



**GDAŃSK UNIVERSITY
OF TECHNOLOGY**

The author of the doctoral dissertation: Robert
Okuła
Scientific discipline: information and communication technology

DOCTORAL DISSERTATION

Title of doctoral dissertation: Quantifying Quantum Information:
Relationships between measures in Quantum Cryptography

Title of doctoral dissertation (in Polish): Szacowanie informacji
kwantowej: relacje między miarami w kryptografii kwantowej

Supervisor	Second supervisor
<i>signature</i>	<i>signature</i>
dr hab. inż. Piotr Mironowicz, prof. PG	
Auxiliary supervisor	Cosupervisor
<i>signature</i>	<i>signature</i>

Gdańsk, year 2026

Acknowledgements

I would like to thank my supervisor, dr hab. inż. Piotr Mironowicz, for all his advice and friendly and patient help in many situations, including those in which the main problem was my personal character flaws. I would also like to thank him for the many engaging discussions we shared, even including those that ventured into scientific topics.

I would also like to thank dr hab. Marcin Pawłowski, prof. Dariusz Dere-niowski, and prof. Mohamed Bourenmane for providing the opportunity to engage in remarkable research.

I would also like to thank my parents, whose steadfast presence has been my primary anchor. Their lifelong commitment to my education and well-being has made this work possible; I am, and will remain, forever in their debt.

Abstrakt

Niniejsza dysertacja analizuje zależności między różnymi miarami informacji kwantowej, aby wzmocnić teoretyczne podstawy kryptografii kwantowej. Analizując konkretne protokoły, wskazuje, opisuje i rozszerza metody certyfikacji zarówno bezpieczeństwa, jak i jakości generowanych danych. Przedstawione zostały szczegółowe opisy implementacji, które wykorzystują zaawansowane techniki programowania nieliniowego i półokreślonego (ang. *semidefinite programming*, SDP). Zaprezentowane zostały również analityczne rozważania na temat tych zagadnień.

Rozdział 1 zawiera zwięzły przegląd fundamentalnych zasad teorii informacji kwantowej. Rozdział 2 wprowadza w dziedzinę kryptografii kwantowej, szczegółowo omawiając koncepcje kwantowej dystrybucji klucza, modelu bezpieczeństwa niezależnego od konstrukcji urządzenia (DI) oraz teoretyczne podstawy losowości kwantowej. Rozdział 3 bada ramy kwantowego Darwinizmu (QD), teorii wyjaśniającej wyłonienie się świata klasycznego z kwantowej rzeczywistości poprzez proces doboru naturalnego indukowanego przez środowisko. W rozdziale 4 przedstawione zostały wcześniej nieopublikowane wyniki dotyczące analizy bezpieczeństwa kwantowej dystrybucji w kontekście kwantowego darwinizmu. Rozdział 5 szczegółowo opisuje ustalenia dotyczące certyfikacji losowości opartej na splątaniu z wykorzystaniem entropii Shannona. Wyniki te obejmują certyfikację nierówności Bella w kontekście generowania losowości, a także szeroko zakrojone poszukiwania optymalnych protokołów certyfikacji. Wreszcie, rozdział 6 analizuje związek między nielokalnością Bella a dyskordem kwantowym, ustanawiając również numeryczną korelację między wartością łamania Bella dla różnych nierówności Bella a dyskordem.

Abstract

This study investigates the relationships between various quantum information measures to strengthen the theoretical foundations of quantum cryptography. By analyzing specific protocols, we indicate, describe, and expand benchmarks for certifying both the security and the quality of the produced data. We provide a detailed description of our implementations, which utilize advanced non-linear and semidefinite programming (SDP) techniques. We also present analytical considerations on these issues.

Chapter 1 provides a concise overview of the fundamental principles of quantum information theory. Chapter 2 introduces the field of quantum cryptography, detailing the concepts of quantum key distribution (QKD), device-independence (DI), and the theoretical foundations of quantum-based randomness. Chapter 3 explores the framework of quantum Darwinism (QD), a theory that explains the emergence of the classical world from the quantum realm through a process of environment-induced natural selection. In Chapter 4, we present our pioneering results regarding QKD security analysis within the context of QD. Chapter 5 details our findings on entanglement-based randomness certification using Shannon entropy. These results encompass certification for Bell inequalities in the context of randomness generation, alongside an extensive search for optimal certification protocols. Finally, Chapter 6 analyzes the relationship between Bell non-locality and quantum discord, establishing a numerical correlation between Bell violation for different Bell inequalities and discord.

Table of Contents

Acknowledgements	3
Abstrakt (polski)	4
Abstract (English)	5
Notation	9
Acronyms	11
Preface	13
1 Introduction	16
1.1 The formalism of quantum theory	16
1.1.1 Hilbert space and states	16
1.1.2 Measurement	18
1.2 Quantum information	20
1.2.1 Bell operators and inequalities	20
1.2.2 Classical and quantum probability distributions . . .	22
1.3 Measures of information	25
1.3.1 Shannon entropy	25
1.3.2 von Neumann entropy	27
1.3.3 Min-entropy	27
1.3.4 Rényi entropy	29
1.3.5 Quantum discord	29
1.4 Numerical methods	31
1.4.1 Non-linear optimization	31
1.4.2 Solvers	33
1.4.3 Semidefinite programming	34
1.4.4 Navascués-Pironio-Acín hierarchy	35

