputs (x, y) is given by the Born rule $p(a, b|x, y) = \text{Tr}\left[M_{a|x} \otimes N_{b|y} \rho_{AB}\right]$. To explore the local hidden variable (LHV) bound and quantum violation, let's consider the simplest bipartite Bell inequality, the Clauser-Horne-Shimony-Holt (CHSH) inequality, applicable when $n_A = n_B = m_A = m_B = 2$. This is know as $(2, 2, 2)$ Bell scenario, indicating that it involves two parties, each one measuring one of two possible measurements, and each measurement having two possible outcomes. The CHSH expression is $\langle A_0, B_0\rangle + \langle A_0, B_1\rangle + \langle A_1, B_0\rangle - \langle A_1, B_1\rangle$, where each correlator $\langle A_x, B_y\rangle$ is calculated as $\langle A_x, B_y\rangle = \sum_{a,b} (-1)^{a+b} p(a, b|x, y)$. Each correlator $\langle A_x, B_y\rangle$ must lie between -1 and 1. To find the maximal value for this expression under LHV theories, we rewrite it as $a_0 \cdot (b_0 + b_1) + a_1 \cdot (b_0 - b_1)$, with a_x and b_y being predetermined outcomes, that can take values -1 and 1. The value is maximised by choosing $a_0 = a_1 = 1$, which reduced the LHV bound of the CHSH inequality to $2b_0$, which is maximised when $b_0 = 1$, implying the local bound is equal to 2. So we have that:

$$\beta_{\text{CHSH}} = \langle A_0 B_0\rangle + \langle A_1 B_0\rangle + \langle A_0 B_1\rangle - \langle A_1 B_1\rangle \leq 2$$

Quantum mechanics, however, allows this inequality to be violated. If Alice and Bob share the maximally entangled Bell state $|\phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$ and measure the observables σ_X and σ_Z (Alice) and $\frac{\sigma_X + \sigma_Z}{\sqrt{2}}$ and $\frac{\sigma_X - \sigma_Z}{\sqrt{2}}$ (Bob), they observe the maximal quantum violation, known as the Tsirelson bound, which is equal to $2\sqrt{2}$.

1.2.2 Geometrical interpretation

The correlations $p(ab|xy)$ can be represented as points on the probability simplex. We are interested in three types of correlations: The local, the quantum and the non-signaling correlations.

- **Local correlations**: They can be explained by local hidden variables and respect what classical physics predicts. Correlations $p(a, b|x, y)$ are said to be local if they allow for a decomposition

$$p(a, b|x, y) = \int d\lambda p(\lambda) p(a|x, \lambda) p(b|y, \lambda),$$

where λ is the shared hidden variable. In local correlations outputs a and b are functions only of the hidden variable λ and the respective input. The set of local correlations forms a polytope. It is the smallest set of the three that we examine. It is bound by **Bell inequalities**. Bell inequalities are mathematical formulations that define the boundaries between what can be described by a local hidden variable model and what cannot.

- **Quantum correlations**: They can be explained by quantum mechanics. Correlations $p(a, b|x, y)$ are said to be quantum if there exists a quantum state $|\psi\rangle$ and measurements $M_{a|x}$ and $N_{b|y}$ such that

$$p(a, b|x, y) = \langle\psi| M_{a|x} \otimes N_{b|y} |\psi\rangle .$$

The set of quantum correlations is convex. It includes the local set but also extends beyond it. It is larger than the local set, since it allows correlations that violate Bell inequalities.

- **Non-signaling correlations**: This is the most general type of correlations that respect the non-signaling principle. Correlations $p(a, b|x, y)$ are said to be no-signalling if they satisfy relations

$$\sum_a p(a, b|x, y) = \sum_a p(a, b|x'.y), \qquad \forall x, x'$$
$$\sum_b p(a, b|x, y) = \sum_b p(a, b|x.y'), \qquad \forall y, y'.$$

These constraints rule-out non-physical behaviours in which Alice and Bob can signal to each other instantaneously by simply choosing different inputs. They can be much stronger than quantum correlations, but they still prevent faster-than-light communication. The non-signaling set is also a polytope and it includes the quantum set.

In Figure 2 we can see the representation of the three sets described above on the probability vector space.

In Figure 3 we see how the 3 sets form when we examine the case of 2 players with 2 inputs and 2 outputs. The facet inequality is the CHSH inequality, with the local bound 2, as shown in the previous section. The maximum possible violation is $2\sqrt{2}$, called Tsirelson's bound.

1.2.3 Quantifying Nonlocality

A common choice for quantifying nonlocality is through the amount of violation of a Bell inequality. This method compares how much a given correlation exceeds the bounds set by a Bell inequality. However, direct quantification based on Bell inequality violations can be problematic, because a given Bell inequality can be written in many equivalent ways using the normalization conditions.

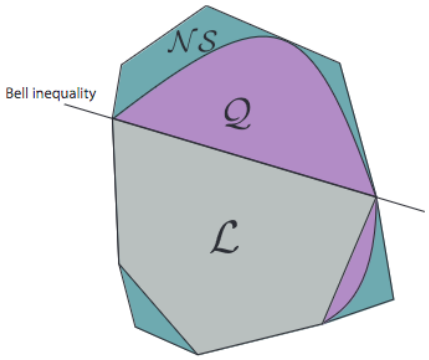

Figure 2: Local (L), Quantum (Q) and Non-signaling (NS) sets.

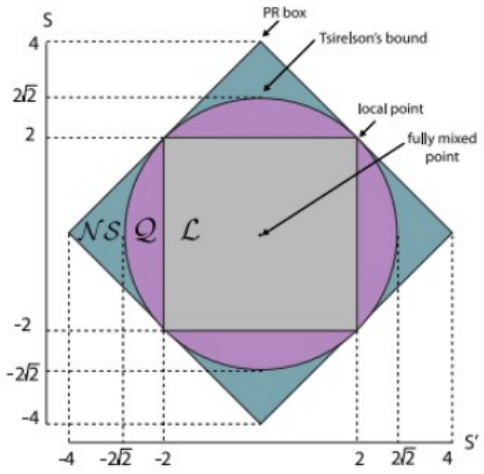

Figure 3: Local, Quantum and Non-Signaling sets for the $2 \times 2 \times 2$ scenario

1.3 Self testing

Self testing is a device independent certification technique for quantum systems. We will explore the term through an example.

Two players, Alice and Bob, each have a device, modeled as a black box; it takes an input and returns an output, without knowing the underlying mechanism. A source transmits some physical systems that may or may not be entangled to Alice and Bob. Alice may perform a number of possble settings $x = 0, 1, ...$ to her part and Bob may perform a number of possible settings $y = 0, 1, ...$ to his part. These are the inputs they give to their devices. The results, or outputs, are the possible outcomes, $a = 0, 1, ...$ for Alice and $b = 0, 1, ...$ for Bob.

Alice and Bob try different inputs and repeat their experiment many times, so they collect statistics. They can now estimate the correlations $p(a, b|x, y)$; the probabilities to see the outcomes a and b, given the inputs x and y.

As we mentioned before, Alice and Bob treat their devices as black boxes: They observe the results given the known inputs without knowing the underlying physics of their experiments. This approach is called **Device Independent** Scenario [Wol]. Interestingly, even with such little knowledge, Alice and Bob can still claim if the source emmits entangled particles or not. The key is to use a Bell inequality and check if there is a violation.

A Bell inequality consists of a function I of the probabilities $p(a, b|x, y)$. If the source is

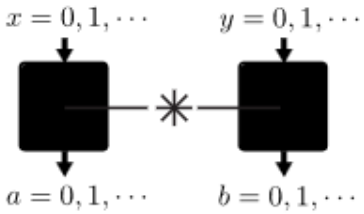

Figure 4: Alice and Bob's devices, with possible inputs and outputs

producing separable (non entangled) particles, then we are in the local case and we have;

$$I(p(a, b|x, y)) \leq \beta_L$$

However, Bell inequalities can be violated by entangled sources, so as ;

$$I(p(a, b|x, y)) > \beta_L$$

So Alice and Bob, after collecting their statistics, compare the correlations against Bell inequalities and if they find a violation, then there exist quantum correlations and the source distributes entangled particles.

Furthermore, it is possible for Alice and Bob not only to verify the entanglement, but also to identify the entangled state. This can happen if there is a maximal violation of the Bell inequality. This procedure is called **device independent self-test** or simply **self-test** of the state [ŠB20]. Self testing is interesting because we can identify the entangled state $|\psi\rangle$ purely from the probabilities of different outputs based on chosen inputs.