2	Quantum cryptography	39
2.1	Key distribution	39
2.1.1	Quantum cryptography with classical keys	42
2.1.2	Protocols	42
2.2	Device-independence	44
2.3	Randomness	46
2.3.1	Extraction and amplification of randomness	48
2.3.2	Certification	49
3	Quantum Darwinism	51
3.1	Model of measurement	52
3.2	Environment-induced selection	54
3.3	Information redundancy	55
4	Decoherence and QKD	59
4.1	Measurement and Decoherence in BB84	60
4.2	Single-qubit layered environment	63
4.3	Distinguishability analysis	66
5	Randomness certification	71
5.1	Device-independent randomness certification	72
5.1.1	Randomness extraction and certification	73
5.1.2	Bounding the probabilities	75
5.1.3	Calculating entropy	76
5.1.4	Shannon entropy certification	78
5.2	Certification for existing Bell inequalities	81
5.2.1	Clauser-Horne-Shimony-Holt inequality	82
5.2.2	Braunstein-Caves inequalities	82
5.2.3	I_1 and I_2	83
5.2.4	Woollorton-Brown-Colbeck inequalities	85
5.2.5	Comparison	87
5.2.6	General form for Shannon entropy	87
5.2.7	Entropy as a composite function	91
5.2.8	Additional constraints	93
5.2.9	Three-outcome scenario	94
5.3	Extensive search for certification protocols	96
5.3.1	General analysis	96
5.3.2	Selected protocols	98
5.3.3	Boxes self-testing	101

6	Dependence between quantum discord and non-locality	104
6.1	Characterization for entangled states	105
6.1.1	Parametrization of the measurement	107
6.1.2	Discord calculation	108
6.2	Results	108
6.2.1	Discord for canonical Bell inequalities	109
6.2.2	Structural Patterns in Discord Minimization	112
	Concluding remarks	115
	References	118
	List of Figures	142
	List of Tables	143
	Index	145
	Appendices	146
A	QR decomposition	146
B	Second-degree derivation for Shannon entropy	147

Notation

$\mathbb{R}$	set of real numbers
$\mathbb{C}$	set of complex numbers
$\mathcal{H}$	Hilbert space
$X \in \mathbb{R}^{n \times n}$	single upper-case letters denote matrices
$\mathcal{X}$	calligraphic upper-case letters denote sets of probability distributions or Hilbert spaces
ρ	density matrix
$U(\mathcal{X})$	unitary operator acting on subspace $\mathcal{X}$
$M^{p,x}$	measurement operator (observable) with a measurement setting x , used by party p
$\Pi_m^{p,x}$	projective measurement operator (projector) with a measurement setting x , onto the eigenspace with eigenvalue (measurement result) m , used by party p
$\Pi_m^{(\mathcal{X})}$	projective measurement operator (projector) acting on a subspace $\mathcal{X}$, for measurement result m
G	Bell operator
p	Werner white noise level
ε	operator interaction noise level (the level of interaction)
P	probability
Γ	decoherence factor
$\mathbf{\Gamma}$	moment matrix
$P(a, b x, y)$	conditional probability
$\mathfrak{P}$	probability distribution
$\mathcal{P}$	set of all probability distributions
$\mathcal{L}$	set of all local probability distributions
$\mathcal{Q}$	set of all quantum probability distributions
$\mathcal{N}$	set of all no-signalling probability distributions
$\mathfrak{B}$	Bell expression
$ \mathfrak{B} $	value of the Bell expression

$ \mathfrak{B} _{\mathcal{L}}$	classical/local bound of the Bell expression
$ \mathfrak{B} _{\mathcal{Q}}$	quantum bound of the Bell expression
$ \mathfrak{B} _p$	value of the Bell expression for a noisy quantum state
$\mathfrak{B} \leq \mathfrak{B} _{\mathcal{L}}$	Bell inequality
$\mathcal{S}$	a subspace of a Hilbert space that corresponds to the quantum system in decoherence
$\mathcal{A}$	a subspace of a Hilbert space that corresponds to the apparatus in decoherence
$\mathcal{E}$	a subspace of a Hilbert space that corresponds to the environment in decoherence
$ x\rangle$	state vector in a Hilbert space
$\langle x $	linear functional in a dual space $\mathcal{H}^*$
$\langle A \rangle$	expectation value of an operator A

Acronyms

AEP asymptotic equipartition property

BQP bounded-error quantum polynomial time

DI device-independent

ECC Elliptic Curve Cryptography

i.i.d. independent and identically distributed

LP linear programming

NLP non-linear programming

NP nondeterministic polynomial time

NPA Navascués-Pironio-Acín hierarchy

OTP one-time pad

POVM positive-operator valued measure

PQC post-quantum cryptography

PRNG pseudorandom number generation

QBER quantum bit error rate

QCI quantum communication infrastructure

QD quantum darwinism

QKD quantum key distribution

QRNG quantum random number generation

SDP semidefinite programming

SQP Sequential Quadratic Programming

BB84 Bennett-Brassard 1984 quantum key distribution protocol

E91 Ekert 1991 quantum key distribution protocol

CHSH Clauser-Horne-Shimony-Holt Bell inequality

BCn Braunstein-Caves chain Bell inequalities

Preface

In the realm of quantum information, we often find ourselves caught between the ethereal beauty of Hilbert space and the uncompromising demands of real-world security. While classical cryptography relies on the presumed difficulty of mathematical problems, quantum cryptography grounds its guarantees in the very fabric of physical reality – the uncertainty of a measurement, the fragility of a state, and the monogamy of entanglement. However, the transition from these abstract principles to a verifiable, secure communication channel requires more than just physical laws – it requires a rigorous way to quantify the quantum data in a way that is comparable with other forms. This thesis is born from the pursuit of that.

The task of this work is the formulation of the models of quantum phenomena utilized in the framework of quantum cryptography, and based on the methodological analysis and numerical representation, investigate the relations between different measures of quantum correlations and the impact of these relations on the safety of the quantum key distribution (QKD) and the extractability of random data.

The interest in quantum-based technology and its practical implementations is the subject of ongoing scrutiny. The interest is crystallized in massive infrastructure projects like the European Union EuroQCI (quantum communication infrastructure) [59], which is now moving into its operational phase. This pan-European initiative utilizes a hybrid architecture of terrestrial fiber [168, 145] and the newly built Eagle-1 [60] satellite to establish a sovereign, tamper-proof backbone for government communications. Similarly, China has expanded its integrated space-to-ground network, utilizing the Micius satellite and the 2000 km Beijing-Shanghai fiber backbone to achieve unconditional security across its financial and administrative sectors [30, 33].

Corporate programs have mirrored this momentum, transitioning from pilot studies to full-scale infrastructure integration. Leading telecommunications firms, such as Toshiba and KDDI, recently demonstrated the

first world-scale QKD multiplexing, allowing quantum keys to share existing commercial fiber alongside 33.4 Tbps of classical data [177, 162]. In 2025, Spanish firm LuxQuanta commercialized its NOVA LQ system, a Continuous-Variable QKD solution designed to co-exist with classical data on existing metropolitan fiber without requiring dedicated infrastructure [176]. Similarly, Polish company Creotech Instruments launched its proprietary QKD transmitter and receiver modules, specifically targeting the high-security needs of the defense and public administration sectors within the EuroQCI framework [42].

With these developments, the analysis of theoretical quantum information theory might be viewed as significantly removed from practical applications and therefore less important. However, many potential aspects of the security of quantum information remain unknown, even on the theoretical level, and with the advent of the quantum hacking community (which utilizes the recent experimental advancements to eavesdrop on different quantum cryptography methods), it is important to investigate the potential theoretical threats and chances.

The work is organized as follows. The first part of this thesis establishes the necessary rigor for navigating the quantum information landscape. Beginning with the essential mathematical formalism of Hilbert spaces and information measures, Chapter 1 provides the conceptual scope needed to describe the behavior of quantum systems. Furthermore, in Chapter 2, we introduce the basic concepts of quantum cryptography, including quantum key distribution, and the methods that allow for the generation of verifiable randomness.

Chapter 3 presents the framework of quantum Darwinism. Here, the environment is reimaged not merely as a source of decoherence but as an active witness. This theoretical introduction serves as the catalyst for the original research presented in Chapter 4, which investigates the security implications of this process. By modeling the measurement process of the BB84 protocol through a generalized *layered environment* model, we quantify how information potentially leaks into the surroundings. This analysis specifically evaluates the vulnerability of cryptographic keys to side-channel attacks.

Chapter 5 introduces a novel randomness certification framework that utilizes the NPA hierarchy to establish rigorous bounds on probability distributions and their linear combinations. These bounds serve as fundamental constraints for a non-linear optimization process that determines the Shannon entropy and facilitates the certification of quantum correlations. The

methodology involves a comparative analysis of four distinct families of Bell inequalities, specifically the CHSH [36], Braunstein-Caves family of chain inequalities [24], I_n [116], and Woollerton-Brown-Colbeck [194], to identify optimal certificates for maintaining QRNG robustness across varying noise thresholds. The work encompasses the derivation of analytical forms for Shannon entropy under NPA constraints and the implementation of a computationally efficient lower bound that bypasses intensive optimization. Furthermore, the study scales these techniques to three-outcome scenarios for qudit applications and employs a high-throughput quantitative framework to evaluate over 500 thousand Bell expressions. Finally, the research investigates the self-testing properties of selected certificates.

Finally, Chapter 6 delves into the nuanced relationship between different ways of quantifying the quantumness of a correlation. Through a novel numerical framework, we investigate the interplay between Bell non-locality and quantum discord. Although quantum discord describes the weakest forms of quantum correlations, persisting even in the complete absence of entanglement, it can still be effectively harnessed as a bipartite resource for secure quantum cryptography [138].

The discerning reader will note that this thesis touches many different aspects of quantum theory, including, e.g., the mathematical background for the description of quantum states and correlations, or practical quantum cryptography. This thesis was written in a way that can be useful for a person with general computer science knowledge to familiarize themselves with the basics of quantum information theory. We also assume some knowledge of the basics of linear algebra.

This work contains the results of the following publications:

1. **Robert Okuła** and Piotr Mironowicz. *How decoherence affects the security of BB84 quantum key distribution protocol*. Quantum Information Processing, 24(2), February 2025. ISSN 1573-1332. doi: 10.1007/s11128-025-04650-8 [129];
2. **Robert Okuła** and Piotr Mironowicz. Device-independent Shannon entropy certification. New Journal of Physics, 27(11):114519, November 2025. ISSN 1367-2630. doi: 10.1088/1367-2630/ae20b2 [130];
3. **Robert Okuła** and Piotr Mironowicz. Extensive search of Shannon entropy-based randomness certification protocols, 2025. arXiv: 2511.22771 [131].