One limitation of self-testing is that it cannot precisely determine the exact quantum state ρ'. Instead, what can be certified is that the state ρ' is equivalent to $|\psi\rangle$ up to a local **isometry**. The first reason for this is the fact that different states that are locally unitarily equivalent can lead to the same measurement statistics when subjected to local operations. The second reason is that the existence of uncorrelated degrees of freedom on which measurements act trivially cannot be detected through measurement statistics. Exactly composing local basis change and appending uncorrelated degrees of freedom constitute a local isometry.

A local isometry Φ is a mathematical operation that preserves the entanglement structure of a state up to local transformations on each subsystem, without affecting the correlations between the parties involved.

So, we can prove that the two states are related by a suitable local isometry $\Phi = \Phi_A \otimes \Phi_B$:

$$\Phi(\rho') = |\psi\rangle \langle\psi| \otimes \rho_{\text{junk}}$$

where ρ_{junk} represents the state of the uncorrelated degrees of freedom. Let us give a formal definition of a self-test.

Definition 1. *Let $p(a, b|x, y)$ be the set of probability distributions observed in an experiment where two parties choose measurement settings x and y and obtain outcomes a and b, respectively. Then, $p(a, b|x, y)$ constitutes a self-test for the target state $|\psi\rangle$ and target measurement operators $M_{a|x}$ for and $N_{b|y}$ if the following conditions hold:*

- *Existence of an Isometry: There exists a local isometry $\Phi = \Phi_A \otimes \Phi_B$, such that, for any physical state $|\psi'\rangle$ and measurement operators $M'_{a|x}$ and $N'_{b|y}$ that reproduce the observed probabilities it holds*

$$\Phi(|\psi'\rangle) = |\psi\rangle \otimes |junk\rangle\,, \tag{1}$$

where junk is a normalized quantum state;

- *Equivalence of Measurement Operators: Under the isometry* Φ *measurement operators* $M'_{a|x}$ *and* $N'_{b|y}$ *map to the ideal measurement operators* $M_{a|x}$ *for and* $N_{b|y}$.

1.4 Randomness in quantum physics

We are interested to know when a given process, represented by a device or black box in the user's hands that produces bits, generates "good" randomness. High-quality random bits are crucial in various fields, especially in cryptography for secure key generation and transmission, where weak randomness can lead to vulnerabilities. There lies our interest in randomness. Beyond cryptography, random numbers are also essential for accurate simulations in scientific research, unbiased statistical sampling, and effective algorithms in computer science and machine learning. The pursuit of reliable randomness enhances security, accuracy, and performance across multiple applications, making it a significant area of research.

N bits are perfectly random if they are unpredictable, not only to the user of the device, but to any observer. By demanding that the results should look random to any observer, the generated randomness is guaranteed to be private: the user, by running the process in a secure location, has the guarantee that nobody knows the obtained results, which can later be safely used for cryptographic purposes.

No process can be truly random, because of the unfalsifiable hypothesis of the existence of a super-deterministic model. In such a model, everything, including the entire history of the universe, would be pre-determined in advance and known to an external observer. So, the outcomes could theoretically be predicted by this external observer. Thus, any protocol for randomness generation has to be based on some hypotheses or assumptions. A random number generator (RNG) is considered to be better than another if it is based on fewer or weaker assumptions.

Generating true randomness is a complex task, and there are three main types of random number generators (RNGs):

- **Pseudo-Random Number Generators (PRNGs)**: PRNGs use algorithms and an initial random seed to produce sequences of numbers. They are fast and cost-effective but rely on assumptions about the adversary's computational power, making them less suitable for applications requiring absolute unpredictability.

- **True RNG (TRNG)**: TRNGs exploit physical processes that are hard to predict to generate random numbers. Such can be meteorological phenomena or the mouse movements of a computer user.

- **Quantum Random Number Generators (QRNGs)**: QRNGs utilise quantum processes believed to be fundamentally random.

A typical example of a quantum random number generator (QRNG) involves measuring the clicks from a single photon hitting a beam-splitter.

As seen in figure 5, a single photon is emitted from a source. This photon will be used to determine the random bit. The single photon is directed towards a beam-splitter with a transmission coefficient of 1/2. This beam-splitter divides the incoming photon into two possible paths. There are two single-photon detectors placed at the two outputs of the beam-splitter. Each detector registers whether a photon has arrived in its path. According to quantum mechanics, the photon has an equal probability of traveling down either path due to the 50% transmission coefficient of the beam-splitter. Consequently, each detector has

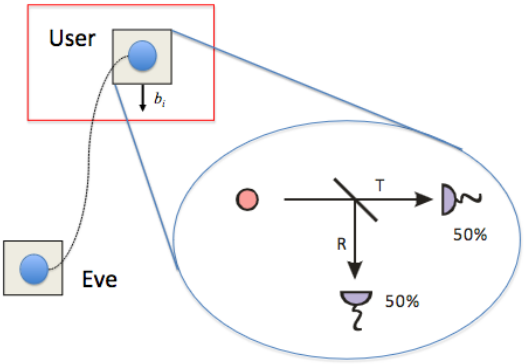

Figure 5: Quantum randomness generation

an equal chance of detecting the photon. The outcome of which detector clicks (or doesn't) is inherently probabilistic and generates a random bit. The randomness arises from the quantum superposition of the photon's paths and is fundamentally unpredictable. That means that if an eavesdropper (Eve) were to observe, they wouldn't get information about the bit, because the measurement outcomes are not determined until they are observed, and before observation, they are in a superposition state. Furthermore, if Eve measures, they would disturb the state and be detected.

However, achieving this ideal scenario in practice is challenging due to device imperfections and potential memory effects. Also, the user needs to trust their device in terms of quantum origin and privacy. Device-independent quantum random-number generators (DIQRNGs) address the previous challenges by providing certified randomness based solely on broad assumptions like the validity of quantum physics. DIQRNG is a framework for producing random bits without relying on the trustworthiness of the specific devices used in the process. Instead, it utilizes the statistical properties of measurement outcomes obtained from entangled quantum states shared between two parties, typically named Alice and Bob. By performing measurements that violate Bell inequalities, DIQRNG ensures that the generated randomness is secure and certified, independent of any assumptions about the internal workings of the devices. This approach offers a quantum advantage, as quantum randomness is inherently more unpredictable than classical randomness, providing stronger guarantees against potential biases or flaws. DIQRNG has significant implications for secure communications and cryptographic protocols, enabling the generation of secure keys for encryption and enhancing privacy.

2 Quantum Key Distribution

2.1 Classical cryptography

Cryptography, the act of sending secret messages, goes back to ancient times, at least 4000 years ago. It was introduced probably around 2000 BC by ancient Egyptians, who used hieroglyphics to decorate tombs of deceased kings. The ancient Chinese also constructed a written language to encrypt the meaning of words. However, in both of those cases, even though the information was encrypted, it was not intended to be kept secret. There have been references of many civilisations sending secret messages, usually during times of war. Some of them are the Mesopotamians, the Babylons, the Assyrians and the Greeks. The Indians used alphabetic substitutions in their messages. The Spartans used a long strip of papyrus which they wraped around a staff of a specific diameter to write their message. Then they would unwrap the papyrus and send it with a messenger. In order to read the message, the receiver had to wrap the strip around a staff of the same diameter. Julius Ceasar used a cryptographic system that displaced each letter of the alphabet to the second next.

Of course, cryptography has evolved throughout the years. A modern example is the assumed unbreakable Enigma Code, used by the Germans during World War II. Eventually, it was decoded by the British and, most famously, Alan Turing.

In cryptography, the goal is to transmit a secret message from party A, usually noted as Alice, to party B, usually noted as Bob. In order for them to do so, without anyone eavesdropping, traditionally called Eve, they need a key to encrypt and decrypt the messages. A key, in general, is a set of rules that transform the original message to ciphertext and vice versa. Since we usually want to transmit a message in the form of a bit string, it makes sense for the key as well to be a sequence of 0s and 1s. Once Alice and Bob both hold the (same) key, they can exchange privately messages through a process called **one-time pad**. It has as follows:

Alice wants to send a message $M = (M_1, M_2, ..., M_n)$ of length n to Bob. Alice and Bob have created a pair of keys S_A, S_B, each of length n. The message and the keys are binary strings.The length of the key has to be at least equal to the length of the message.

1. Alice encrypts the message M with her key S_A. To produce the ciphertext she performs binary addition: Each digit of the key is added to the corresponding bit of the message.

   $C_i = M_i \oplus (S_A)_i$

2. Alice sends the ciphertext $C_i = (C_1, C_2, ..., C_n)$ to Bob, through a public channel. Generally, Eve has access to the ciphertext but cannot alter the message.