Additionally, Chapter 6 contains the results that have not been published previously.

Chapter 1

Introduction

This chapter establishes the theoretical preliminaries essential for a comprehensive understanding of quantum communication. The discussion begins by outlining the relevant mathematical formalism, followed by an introduction to the fundamental principles of quantum information theory. Finally, the chapter defines and analyzes the specific measures of information utilized in quantum protocols.

1.1 The formalism of quantum theory

This section establishes the formal mathematical and conceptual foundations of quantum theory required for the subsequent analysis. We begin by defining the structure of Hilbert spaces and the associated operator algebra that governs quantum states. Building upon this framework, we examine the mechanics of quantum measurement. The section concludes with an overview of multipartite probability distributions, providing the necessary notation to describe correlations in composite systems.

1.1.1 Hilbert space and states

The state of a quantum system is formally defined as a unit vector $|\psi\rangle$ within a separable complex Hilbert space $\mathcal{H}$. The Hilbert space is defined as a vector space over a field $\mathbb{F}$ (typically $\mathbb{C}$ for quantum mechanics) equipped with an inner product $\langle \cdot, \cdot \rangle : \mathcal{H} \times \mathcal{H} \rightarrow \mathbb{F}$ that satisfies conjugate symmetry, linearity in the first argument, and positive-definiteness. This inner product induces a norm $\|x\| = \sqrt{\langle x, x \rangle}$ and a subsequent metric $d(x, y) = \|x - y\|$. A defining technical property is that $(\mathcal{H}, d)$ must be complete, meaning every

Cauchy sequence $\{x_n\}_{n=1}^\infty$ satisfying $\lim_{n,m \rightarrow \infty} \|x_n - x_m\| = 0$ converges to some $x \in \mathcal{H}$. Furthermore, the inner product must satisfy the Cauchy-Schwarz inequality, $|\langle x, y \rangle| \leq \|x\| \|y\|$.

In infinite-dimensional settings, Hilbert spaces are often characterized by their separability, implying the existence of a countable orthonormal basis $\{e_k\}_{k=1}^\infty$. For any $x \in \mathcal{H}$, the Parseval's Identity holds, $\|x\|^2 = \sum_{k=1}^\infty |\langle x, e_k \rangle|^2$, which generalizes the Pythagorean theorem to infinite dimensions.

Dirac's bra-ket notation provides a robust algebraic framework for quantum mechanics by representing state vectors as *kets* ($|\psi\rangle$) in a Hilbert space $\mathcal{H}$ and their corresponding continuous linear functionals as *bras* ($\langle\phi|$) in the dual space $\mathcal{H}^*$. This notation abstracts the complex vector operations into a symbolic calculus where the inner product is represented by the *bra-ket* $\langle\phi|\psi\rangle$, satisfying the property $\langle\phi|\psi\rangle = \langle\phi|\psi\rangle^*$. Key to this formalism is linearity in the ket, $|a\psi + b\phi\rangle = a|\psi\rangle + b|\phi\rangle$, and anti-linearity in the bra, $\langle a\psi + b\phi| = a^*\langle\psi| + b^*\langle\phi|$. Furthermore, the notation seamlessly handles outer products $|\psi\rangle\langle\phi|$, which define linear operators acting on the space, and the expectation value of an operator $\hat{A}$, expressed compactly as $\langle\psi|\hat{A}|\psi\rangle = \langle\hat{A}\rangle_\psi$. If $\hat{A}$ has a complete set of eigenvectors $|\phi_i\rangle$, with eigenvalues λ_i , so that $\hat{A} = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|$, then $\langle\hat{A}\rangle_\psi = \sum_i \lambda_i |\langle\psi|\phi_i\rangle|^2$. Additionally, the infinity norm, or spectral norm, of an operator $\hat{A}$ measures the maximum extent to which the operator scales the magnitude of a vector, formally defined as the supremum of the ratio between the Euclidean norm of the mapped vector and that of the original non-zero vector, given by $\|\hat{A}\|_\infty = \sup_{|\psi\rangle \neq 0} \frac{\|\hat{A}|\psi\rangle\|_2}{\| |\psi\rangle \|_2}$.

In a more rigorous statistical framework, the state of a quantum system is represented by a density operator ρ , a linear, self-adjoint operator acting on the Hilbert space $\mathcal{H}$ that satisfies the requirements of positivity ($\rho \geq 0$) and a unit trace ($\text{Tr}(\rho) = 1$). This representation provides a unified framework for mixed states arising from either classical statistical ensembles (where the specific state preparation is unknown) or quantum entanglement, where the state of a local subsystem cannot be purified without considering its correlations to a larger Hilbert space. While a pure state can be represented as a rank-1 projection operator $\rho = |\psi\rangle\langle\psi|$ satisfying the idempotency condition $\rho^2 = \rho$, a mixed state must be expressed as a convex combination $\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$, where p_i are classical probabilities. The transition from pure to mixed states is quantified by the purity $\text{Tr}(\rho^2)$, which is strictly less than unity for mixed states and exactly one for pure states. The infinity norm of a density operator reduces exactly to its largest

eigenvalue, $\|\rho\|_\infty = \sup_{\langle\psi|\psi\rangle=1} \langle\psi|\rho|\psi\rangle = \max_x \lambda_x$.