3. Bob decodes the message by doing binary addition of the ciphertext C_i and his key S_B.

   $M_i = C_i \oplus (S_B)_i$

Given that the keys are identical, Bob, after decoding the ciphertext, holds the original message M_i sent by Alice.

So we have:

$$message \oplus key = ciphertext$$
$$ciphertext \oplus key = (message \oplus key) \oplus key = message$$

It is important that the keys are truly random and are used only once, to secure the privacy of the message. Of course the keys have to remain completely secret from third parties. In addition, Alice and Bob should be honest. That is, they follow the decided protocol precisely.

2.2 Quantum cryptography

Classical cryptography has a disadvantage when it comes to creating a pair of keys. The keys of Alice and Bob should be truly random, completely secret (to ensure security) and correct (Alice's key has to be the same as Bob's). However, this is hard to be done when physical distance lies between them. If they were to meet, they could just exchange the message itself and public communication channels carry the risk of eavesdropping. In addition, even if they produced and distributed the key, today's quantum computers pose a threat to break the cryptographic code.

Naturally, it was a matter of time before scientists tried to solve those problems using principles of quantum mechanics. Thus, quantum cryptography or quantum key distribution (QKD) was born. Alice and Bob can now take advantage of quantum properties to create a private key between them using a public channel. The security of the key is guaranteed and, furthermore, if Eve interferes, she will be detected, so Alice and Bob abort the process.

The first QKD protocol was developed in 1984 by Charles Bennet and Gilles Brassard and is known as the **BB84 protocol** [BB84] . It can be summarised as follows:

1. Alice chooses two random binary bit strings $a = (a_1, a_2, a_3, ..., a_{4n})$ and $b = (b_1, b_2, b_3, ..., b_{4n})$.

2. She encodes the bits of a into the computational basis if the corresponding bit in b is 0 and into the Hadamard basis if the corresponding bit in b is 1. This results in a 4n block of qubits:

$$|\Psi\rangle_A = \bigotimes_{i=1}^{4n} |\psi_{a_i b_i}\rangle$$

   Each of the individual qubits is in one of the following 4 states:

$$|\psi_{00}\rangle_A = |0\rangle_A \quad |\psi_{10}\rangle_A = |1\rangle_A$$
$$|\psi_{01}\rangle_A = |+\rangle_A \quad |\psi_{01}\rangle_A = |-\rangle_A$$

   This outcome is derived like this:

a_i	b_i	basis	outcome
0	0	C	$\|\psi_{00}\rangle_A = \|0\rangle_A$
1	0	C	$\|\psi_{10}\rangle_A = \|1\rangle_A$
0	1	H	$\|\psi_{01}\rangle_A = \|+\rangle_A$
1	1	H	$\|\psi_{01}\rangle_A = \|-\rangle_A$

3. Alice sends the state $|\psi\rangle_A$ to Bob over a quantum channel ε. Bob receives 4n qubits (state $\varepsilon(|\psi\rangle_A \langle\psi|)$) and publicly announces the fact.

4. Bob measures each qubit in the Computational or Hadamard basis at random. He ends up possesing bit strings a' and b'. The first one encodes in which basis Bob measured his qubits ($a'_i = 0$ if Bob measured in the computational basis, and $a'_i = 1$ if he measured in the Hadamard basis). The bits of b' are his measurement results. Both strings have length $4n$.

5. Alice publicly announces b via the classical communication channel. This step is called *sifting step*.

6. Bob compares b to b' and announces the positions where $b_i \neq b'_i$. Alice and Bob discard the bits in a and a' for which $b_i \neq b'_i$. At this point the length is ≈2n.

7. Alice and Bob use n bits to estimate the number of errors, *i.e.* the number of bits of a and a' which are different. This way they find out the information Eve holds about the bit strings. This step is called *parameter estimation*.

8. After parameter estimation, they discard the n bits used for error estimation and keep the remaining bits. They apply *error correction* to ensure their bits match and *privacy amplification* to reduce any knowledge Eve might have. The final result is a shorter, shared secret key of length m (where $m < n$), which is secure and unknown to any potential eavesdropper.

Protocols like this, where quantum states are prepared, shared via a quantum channel and finally measured are called "**prepare and measure**" protocols.

There is another category of protocols, that exploits entanglement to create a shared key. This requires a source that provides entangled pairs of qubits (EPR pairs). Alice and Bob share an EPR pair and perform measurements each on their qubit. These protocols are known as "**entanglement-based**" protocols. One of them is the **modified Lo-Chau protocol** or **entanglement-based BB84** [Wol], which is described below.

If Alice and Bob share the maximally entangled state:

$$|\beta_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB})$$

then their state cannot be entangled with any other state, as discussed in Section 1.1.4. Thus, Eve cannot have any information about the measurement results that are obtained from this state. So, Alice and Bob need to have a sequence of $m = 2n$ of these states:

$$|\beta_{00}\rangle_{AB}^{\otimes m} = |\beta_{00}\rangle \otimes |\beta_{00}\rangle \otimes ... \otimes |\beta_{00}\rangle$$

and measure them to obtain the secret key. They will have to use an insecure quantum channel (since Eve interacts with the states and, in general, there is noise), so they will end up with a mixed state ρ and not the exact state $|\beta_{00}\rangle_{AB}^{\otimes 2n}$ they shared before. It is their mission to correct the errors that occured during the transmission of the state through the quantum channel. The protocol is as follows:

1. Alice creates $m = 2n$ EPR pairs in the state $|\beta_{00}\rangle^{\otimes 2n}$.

2. Alice randomly selects n out of $2n$ EPR pairs (check qubits) that will later be used to estimate the errors due to Eve's interference.

3. Alice selects a random classical $2n$-bit string $b = (b_1, b_2, ..., b_{2n})$. She performs Hadamard transform to her half of the EPR pair whenever $b_i = 1$.

4. She sends the other half of the qubit pairs to Bob.

5. Bob receives the qubits and publicly announces the fact.

6. Alice announces the string b and the positions of the n check qubits she selected in step 2.

7. Bob performs Hadamard transform on the qubits where $b = 1$.

8. Alice and Bob measure their check qubits in the computational basis $|0\rangle, |1\rangle$ to estimate the error rate. They publicly announce their results and if more than t errors occur, they abort the protocol.

9. If the errors are less than t, they use error correction codes in the remaining n bits. Thus they obtain $|\beta_{00}\rangle^{\otimes m}$.

10. Finally, Alice and Bob measure the m EPR pairs (state $|\beta_{00}\rangle^{\otimes m}$) in the computational basis to obtain the shared secret key.

There are many other QKD protocols, like the six-state protocol [Bru98], the SARG04 protocol [Sca+04a], the Ekert91 protocol [Eke91] and others.

2.3 Device independent Quantum Key Distribution

2.3.1 DIQKD and motivation

QKD security relies on the validity of quantum theory and the trust of each party's device. (The term device covers any equipment Alice and Bob use to either prepare or measure their qubits.) Device independent QKD (DIQKD) aims to remove the second assumption. Untrusted devices refer to the mistakes that might happen during the preparation and measurement of the qubits, but also to the possible interference of Eve.

In the DI setting we treat the devices as black boxes, without making any assumptions about their inner function. Alice's device has input x and Bob's has input y. Their devices produce outputs a and b respectively. We do not examine how the outcome is created, but the input-output statistics. The boxes are fully described by the conditional probability distribution $p_{ab|xy}$.

For most DIQKD protocols we are usually interested in the case where Alice and Bob have binary inputs and outputs. That means that $x, y, a, b \in \{0, 1\}$.

Let's use the entanglement based BB84 protocol to examine why Device Independence is powerful. Alice and Bob share a maximally entangled state:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle = \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle$$

For Alice, we have:

If $x = 0$, Alice measures in the computational basis: ($|0\rangle\langle 0| \to a = 0$ and $|1\rangle\langle 1| \to a = 1$).

If $x = 1$, Alice measures in the Hadamard basis: ($|+\rangle\langle +| \to a = 0$ and $|-\rangle\langle -| \to a = 1$).

Similarly, for Bob:

If $y = 0$, Bob measures in the computational basis: ($|0\rangle\langle 0| \to b = 0$ and $|1\rangle\langle 1| \to b = 1$).

If $y = 1$, Bob measures in the Hadamard basis: ($|+\rangle\langle +| \to b = 0$ and $|-\rangle\langle -| \to b = 1$).

By performing a number of measurements, Alice and Bob observe the following correlations:

$$p(a = b|x = y) = 1$$
$$p(a \neq b|x = y) = 0$$
$$p(a, b|x \neq y) = \frac{1}{4}$$

This means that when Alice and Bob choose the same input ($x = y$), they receive perfectly correlated outcomes and when they choose different inputs ($x \neq y$), the output is uncorrelated. These correlations can only be achieved if Alice and Bob share the maximally entangled state. So, if they observe them, they can conclude that they indeed share a maximally entangled state and, hence, their results can be used to produce a secret key.