We call a composite quantum state independent and identically distributed (i.i.d.) if the n -partite system is the tensor product of identical, uncorrelated subsystems:

$$\rho^{\otimes n} = \rho \otimes \cdots \otimes \rho,$$

where *independent* means there is no entanglement or classical correlation between subsystems, and *identically distributed* means every subsystem is described by the exact same state ρ .

The density matrix serves as the primary tool for the partial trace operation, $\rho_A = \text{Tr}_B(\rho_{AB})$, which maps a bipartite state in the tensor product space $\mathcal{H}_A \otimes \mathcal{H}_B$ to a reduced density operator for subsystem A . This operation is fundamental to the study of decoherence, as it effectively averages out the environmental degrees of freedom, causing the decay of off-diagonal elements in the basis of the observable, as explained later in Section 3.3.

1.1.2 Measurement

To characterize the physical outcomes of an observation, we introduce an operator called an *observable*, acting on the state space of a quantum system, representing a physical property that can be measured, such as position, momentum, or spin. To be precise, physical observables are represented by linear, self-adjoint (Hermitian) operators $M : \mathcal{D}(M) \rightarrow \mathcal{H}$, where the domain $\mathcal{D}(M)$ is dense in $\mathcal{H}$. According to the Spectral Theorem, these operators admit a spectral decomposition, allowing any state to be resolved into an orthonormal basis of eigenvectors corresponding to real-valued eigenvalues.

Projective measurements represent a common special case of the general measurement postulate. A projective measurement is defined by an observable M . This observable has a spectral decomposition $M = \sum_m m \Pi_m$, where Π_m is a projector onto the eigenspace of M with eigenvalue m . The possible outcomes of the measurement correspond to these eigenvalues m . If the state of the system is $|\psi\rangle$ immediately before the measurement, the probability of obtaining result m is given by $p(m) = \langle\psi|\Pi_m|\psi\rangle$. Projective measurements are characterized by the fact that they are idempotent, which is characterized by the fact that for the projector Π_m we have $\Pi_m \Pi_m = \Pi_m$. A complete set of orthogonal projectors $\{\Pi_m\}_m$ must satisfy the completeness relation $\sum_m \Pi_m = I$ to ensure the sum of probabilities for all possible outcomes equals one. The only possible eigenvalues for a projector are 0

and 1; an eigenvector $|\psi\rangle$ is either in the projected subspace ($\Pi_m|\psi\rangle = |\psi\rangle$) or orthogonal to it ($\Pi_m|\psi\rangle = 0$).

A measurement is *conducted in a basis* $\{|i\rangle\}_i$ when a projective measurement is performed, where the measurement operators are the projectors $\Pi_i = |i\rangle\langle i|$ onto the orthonormal basis vectors of the system's Hilbert space. Operationally, this means that for any arbitrary input state $|\psi\rangle$, the system is first resolved into a linear combination of these basis elements, $|\psi\rangle = \sum_i \alpha_i |i\rangle$, where the complex amplitudes are determined by the inner product $\alpha_i = \langle i|\psi\rangle$. The computational basis of a Hilbert space of dimension d is denoted by $|0\rangle, \dots, |d-1\rangle$, where

$$|i\rangle = \left[\underbrace{0 \dots 0}_{i-1} 1 \underbrace{0 \dots 0}_{i-1} \right]^T.$$

The following vectors define a Hadamard basis for a two-dimensional system:

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

The Hadamard basis is *mutually unbiased* with the $d = 2$ computational basis, which means that a system prepared in an eigenstate of one basis yields a completely uniform distribution of results if measured in the other. Mathematically, this implies that for a Hilbert space of dimension d , the probability of obtaining any specific outcome m is exactly $1/d$.

A generalization of quantum measurement is called a *Positive Operator-Valued Measure* (POVM). While standard projective measurements require that the measurement operators be orthogonal projectors, a POVM is defined more broadly by a set of positive operators $\{E_m\}_m$ that satisfy the completeness relation $\sum_m E_m = \mathbb{1}$. They are essential in quantum information theory for tasks such as distinguishing non-orthogonal quantum states, where they can provide a higher probability of success than is possible with restricted projective measurements. The probability of obtaining a particular outcome m when the system is in the state is given by the same formulas as for projective measurements.

In this thesis, we use $\Pi_m^{p,x}$ to describe projectors on results m for measurement settings x , and p denotes the party that uses a given operator. Similarly, $M^{p,x}$ denotes an observable for a party p and setting x .

1.2 Quantum information

In 1964, John Bell [18] established that the predictions of quantum mechanics cannot be reconciled with local hidden-variable theories, which had been famously advocated in the context of the Einstein-Podolsky-Rosen paradox [56]. He demonstrated that the correlations exhibited by entangled systems surpass the maximum limits achievable by any local realistic framework. This result effectively ruled out the possibility that quantum statistical distributions arise from a deeper, deterministic classical layer, instead highlighting the fundamental nature of quantum indeterminacy.

Building upon the foundational shift initiated by Bell's theorem, the field of quantum information treats the unique properties of quantum states as physical resources, which can be used as a means for acquisition, transmission, and processing of data in a completely different way. This topic at large covers many separate issues, like quantum algorithms [163, 167], quantum error correction [29, 2], quantum machine learning [21, 47], just to name a few. It also includes the topic of quantum cryptography, which is covered separately in Chapter 2. In this section, we introduce the elementary concepts for quantum information theory, including the Bell theorem and the division between classical and quantum.