However, in the DI setting that is not the case and the outputs cannot be used to generate a secure key! To conclude that they share a maximally entangled state, Alice and Bob had to assume the dimension of the Hilbert space of the shared state: a two-qubit space. Device Independence removes this assumption. This implies that we can find a separable state that gives the same input-output statistics as $|\phi^+\rangle$.

For example, the state:

$$\rho^{AB} = \frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|) \otimes \frac{1}{2}(|{+}{+}\rangle\langle {+}{+}| + |{-}{-}\rangle\langle {-}{-}|)$$

produces the same probability distribution when for inputs $x = 0$ and $y = 0$ Alice and Bob measure the first qubit in the computational basis and for inputs $x = 1$ and $y = 1$ they measure their second qubits in the Hadamard basis. The correlation between Alice and Bob's systems is completely local, so it is possible for Eve to hold a putification of the mixed state ρ^{AB}, that is Alice, Bob and Eve share a tripartite state:

$$|\psi^{ABE}\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle) \otimes \frac{1}{\sqrt{2}}(|{+}{+}{+}\rangle + |{-}{-}{-}\rangle)$$

One can see that by tracing out Eve's part of the tripartite state the state Alice and Bob have is exactly ρ^{AB}. This is not possible if the correlations between Alice and Bob's systems are nonlocal (they violate a Bell inequality). In the DI setting it is vital that the results violate a Bell inequality and so there are non-local correlations. That prevents Eve from having knowledge about Alice's and Bob's measurement outcomes.

It is important to state here that Eve is bound by the laws of quantum physics: we assume that the correlations that Eve can pursue are quantum.

2.3.2 Non-locality and DIQKD

Previously, we introduced the concepts of non-locality and DIQKD. Let's now see how the two are connected.

To produce a secret key, in the Device Independent setting, Alice and Bob share entangled systems. Entanglement grants correlations that belong to the quantum set and can not be explained with the hidden variable model. Then, they perform measurements on their systems. Each device has a number of settings (inputs): x for Alice and y for Bob. The outcomes (outputs) are a for Alice and b for Bob. We are examining the case where the inputs and outputs are binary ($x, y, a, b \in 0, 1$). The results of these measurements generate a set of raw data, consisting of measurement outcomes. This data forms the basis from which the cryptographic key will be extracted.

Next, they collect measurement statistics and check for non-locality (Self-testing). To achieve this they check if their results violate a Bell inequality. If they confirm a violation, they know that their systems were indeed entangled and they share non-local correlations. The communication is secure, because if Alice and Bob self-test a pure state, it means that it cannot be entangled with Eve's state (monogamy of entanglement).

Once Alice and Bob confirm the Bell inequality violation, they proceed to extract a secure key from their measurement outcomes. They perform error correction and privacy amplification (classical post-processing). After the classical post-processing steps are completed, the parties obtain a final, secure cryptographic key.

Although the nonlocality of observed correlations is essential for DIQKD, it has been proven that it is not sufficient. So a question is raised: Is there a minimum amount of nonlocality needed for any DIQKD implementation? The answer to that question is that no such bound exists. We can have quantum correlations with arbitrarily small nonlocality that can be used for DIQKD with near perfect key (1 bit of key per pair of entangled qubits).

2.3.3 DIQKD and security against attacks

A DIQKD protocol needs to be secure against attacks. There are two main types of attacks that interest us, and they are related to the way an eavesdropper interferes with the different rounds of the key extraction protocol. Let us remind that for estimating Bell inequality violation Alice and Bob repeat the measuring process many times, *i.e.* there are many rounds.

- Collective attacks: Eve applies the same attack on each particle of Alice and Bob, but no other limitations are imposed to her. In particular she can intercept the quantum states sent between Alice and Bob and perform independent measurements on each state. She can keep her systems in a quantum memory and perform a (coherent) measurement on them at any time. She analyzes each state separately without exploiting any quantum correlations between them.

- Coherent (general) attacks: Eve can act differently in each round. Eve can manipulate and measure the quantum states collectively. She can entangle the intercepted quantum states with her own systems, allowing her to perform coordinated measurements on multiple states simultaneously.

2.3.4 DI randomness generation

In the introduction we addressed the usefulness of DI in random number generation.

DIQRNG protocols make use of the correlations observed when measuring entangled particles that do not have a classical analogue, as certified by the violation of a Bell inequality.

In a general protocol for DIQRNG the user has access to $n \geq 2$ correlated devices. In figure 6 we see the most simple case of 2 parties who have inputs x and y and outputs a and b. Eve may have a system correlated with the user's devices. The randomness of one of the outputs, for example a, can be quantified by the optimal probability P_{guess} that Eve guesses it correctly, $e = a$, after performing a measurement z on her system. For quantum eavesdroppers, this guessing probability is optimized over all possible quantum preparations, including the tripartite state and measurements compatible with the correlations observed by the user. We can relax the assumption of quantum mechanics and consider eavesdroppers

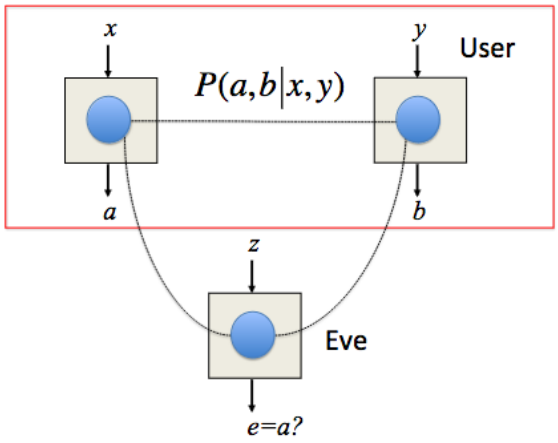

Figure 6: QIQRNG

who can prepare any tripartite correlations compatible with the no-signaling principle (no faster than light communication), even beyond quantum physics.

As said before, the user needs at least 2 devices, so that they can perform a Bell test. After N rounds of collecting data (x, y, a, b), the user calculates the probabilities $P(a, b \mid x, y)$, which can be estimated without making any assumption about the internal working of the devices (DI setting). These probabilities can be used to check if there is a violation of a Bell inequality.

A violation of: $\beta = \sum c_{abxy} P(a, b \mid x, y) \leq \beta_L$ (β_L: Local bound) points out non local correlations between the two devices.

Witnessing a Bell inequality violation guarantees that the unknown quantum state in the devices has certain entanglement (the local state of one of the devices is mixed and, thus, a measurement on it generates random outcomes) and purity (the quantum state certifies that the two devices are not too correlated with the environment or the external observer).

Finally, the Bell certification of randomness is intrinsically quantum (classical devices always satisfy a Bell inequality) and device-independent (for its computation only the observed statistics $P(a, b \mid x, y)$ is needed). The user has, however, to ensure two conditions:

- the inputs x, y should not be correlated with the devices
- there is no exchange of information between the two devices while the two distant outcomes are being generated.

3 Key from arbitrarily small non-locality

3.1 Introduction

As mentioned before, we need non-locality to have a secret cryptographic key. The work [WBC24] shows that there is no minimum amount of non-locality required to have a secret key and that it is possible to have near-perfect DIQKD with arbitrarily small nonlocality.

In the (2,2,2) scenario (2 players, 2 inputs each, 2 outputs each), a measure of non-locality is a violation of the CHSH inequality, which is the only facet inequality in this scenario.

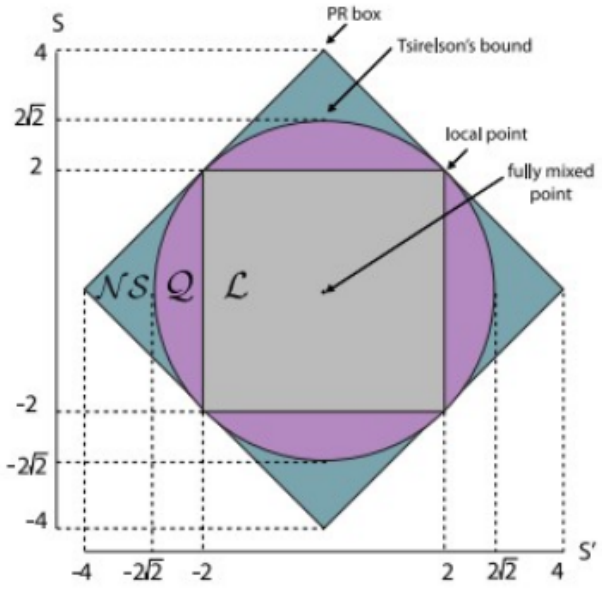

Figure 7: Enter Caption

Let us examine a violation s between 2 and $2\sqrt{2}$. In their work [WBC24], they prove that a point on the boundary of the quantum set, that corresponds to a violation s ($2 < s < 2\sqrt{2}$), is a self test not for CHSH, but for another inequality belonging to a family they introduce. This point self tests the state:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

and the measurements can be used to obtain the secret key.

3.2 Preliminaries

We are interested in the minimal Bell scenario: 2 players (Alice and Bob) with 2 inputs $a, b \in \{0, 1\}$ and 2 outputs $x, y \in \{0, 1\}$. The joint probability $p(a, b|x, y)$ that characterises the devices must be non-signaling.

A quantum strategy describes a joint quantum state $\rho_{\tilde{Q}_A\tilde{Q}_B}$ and sets of observables $\tilde{A}_x = \tilde{M}_{0|x} - \tilde{M}_{1|x}$ and $\tilde{B}_y = \tilde{N}_{0|y} - \tilde{N}_{1|y}$, where $\{\tilde{M}_{a|x}\}_a$ and $\{\tilde{N}_{b|y}\}_b$ are projective measurements. Eve holds a purification $|\Psi\rangle_{\tilde{Q}_A\tilde{Q}_B\tilde{Q}_E}$ of $\rho_{\tilde{Q}_A\tilde{Q}_B}$, aiming to learn about Alice's outcomes undetected. She tries to establish correlations with device A, so that she gains information about Alice's raw key when Alice makes measurements.

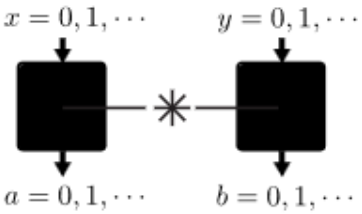

Figure 8: Alice and Bob's devices, with possible inputs and outputs

Since we are in the (2,2,2) scenario, we can quantify the non-locality of the resulting joint behaviour using its CHSH value, I_{CHSH}. We know that the local and quantum bounds are given by 2 and $2\sqrt{2}$ respectively. There is a unique quantum state and sets of measurements that achieve the quantum bound, up to local isometries: The CHSH inequality self-tests this state.

DIQKD protocols use spot-checking with two measurements per party and a single Bell inequality (e.g., CHSH) to compute the secret key rate. The key rate is determined by two conditional von Neumann entropies: $H(A|X = x, E)$, which captures the randomness of Alice's raw key conditioned by Eve, and $H(A|X = x, Y = y, B)$, which captures the reconciliation cost between Alice and Bob. The Devetak-Winter formula [DW05] provides a lower bound for the key rate:

$$r^{key} \geq \max_{x,y} \left(\inf \left[H(A|X = x, E)_{\rho_{AE|X=x}} - H(A|X = x, Y = y, B)_{\rho_{AB|X=x,Y=y}} \right] \right)$$

The global randomness rate is defined as:

$$r_{\text{global}} = \max_{x,y} \inf H(AB|X = x, Y = y, E)_{\rho_{ABE|X=x,Y=y}}$$

To attain a key rate approaching 1 bit per shared entangled state, we examine a family of three-parameter Bell inequalities. These inequalities have a maximum quantum violation that self-tests a unique state and corresponding measurements (up to local isometries). We consider a single functional $f = \langle B_{\theta,\phi,\omega} \rangle$ with observed value η, denoting the key rate as $R^{\text{key}}_{\theta,\phi,\omega}(\eta)$. Achieving the quantum bound self-tests a pure, (maximally entangled) state, therefore uncorrelated with Eve, allowing us to compute the entropy directly from the observed behaviour. We find $H(A|X = 0, E) = 1$ and $H(A|X = Y = 0, B) = \epsilon$ for any $\epsilon \in (0, 2 - (3/4)\log(3)]$, resulting in a key rate of $1 - \epsilon$ that approaches 1 as ϵ approaches 0, with a CHSH value near the classical bound. The randomness rate is denoted as $R^{\text{global}}_{\theta,\phi,\omega}(\eta)$ based on the same functional.

3.3 Methods and results

As mentioned before, we are going to use a family of self-testing Bell expresions. Let $\theta, \phi, \omega \in \mathbb{R}$. Then, we can define the following family of Bell expressions introduced in [WBC24]:

$$\begin{aligned} \langle B_{\theta,\phi,\omega} \rangle = &\cos(\theta + \phi)\cos(\theta + \omega)\langle A_0 \left(\cos\omega B_0 - \cos\phi B_1\right)\rangle \\ &+ \cos\phi\cos\omega\langle A_1 \left(-\cos(\theta + \omega)B_0 + \cos(\theta + \phi)B_1\right)\rangle \end{aligned} \tag{2}$$

The discussed family of inequalities has applications in device-independent cryptography. Additionally, this family consists of infinite hyperplanes tangent to the boundary of the

quantum set of correlations and is involved in self-testing with linear functions of correlators. In the following text we provide several lemmas allowing to analyse the usefulness of the introduced family of Bell inequalities in DI QKD.

Lemma 1. *For a given triple θ, ϕ, ω the local bound $\pm\eta^L_{\theta,\phi,\omega}$ of the inequality (2) is given by:*

$$\begin{aligned}\eta^L_{\theta,\phi,\omega} = \{&\max_{\pm} |\cos(\theta+\omega)\cos(\omega)(\cos(\theta+\phi) \pm \cos(\phi))| \\ &+ |\cos(\theta+\phi)\cos(\phi)(\cos(\theta+\omega) \pm \cos(\omega))|\}\end{aligned} \tag{3}$$

Proof. In local hidden variable models we can take $\langle A_x B_y\rangle = a_x b_y$, with a_x and b_y taking values 1 or -1 We can rearrange (2) and exchange $\langle A_x B_y\rangle = a_x b_y$ as follows:

$$\begin{aligned}\eta^L_{\theta,\phi,\omega} = &\max_{a_x,b_y\in\{\pm1\}}[\cos(\theta+\phi)\cos(\theta+\omega)(a_0(\cos\omega b_0 - \cos\phi b_1) = \\ &+ \cos\phi\cos\omega a_1\,(-\cos(\theta+\omega)b_0 + \cos(\theta+\phi)b_1)] = \\ &= \max_{a_x,b_y\in\{\pm1\}}[(\cos(\theta+\phi)\cos(\theta+\omega))(a_0\cos(\omega)b_0 - a_0\cos(\phi)b_1) + \\ &+ (\cos(\phi)\cos(\omega))(a_1(-\cos(\theta+\omega)b_0 + a_1\cos(\theta+\phi)b_1)] = \\ &= \max_{a_x,b_y\in\{\pm1\}}[b_0\{\cos(\theta+\phi)\cos(\theta+\omega)a_0\cos(\omega) - \cos(\phi)\cos(\omega)a_1\cos(\theta+\omega)\} + \\ &+ b_1\{-\cos(\theta+\phi)\cos(\theta+\omega)a_0\cos(\phi) + \cos(\phi)\cos(\omega)a_1\cos(\theta+\phi)\}] = \\ &= \max_{a_x,b_y\in\{\pm1\}}[b_0\{\cos(\theta+\omega)\cos(\omega)(a_0\cos(\theta+\phi) - a_1\cos(\phi))\} + \\ &+ b_1\{\cos(\theta+\phi)\cos(\phi)(-a_0\cos(\theta+\omega) + a_1\cos(\omega))\}]\end{aligned}$$

Then, in order to maximise the above expression, we want:

$$\begin{aligned}b_0 &= \mathrm{Sgn}\{\cos(\theta+\omega)\cos(\omega)(a_0\cos(\theta+\phi) - a_1\cos(\phi))\} \\ b_1 &= \mathrm{Sgn}\{\cos(\theta+\phi)\cos(\phi)(-a_0\cos(\theta+\omega) + a_1\cos(\omega))\}\end{aligned}$$

where Sgn is the sign function.
We have two options: $a_0 = a_1$ or $a_0 = -a_1$. So the maximum value is:

$$\begin{aligned}\eta^L_{\theta,\phi,\omega} = \max_{\pm}\{&|\cos(\theta+\omega)\cos(\omega)(\cos(\theta+\phi) \pm \cos(\phi))| \\ &+ |\cos(\theta+\phi)\cos(\phi)(\cos(\theta+\omega) \pm \cos(\omega))|\}\end{aligned}$$

□

Lemma 2. *For given θ, ϕ, ω if*

$$\cos(\theta+\phi)\cos(\phi)\cos(\theta+\omega)\cos(\omega) < 0 \tag{4}$$

then the quantum bounds $\pm\eta^Q_{\theta,\phi,\omega}$ are given by:

$$\eta^Q_{\theta,\phi,\omega} = \sin(\theta)\sin(\omega-\phi)\sin(\theta+\omega+\phi)$$

Proof. For a Bell operator B that defines the quantum Bell inequality $\langle B\rangle \leq \eta^Q$, the shifted Bell operator $\overline{B} = \eta^Q\mathbb{I} - B$ satisfies $\langle\phi|\overline{B}|\phi\rangle \geq 0$ for all quantum states $|\phi\rangle$, i.e.$\overline{B} \geq 0$.