1.2.1 Bell operators and inequalities

In the Bell's theorem, a scenario is considered in which two independent and spatially separated parties, Alice and Bob, together with a third entity acting as a referee, are involved. The referee distributes an entangled quantum state to Alice and Bob in the form of a bipartite entangled system, such as a pair of polarization-entangled photons, with one particle sent to each party. Upon receiving their respective subsystems, Alice and Bob perform local measurements, randomly selecting from a set of observables: $\{M^{0,0}, M^{0,1}, \dots\}$ for Alice and $\{M^{1,0}, M^{1,1}, \dots\}$ for Bob. For instance, when considering binary observables, they are in the form of $M^{p,x} = \Pi_+^{p,x} - \Pi_-^{p,x} = 2\Pi_+^{p,x} - \mathbb{1}$. A linear combination of the expected values for these measurements is considered: [36]:

$$\mathfrak{B} = \langle C(0,0) \rangle + \langle C(0,1) \rangle + \langle C(1,0) \rangle - \langle C(1,1) \rangle. \quad (1.1)$$

where $C(x,y)$ is a correlation operator:

$$\begin{aligned} C(x,y) &= M^{0,x} \otimes M^{1,y} \\ &= 4\Pi_+^{0,x}\Pi_+^{1,y} - 2\Pi_+^{0,x} - 2\Pi_+^{1,y} + \mathbb{1}, \end{aligned} \quad (1.2)$$

x and y stand for the measurement settings, Alice's projector on results $+1$ (-1) is denoted as $\Pi_+^{0,x}$ ($\Pi_-^{0,x}$), and analogously for Bob $\Pi_+^{1,y}$ ($\Pi_-^{1,y}$). If the measured properties of the objects exist independently of observation (which we call *realism*) and if the choice of the observable by one party cannot influence the results of the other (which we call *locality*), the upper bound of (1.1) is 2. This limit is referred to as the classical (or local) bound. The expression in the form of (1.1) is commonly called CHSH and is a member of a group that we call Bell expressions.

To derive the maximum value of the CHSH expression for entangled states, we rewrite the (1.1) as $\mathfrak{B} = \langle G \rangle$, where $G_{CHSH} = M^{0,0} \otimes (M^{1,0} + M^{1,1}) + M^{0,1} \otimes (M^{1,0} - M^{1,1})$. By squaring this operator and utilizing the property of Hermitian observables $-(M^{0,i})^2 = (M^{1,i})^2 = \mathbb{1}$ and that Alice's and Bob's operators commute, the expression simplifies to:

$$G_{CHSH}^2 = 4\mathbb{1} - [M^{0,0}, M^{0,1}][M^{1,0}, M^{1,1}]. \quad (1.3)$$

In classical mechanics, these commutators are zero, bounding the expectation value $|\mathfrak{B}|_{\mathcal{L}} = |\langle G_{CHSH} \rangle|_{\mathcal{L}}$ at 2. By selecting anti-commuting observables, such as the Pauli matrices σ_x and σ_z , the squared operator reaches $\|G_{CHSH}^2\| = 4 + 4 = 8$, yielding the *Tsirelson's bound* of $|\mathfrak{B}_{CHSH}|_{\mathcal{Q}} = |\langle G_{CHSH} \rangle|_{\mathcal{Q}} = \sqrt{8} = 2\sqrt{2}$. If a Bell expression yields a value exceeding its classical bound, the state is at least partially entangled. Furthermore, while the violation of a Bell inequality quantifies the system's non-classical behavior, it should not be conflated with a strict measure of the state's entanglement. When the expression reaches its Tsirelson's bound, the state is maximally entangled.

Since the derivation of the CHSH expression, a plethora of other Bell expressions have been formulated [24, 102, 194, 186], e.g., for detection of states that are partially separable [69, 158, 179] or using the property of Frank-Wolfe algorithms for constructing Bell inequalities with a high resistance to noise [50, 52, 25]. The general form of the Bell operator can be represented as:

$$G(A, B, X, Y) = \sum_{a \in A} \sum_{b \in B} \sum_{x \in X} \sum_{y \in Y} \alpha_{a,b,x,y} \left(\Pi_a^{0,x} \otimes \Pi_b^{1,y} \right), \quad (1.4)$$

where $\alpha_{a,b,x,y} \in \mathbb{R}$ are coefficients that define the specific Bell expression. Bell inequality is thus defined as:

$$\sum_{a \in A} \sum_{b \in B} \sum_{x \in X} \sum_{y \in Y} \alpha_{a,b,x,y} |\langle \Pi_a^{0,x} \otimes \Pi_b^{1,y} \rangle| \leq |\mathfrak{B}|_{\mathcal{L}}, \quad (1.5)$$

where $|\mathfrak{B}|_{\mathcal{L}}$ is the local bound. When the value of the Bell expression (sometimes called a Bell value) exceeds its local bound ($|\mathfrak{B}|_{\mathcal{L}} < |\langle G \rangle| \leq |\mathfrak{B}|_{\mathcal{Q}}$), we call it a Bell violation.

1.2.2 Classical and quantum probability distributions

Let us again consider a bipartite scenario with two independent and spatially separated parties, with a referee distributing two quantum objects (for example photons, entangled or not) to Alice and Bob. Upon receiving their respective subsystems, parties perform their measurements, with settings $x \in X$ and $y \in Y$ with results $a \in A$ and $b \in B$ (for Alice and Bob respectively). $X \neq \emptyset$ and $Y \neq \emptyset$ are finite sets of all possible measurement settings and $A \neq \emptyset$ and $B \neq \emptyset$ are finite sets of all possible measurement results. The joint probability of outcomes a, b for settings x, y we denote as $P(a, b|x, y)$. Probability of Alice receiving the outcome a we denote as $P(a|x, y) = \sum_{b \in B} P(a, b|x, y)$ and for Bob analogously $P(b|x, y) = \sum_{a \in A} P(a, b|x, y)$.

We want to characterize the probability distributions that describe the quantum correlations and quantum measurements. For that, let us consider the set of probability distributions:

$$\mathcal{P}(A, B|X, Y) \subset \mathbb{R}_+^{|A| \cdot |B| \cdot |X| \cdot |Y|}, \quad (1.6)$$

where a single distribution $\mathfrak{P}(A, B|X, Y) = \{P(a, b|x, y)\}_{a \in A, b \in B, x \in X, y \in Y}$ gives the complete characterization of the behaviour of the joint state of two quantum objects. First, let us define the classical description of a state [114]:

Definition 1.2.1. The probability distribution $\mathfrak{P}(A, B|X, Y)$ is called a *classical* or *local* probability distribution iff there exists conditional probability distributions $\mathfrak{P}(\Lambda)$, $\mathfrak{P}(A|X, \Lambda)$, $\mathfrak{P}(B|Y, \Lambda)$, satisfying:

$$P(a, b|x, y) = \sum_{\lambda} P(\lambda) \cdot P(a|x, \lambda) \cdot P(b|y, \lambda) \quad (1.7)$$

where the distribution $\mathfrak{P}(\Lambda)$ describes the probability of the state being in one of the internal states $\lambda \in \Lambda$ before any measurement takes place and distributions $\mathfrak{P}(A|X, \Lambda)$, $\mathfrak{P}(B|Y, \Lambda)$ describes the probability of obtaining the results from sets A and B , given the separate measurement settings and initial (potentially shared) state λ .

We denote the set of all local distributions as $\mathcal{L}$. In the local scenario, the devices could have been initially connected and in a shared state. However, as the two parties are performing their measurements in a spatially separated situation (in which they are not able to share the information about their measurement settings), the results of these measurements are independent, not influenced by the other party's actions.

Subsequently, we want to define the set of probability distributions that correspond to the quantum relations between objects:

Definition 1.2.2. A bipartite probability distribution $\mathfrak{P} = \{P(a, b|x, y)\}$ is said to be *quantum* if there exists a complex Hilbert space $\mathcal{H}$, a density operator ρ acting on $\mathcal{H}$, and sets of local projectors $\{\Pi_a^{0,x}\}_a$ and $\{\Pi_b^{1,y}\}_b$ such that the following conditions are satisfied:

1. the sets of projectors $\{\Pi_a^{0,x}\}_a$ and $\{\Pi_b^{1,y}\}_b$ are orthogonal;
2. to ensure that Alice and Bob's measurements are locally independent and spatially separated, their respective operators must commute:

$$\forall a, b, x, y \quad [\Pi_a^{0,x}, \Pi_b^{1,y}] = 0.$$

The probabilities are then obtained via the trace of the product of the state and the measurement operators:

$$P(a, b|x, y) = \text{Tr}(\rho(\Pi_a^{0,x} \otimes \Pi_b^{1,y})). \quad (1.8)$$

The set of all quantum probability distributions we denote as $\mathcal{Q}$. If we analyze the course of a quantum process using just the probability distribution that it generates, we call this distribution a *quantum behavior*. This, however, does not exhaust the scope of all possible correlations described by the relevant probability distributions. The quantum correlations can be further generalized to account only for the fact that the physical system must be consistent with special relativity, specifically prohibiting faster-than-light communication.

Definition 1.2.3. A bipartite distribution $\mathfrak{P}(A, B|X, Y)$ belongs to the set of no-signaling correlations if it satisfies the following two sets of linear constraints for all $a \in A, b \in B, x \in X, y \in Y$:

$$\begin{aligned} \forall x, x' \in X \quad \sum_{a \in A} P(a, b|x, y) &= \sum_{a \in A} P(a, b|x', y), \\ \forall y, y' \in Y \quad \sum_{b \in B} P(a, b|x, y) &= \sum_{b \in B} P(a, b|x, y'). \end{aligned} \quad (1.9)$$

The set of all no-signaling probability distributions is denoted as $\mathcal{N}$. We visualize the relationship between different sets of correlation (local, quantum and no-signalling) in Figure 1.1. The set of quantum correlations is a strict subset of the no-signaling set ($\mathcal{L} \subset \mathcal{Q} \subset \mathcal{N}$). This means there exist mathematically consistent no-signaling distributions that cannot be realized by any quantum state or measurement, the most famous being the Popescu-Rohrlich (PR) Box [15]. It is an extremal no-signaling correlation that demonstrates a maximum no-signaling violation of the CHSH inequality. Defined by the probability distribution $\mathfrak{P}(a, b|x, y) = \frac{1}{2}\delta_{a \oplus b, xy}$ (where δ is the Kronecker delta) it ensures that the outputs are correlated for all input pairs except $(x, y) = (1, 1)$, where they are anti-correlated. While consistent with the no-signaling principle, a PR box yields a Bell value for CHSH of $|\mathfrak{B}|_{\mathcal{N}} = 4$.