If there exist a set of operators R_μ that satisfy: $\overline{B} = \sum R_\mu^\dagger R_\mu$ then we have found a Sum-Of-Squares (SOS) decomposition for the operator $\overline{B}$, implying $\overline{B} \geq 0$. For our scenario:

$$\overline{B}_{\theta,\phi,\omega} = c_0 R_0^\dagger R_0 + c_1 R_1^\dagger R_1$$

where the polynomials $\{R_0, R_1\}$ are defined as:

$$R_0 = \sin\theta B_0 + \cos(\theta+\phi)A_0 - \cos\phi A_1$$

$$R_1 = \sin\theta B_1 + \cos(\theta+\omega)A_0 - \cos\omega A_1$$

and the constants c_0, c_1 (for a specific value for θ, ϕ and ω) are given by:

$$c_0 = -\frac{\cos\omega\cos(\theta+\omega)}{2\sin\theta}$$
$$c_1 = \frac{\cos\phi\cos(\theta+\phi)}{2\sin\theta}$$

So the operator $\overline{B}_{\theta,\phi,\omega}$ is positive (or zero) and therefore: $B_{\theta,\phi,\omega} \leq \eta^Q$

□

By explicitly comparing the quantum and local bounds we obtain the following condition:

$$|\eta^Q_{\theta,\phi,\omega}| > \eta^L_{\theta,\phi,\omega} \Leftrightarrow (4) \text{ holds.} \tag{5}$$

Lemma 3. *If (4) holds then up to local isometries there is a unique strategy that achieves $\langle B_{\theta,\phi,\omega}\rangle = \eta^Q_{\theta,\phi,\omega}$:*

$$\rho_{QAQB} = |\psi\rangle\langle\psi|, \quad \textit{where } |\psi\rangle = \frac{|00\rangle + i|11\rangle}{\sqrt{2}},$$
$$A_0 = \sigma_X, \quad A_1 = \cos\theta\sigma_X + \sin\theta\sigma_Y,$$
$$B_0 = \cos\phi\sigma_X + \sin\phi\sigma_Y, \quad B_1 = \cos\omega\sigma_X + \sin\omega\sigma_Y$$

Proof. We want to prove that up to local isometries there is only one quantum strategy that reaches the quantum bound. We have to search over all quantum strategies without making any assumption about the Hilbert space dimension. This is a difficult task, so we use a sequence of results which will help us reduce the search.

We will need the following lemmas:

Lemma 4. *Let B be a bipartite Bell operator in the two-input, two-output scenario with a quantum bound η^Q. Suppose, for every two-qubit strategy $(\tilde{\rho}^q_{QAQB}, \tilde{A}^q_x, \tilde{B}^q_y)$ achieving $\langle B\rangle = \eta^Q$, there exist unitaries U_A on $\mathcal{H}_{QA}$ and U_B on $\mathcal{H}_{QB}$ such that*

$$(U_A \otimes U_B)\tilde{\rho}^q_{QAQB}(U_A^\dagger \otimes U_B^\dagger) = |\psi\rangle\langle\psi|,$$

$$U_A\tilde{A}^q_x U_A^\dagger = A_x, \quad \textit{and} \quad U_B\tilde{B}^q_y U_B^\dagger = B_y,$$

for a target strategy $(|\psi\rangle, \{A_x\}_x, \{B_y\}_y)$. Then, for every quantum strategy $(\rho_{\tilde{Q}_A\tilde{Q}_B}, \{\tilde{A}_x\}_x, \{\tilde{B}_y\}_y)$ achieving $\langle B\rangle = \eta^Q$, there exist unitaries V_A on $\mathcal{H}_{\tilde{Q}A}$ and V_B on $\mathcal{H}_{\tilde{Q}B}$, and a state $|\xi\rangle_{Junk} \in \mathcal{H}_{Junk}$, such that for any purification $|\Psi\rangle_{E\tilde{Q}_A\tilde{Q}_B}$ of $\rho_{\tilde{Q}_A\tilde{Q}_B}$

$$(I_E \otimes V_A \otimes V_B)(I_E \otimes \tilde{A}_x \otimes \tilde{B}_y)|\Psi\rangle_{E\tilde{Q}_A\tilde{Q}_B} = |\xi\rangle_{Junk} \otimes (A_x \otimes B_y)|\psi\rangle_{QAQB} \quad \forall x, y.$$

According to Lemma 4 if we prove that among qubit strategies there is, up to local unitaries, a single one reaching the quantum bound, then, in higher dimension, up to local isometries, there is only one quantum strategy that reaches the quantum bound. Lemma 4 utilises Jordan's lemma:

Lemma 5 (**Jordan's Lemma**). *When we have two binary (two outout) measurements observables* $A_0 = M_{0|0} - M_{1|0}$ *and* $A_1 = M_{0|1} - M_{1|1}$ *then they can be simultaneously block-diagonalised, where every block is of size* 2×2 *or* 1×1.

Also, we use the following lemma:

Lemma 6. *Let* ρ *be a two-qubit state, and* A_x *and* B_y *be qubit observables with eigenvalues* ± 1 *for* $x, y \in \{0, 1\}$. *Let* $P(A_x, B_y)$ *be a linear function of* $\{I\} \cup \{A_x B_y\}_{x,y}$ *with real coefficients satisfying* $Tr[\rho P(A_x, B_y)] = 0$. *Then there exists another two-qubit state* ρ', *and observables* A'_x, B'_y *satisfying* $Tr[\rho' P(A'_x, B'_y)] = 0$, *where:*

$$\rho' = \sum_{\alpha=0}^{3} \lambda'_\alpha |\Phi_\alpha\rangle\langle\Phi_\alpha|, \tag{6}$$

$$A'_x = \cos(a'_x)\sigma_Z + \sin(a'_x)\sigma_X, \tag{7}$$

$$B'_y = \cos(b'_y)\sigma_Z + \sin(b'_y)\sigma_X, \tag{8}$$

for some $\lambda'_\alpha \geq 0$, $\sum_\alpha \lambda'_\alpha = 1$ *and* $a'_x, b'_y \in \mathbb{R}$ *for all* x, y.

According to Lemma 6 if a Bell inequality is a correlation inequality (contains only terms $\sum_{x,y} \beta_{xy} \langle A_x B_y \rangle$, without marginal terms $\langle A_x \rangle, \langle B_y \rangle$,) then the only strategies that can maximally violate it have a specific form, as seen in (6),(7),(8), so by plugging these equations into (2) one gets the proof of the self-testing lemma.

□

With the lemmas provided above and specifically Lemma 3 the following result can be proven:

Theorem 1. *For any* $s \in \left(2, \frac{5}{2}\right]$, *there exists a tuple* (θ, ϕ, ω), *along with a set of quantum correlations achieving* $r^{key}_{\theta,\phi,\omega} = 1$ *and* $I_{CHSH} = s$.

This is the crucial theorem showing that with arbitrarily small nonlocality it is possible to extract a perfect key in a device-independent manner. Namely, it implies that for s arbitrarily close to 2, which is arbitrarily close to the local set, and setting $\phi = 0$, there exist values of θ and ω, such that that maximal violation of the Bell inequality corresponding to $\phi = 0, \theta, \omega$ is equal to s. Lemma 3 implies that such maximal violation can be obtained only if Alice and Bob share the maximally entangled pair of qubits, and both Alice and Bob for inputs $x = 0$ and $y = 0$, respectively, measure σ_X. These measurements on the pure entangled state give fully correlated measurement outputs, and as the shared state is maximally entangled it cannot be correlated with Eve, which makes it impossible for Eve to gain any knowledge about the results of any measurements performed by Alice and Bob.

3.4 Conclusion

Alice and Bob can share a secret key in the DI setting using correlations arbitrarily close to being local. However, not all correlations exhibiting nonlocality can be utilized for DIQKD. It is possible to achieve DI randomness with correlations close to the local set. There exist quantum correlations that can simultaneously enable key sharing and maximum randomness while remaining close to the local set.

4 New Interpretation

4.1 Introduction

It has been established that there is a relation between DIQKD and nonlocality. More specifically, nonlocality is necessary for DIQKD. But is it also sufficient? In [Far+21] it is proved that it is not: there exists a nonlocal point for which we cannot extract any key (zero key rate). More specifically, they reported a violation of CHSH with the value 2.105764 (greater than 2), but this is not sufficient to obtain a key. So a natural follow-up question is whether there is a lower bound on nonlocality necessary to extract key (nonzero key rate).The answer, according to [WBC24], is no! There does not exist a minimum amount of nonlocality needed for a DIQKD implementation. That means that for any violation $s \geq 2$ it is possible to obtain a perfect key.

Let us examine the $2 \times 2 \times 2$ scenario. We can visualise the correlations as seen in Figure 9. We can see the local bound ($s = 2$), the quantum set (with maximal violation $s = 2\sqrt{2}$) and the non signaling set.

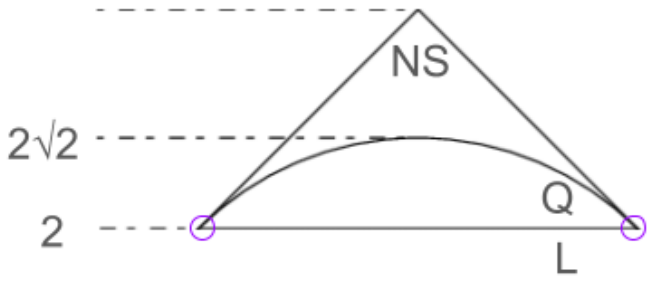

Figure 9: Violation points

Let us assume a violation s, $2 \leq s < 2\sqrt{2}$, as seen in Figure 10. There are infinitely many points that give this violation. However, two of them (the ones in the purple circles) give a perfect key, since they are on the boundary of the quantum set.

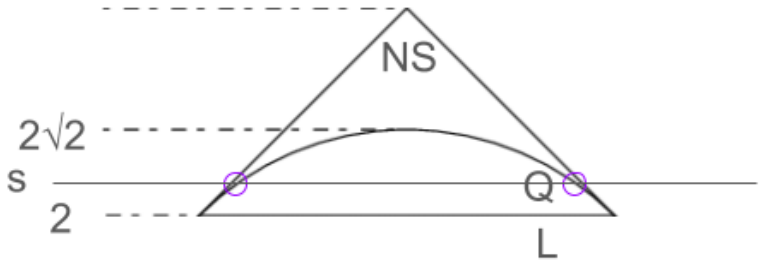

Figure 10: Violation s

It is natural to wonder if all those points with violation s actually exhibit the same amount of nonlocality. It all comes down to the way we "measure" nonlocality. If we assume that the measure for nonlocality is simply the distance from the local set, we could say that all those points expose the same amount of nonlocality. But we suggest that they do not and introduce a new measure of nonlocality.

Our idea for the measure of the amount of nonlocality is the following: All extremal points of the quantum set that are not local (we exclude the circled points in figure 9) should correspond to maximal nonlocality. We can justify by noticing that:

1. All these points are self tests. Each one of them self-tests a pure entangled state.

2. In DIQKD the key rate is calculated by assuming that Eve is quantum. The proof in [WBC24] is based on self testing and self testing assumes the correctness of quantum theory. In general, nonlocality does not assume the correctness of quantum theory. DIQKD, however, does.

Both those justifications are valid, since we look into **quantum** nonlocality.

Just stating that every extremal point has maximum amount of nonlocality (without excluding the circled points in 9) would imply that some local points have maximum nonlocality, because at two points the local and quantum set touch. To avoid such an anomaly we have to further clarify our notion of the nonlocality measure.

4.2 New idea for measure of nonlocality

Let us name the needed distances in Figure 11 in the following way. For a point with violation s: The distance from the local set, which is used in [WBC24] as a measure of nonlocality, is named s_{CHSH}. The smallest distance from an extremal point of the quantum set is d_Q.

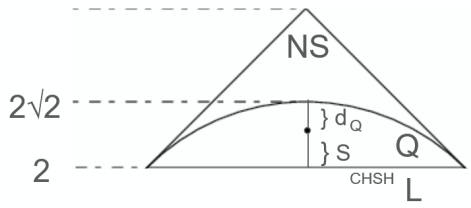

Figure 11: Distances

We introduce a new measure η of nonlocality as the ratio of s_{CHSH} to $s_{CHSH} + d_Q$:

$$\eta = \frac{s_{CHSH}}{s_{CHSH} + d_Q} \tag{9}$$

For $2 < s \leq 2\sqrt{2}$, the point(s) that exist(s) on the boundary of the quantum set (circled points in figure 12) have zero distance from the quantum bound: $d_Q = 0$. That means:

$$\eta = \frac{s_{CHSH}}{s_{CHSH} + 0} = 1$$

For the points that the local and quantum set coincide (Circled points in 13) we have:

$$\eta = \frac{0}{0 + 0}$$

which we determine to be zero.

So we can say that the measure η ranges from zero to one: $0 \leq \eta \leq 1$

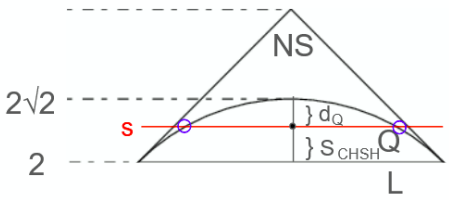

Figure 12: Bound points

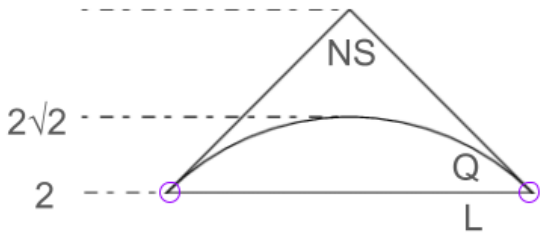

Figure 13: Bound points

4.3 Application of new measure

Let us now examine the value of η for the violation of 2.105764, reported in [Far+21]. As mentioned before, even though we have a violation of the CHSH Bell inequality, the key rate obtained is zero.

The distance of the violation point from the local set is:

$$s_{CHSH} = 2.105764 - 2 = 0.105764$$

and the distance of the violation point from the quantum bound is:

$$d_Q = 2\sqrt{2} - 2.105764 = 0.722663$$

To visualise, we have:

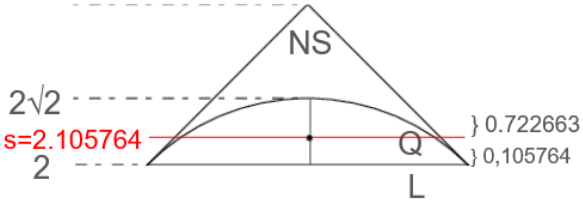

Figure 14: Violation s=2.105764

So the calculation for the new measure of nonlocality η is:

$$\eta = \frac{s_{CHSH}}{s_{CHSH} + d_Q} = \frac{0.105764}{0.105764 + 0.722663} = 0.127668 \tag{10}$$

5 Conclusion

Device-Independent Quantum Key Distribution is strongly linked to nonlocality. In order to obtain a secret key with a non-zero key rate in the DI setting we need nonlocality; the violation of a Bell inequality like CHSH. However, it has been proven that nonlocality is not sufficient for DIQKD. That raises a question whether there is a minimum amount of nonlocality to achieve DIQKD. In order to answer this question we need to use some kind of nonlocality measure. It has been proposed to measure nonlocality in the distance of the violation point to the local set. We introduced a new measure, a "normalised" distance that also takes into account the distance from the quantum bound. So, it is still unclear if there is a lower bound of nonlocality needed for DIQKD and the question remains open for further research.

References

[ABM17] Samson Abramsky, Rui Soares Barbosa, and Shane Mansfield. "The contextual fraction as a measure of contextuality". In: *Phys. Rev. Lett.* 119.5 (Aug. 4, 2017), p. 050504. ISSN: 0031-9007, 1079-7114. DOI: 10.1103/PhysRevLett.119.050504. arXiv: 1705.07918[quant-ph]. URL: http://arxiv.org/abs/1705.07918 (visited on 10/22/2024).

[Aci+07] Antonio Acin et al. "Device-independent security of quantum cryptography against collective attacks". In: *Phys. Rev. Lett.* 98.23 (June 4, 2007), p. 230501. ISSN: 0031-9007, 1079-7114. DOI: 10.1103/PhysRevLett.98.230501. arXiv: quant-ph/0702152. URL: http://arxiv.org/abs/quant-ph/0702152 (visited on 09/30/2024).

[AM16] Antonio Acín and Lluis Masanes. "Certified randomness in quantum physics". In: *Nature* 540.7632 (Dec. 2016), pp. 213–219. ISSN: 0028-0836, 1476-4687. DOI: 10.1038/nature20119. arXiv: 1708.00265[quant-ph]. URL: http://arxiv.org/abs/1708.00265 (visited on 09/19/2024).

[BA19] Boris Bourdoncle and Antonio Acín Dal Maschio. "Quantifying randomness from Bell nonlocality". PhD thesis. Universitat Politècnica de Catalunya, Feb. 13, 2019. DOI: 10.5821/dissertation-2117-131744. URL: http://hdl.handle.net/2117/131744 (visited on 09/19/2024).

[BB84] Charles H. Bennett and Gilles Brassard. *Quantum Cryptography: Public Key Distribution and Coin Tossing*. 1984. URL: https://arxiv.org/pdf/2003.06557.

[Bel] Bell. *On the Einstein Podolsky Rosen paradox*. URL: https://journals.aps.org/ppf/pdf/10.1103/PhysicsPhysiqueFizika.1.195.

[BP15] Cédric Bamps and Stefano Pironio. "Sum-of-squares decompositions for a family of CHSH-like inequalities and their application to self-testing". In: *Phys. Rev. A* 91.5 (May 19, 2015), p. 052111. ISSN: 1050-2947, 1094-1622. DOI: 10.1103/PhysRevA.91.052111. arXiv: 1504.06960[quant-ph]. URL: http://arxiv.org/abs/1504.06960 (visited on 06/17/2024).

[Bra05] Gilles Brassard. "Brief History of Quantum Cryptography: A Personal Perspective". In: *IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, 2005.* 2005, pp. 19–23. DOI: 10.1109/ITWTPI.2005.1543949. arXiv: quant-ph/0604072. URL: http://arxiv.org/abs/quant-ph/0604072 (visited on 05/22/2024).

[Bru+14] Nicolas Brunner et al. "Bell nonlocality". In: *Rev. Mod. Phys.* 86.2 (Apr. 18, 2014), pp. 419–478. ISSN: 0034-6861, 1539-0756. DOI: 10.1103/RevModPhys.86.419. arXiv: 1303.2849[quant-ph]. URL: http://arxiv.org/abs/1303.2849 (visited on 05/16/2024).

[Bru98] Dagmar Bruß. "Optimal Eavesdropping in Quantum Cryptography with Six States". In: *Physical Review Letters* 81.14 (1998), pp. 3018–3021. DOI: 10.1103/PhysRevLett.81.3018. URL: https://doi.org/10.1103/PhysRevLett.81.3018.

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

[Ein] Rosen Einstein Podolsky. *Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? Phys. Rev. 47, 777.* URL: https://journals.aps.org/pr/pdf/10.1103/PhysRev.47.777 (visited on 03/15/1935).

[Eke91] Artur K. Ekert. "Quantum Cryptography Based on Bell's Theorem". In: *Physical Review Letters* 67.6 (1991), pp. 661–663. DOI: 10.1103/PhysRevLett.67.661. URL: https://doi.org/10.1103/PhysRevLett.67.661.

[Far+21] Máté Farkas et al. "Bell nonlocality is not sufficient for the security of standard device-independent quantum key distribution protocols". In: *Phys. Rev. Lett.* 127.5 (July 29, 2021), p. 050503. ISSN: 0031-9007, 1079-7114. DOI: 10.1103/PhysRevLett.127.050503. arXiv: 2103.02639[quant-ph]. URL: http://arxiv.org/abs/2103.02639 (visited on 09/26/2024).

[Fre] associates Fred Cohen. "2.1 - A Short History of Cryptography". In: ().

[Gon+24] Eva M. González-Ruiz et al. "Device Independent Quantum Key Distribution with realistic single-photon source implementations". In: *Opt. Express* 32.8 (Apr. 8, 2024), p. 13181. ISSN: 1094-4087. DOI: 10.1364/OE.497935. arXiv: 2211.16472[quant-ph]. URL: http://arxiv.org/abs/2211.16472 (visited on 06/04/2024).

[Hor+09] Ryszard Horodecki et al. "Quantum entanglement". In: *Rev. Mod. Phys.* 81.2 (June 17, 2009), pp. 865–942. ISSN: 0034-6861, 1539-0756. DOI: 10.1103/RevModPhys.81.865. arXiv: quant-ph/0702225. URL: http://arxiv.org/abs/quant-ph/0702225 (visited on 09/18/2024).

[Hug+21] Ciaran Hughes et al. "Quantum Teleportation". In: *Quantum Computing for the Quantum Curious*. Cham: Springer International Publishing, 2021, pp. 73–79. ISBN: 978-3-030-61600-7 978-3-030-61601-4. DOI: 10.1007/978-3-030-61601-4_8. URL: http://link.springer.com/10.1007/978-3-030-61601-4_8 (visited on 10/28/2024).

[NC] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information*.

[Qua] Quantiki. *Negativity*. URL: https://www.quantiki.org/wiki/Negativity (visited on 10/28/2024).

[Qui] Marco Túlio Quintino. "Bell nonlocality". In: ().

[Rai] Rains. *A rigorous treatment of distillable entanglement*. URL: http://arxiv.org/abs/quant-ph/9809078.

[Rai99] Eric M. Rains. "A rigorous treatment of distillable entanglement". In: *Phys. Rev. A* 60.1 (July 1, 1999), pp. 173–178. ISSN: 1050-2947, 1094-1622. DOI: 10.1103/PhysRevA.60.173. arXiv: quant-ph/9809078. URL: http://arxiv.org/abs/quant-ph/9809078 (visited on 10/28/2024).

[SA19] Alexia Salavrakos and Antonio Acín Dal Maschio. "Bell inequalities for device-independent protocols". PhD thesis. Universitat Politècnica de Catalunya, Mar. 26, 2019. DOI: 10.5821/dissertation-2117-131434. URL: http://hdl.handle.net/2117/131434 (visited on 09/19/2024).

[ŠB20] Ivan Šupić and Joseph Bowles. "Self-testing of quantum systems: a review". In: *Quantum* 4 (Sept. 30, 2020), p. 337. ISSN: 2521-327X. DOI: 10.22331/q-2020-09-30-337. arXiv: 1904.10042[quant-ph]. URL: http://arxiv.org/abs/1904.10042 (visited on 05/31/2024).

[Sca+04a] Valerio Scarani et al. "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations". In: *Physical Review Letters* 92.5 (2004), p. 057901. DOI: 10.1103/PhysRevLett.92.057901. URL: https://doi.org/10.1103/PhysRevLett.92.057901.

[Sca+04b] Valerio Scarani et al. "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations". In: *Physical Review Letters* 92.5 (2004), p. 057901. DOI: 10.1103/PhysRevLett.92.057901. URL: https://doi.org/10.1103/PhysRevLett.92.057901.

[Šup+20] Ivan Šupić et al. "Self-testing and certification using trusted quantum inputs". In: *New J. Phys.* 22.7 (July 1, 2020), p. 073006. ISSN: 1367-2630. DOI: 10.1088/1367-2630/ab90d1. URL: https://iopscience.iop.org/article/10.1088/1367-2630/ab90d1 (visited on 09/25/2024).

[Tho24] Alex Thompson. *Quantum Non-locality: From Bell to Information Causality, Physics 486 March 7, ppt download*. Oct. 3, 2024. URL: https://slideplayer.com/slide/10293068/ (visited on 10/03/2024).

[WBC22] Lewis Wooltorton, Peter Brown, and Roger Colbeck. "Tight analytic bound on the trade-off between device-independent randomness and nonlocality". In: *Phys. Rev. Lett.* 129.15 (Oct. 5, 2022), p. 150403. ISSN: 0031-9007, 1079-7114. DOI: 10.1103/PhysRevLett.129.150403. arXiv: 2205.00124[quant-ph]. URL: http://arxiv.org/abs/2205.00124 (visited on 06/06/2024).

[WBC24] Lewis Wooltorton, Peter Brown, and Roger Colbeck. *Device-independent quantum key distribution with arbitrarily small nonlocality*. Issue: arXiv:2309.09650. Mar. 25, 2024. arXiv: 2309.09650[quant-ph]. URL: http://arxiv.org/abs/2309.09650 (visited on 05/16/2024).

[Wol] Ramona Wolf. *Quantum Key Distribution*.

[Woo] Wooters. *Entanglement of Formation of an Arbitrary State of Two Qubits*. URL: https://arxiv.org/pdf/quant-ph/9709029.