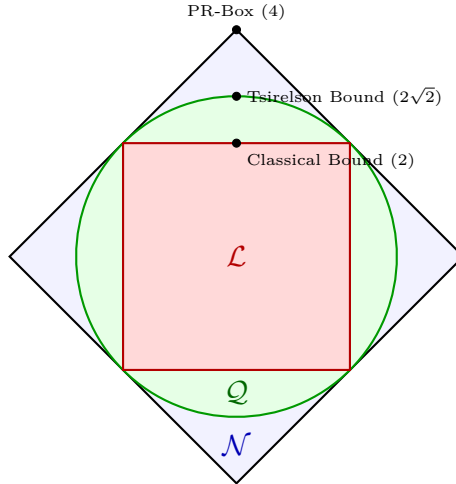


Figure 1.1: The nested hierarchy of bipartite correlation sets. The inner polytope represents the set of local correlations ($\mathcal{L}$), bounded by linear Bell inequalities. The intermediate convex set with curved boundaries denotes the set of quantum correlations ($\mathcal{Q}$), which exceeds the local bound up to the Tsirelson's bound. Both are contained within the no-signaling polytope ($\mathcal{N}$).

Another interesting perspective on the boundaries of physical correlations is provided by the principle called Information Causality [136]. Alice holds a database of N random bits and Bob attempts to guess the value of a single bit a_b . Alice can send a message of only m classical bits to Bob, who can also utilize any previously shared no-signalling re-

sources, such as quantum entanglement or non-local boxes [12]. The authors identify three elementary properties that any consistent measure of information must satisfy: consistency with mutual information for classical correlations, a data-processing inequality (local actions cannot increase information), and a chain rule for conditional mutual information ($I(A : B, C) = I(A : C) + I(A : B|C)$). They prove that following these rules, the total information Bob can gain is bounded by the message size m :

$$\sum_{k=1}^N I(\alpha_k, \beta | b = k) \leq m, \quad (1.10)$$

where β is Bob's output or guess for the value of the bit Alice holds and b is the random variable Bob receives, which tells him which specific bit index he asked to guess. They also demonstrate that this principle is violated by any theory allowing correlations stronger than the quantum bound by showing that if the expectation value of the correlation $\langle C(x, y) \rangle$ exceeds $\frac{1}{\sqrt{2}}$ (for CHSH), the information gain will eventually exceed the message limit as the number of bits N increases.

1.3 Measures of information

This section establishes the formal foundations for quantifying information and correlations in classical and quantum regimes. We begin by defining the fundamental measures of uncertainty and unpredictability within discrete probability distributions. The analysis then transitions to the algebraic framework of density operators, extending these concepts to the statistical properties of quantum systems. The section concludes by addressing the informational gap between total and classical correlations in composite systems.

1.3.1 Shannon entropy

Information entropy quantifies the uncertainty associated with the outcomes of a stochastic process. Formally introduced by Shannon [160], this measure established the mathematical bedrock of information theory and provided the framework necessary for analyzing data compression and reliable communication over noisy channels. For a discrete random variable X taking values in the finite set with distribution $\mathcal{X} = \{x_i\}_{1 \leq i \leq n}$ with

probability distribution $\mathfrak{P}(X) = \{P(x_i)\}_{x_i \in X}$, the measure is defined as:

$$H(X) \equiv - \sum_{i=1}^n P(x_i) \log_d P(x_i), \quad (1.11)$$

where d is the base of the numeral system utilized. Our considerations concern binary data, so $d = 2$. This type of entropy describes the average unpredictability of a certain outcome. In the communication theory, Shannon entropy serves as the definitive measure for lossless data compression and the fundamental limits of information density. According to Shannon's source coding theorem, the entropy of a source sets a lower bound on the average number of bits required to represent a symbol without losing information [160]. This principle is operationalized in prefix codes, such as Huffman coding [83], which aim to approach the theoretical limit. Furthermore, Shannon entropy is the cornerstone of channel capacity calculations; it defines the maximum rate at which information can be transmitted reliably over a noisy medium [41].

Building upon the definition of Shannon entropy for a single variable, we can extend the framework for entropy measures for multiple random variables. The joint entropy, denoted as $H(X, Y)$ quantifies the total uncertainty associated with a pair of discrete random variables following a joint probability distribution $P(x, y)$:

$$H(X, Y) = - \sum_{x \in X} \sum_{y \in Y} P(x, y) \log_d P(x, y). \quad (1.12)$$

This measure captures the combined randomness of the system; if the variables are independent, the joint entropy is simply the sum of their individual entropy values, whereas any correlation between them reduces the joint uncertainty below this sum.

The uncertainty remaining in one variable when the value of another is known is quantified by the conditional entropy, $H(X|Y)$. It is defined as the expected value of the entropy of the conditional distributions $P(x|y)$, averaged over all possible outcomes of Y :

$$H(X|Y) = \sum_{y \in Y} P(y) H(X|Y = y) = - \sum_{x, y} P(x, y) \log_d P(x|y). \quad (1.13)$$

This leads to the chain rule for entropy: $H(X, Y) = H(Y) + H(X|Y)$, which mirrors the classical probability identity $P(x, y) = P(y)P(x|y)$.

The measure of the mutual dependence between the two variables is known as mutual information, $I(X : Y)$. Unlike conditional entropy, mutual

information is symmetric ($I(X : Y) = I(Y : X)$), and it is defined as the difference between the marginal entropy and the conditional entropy:

$$I(X : Y) = H(X) - H(X|Y) \quad (1.14)$$

Mutual information is non-negative and vanishes if and only if X and Y are fully independent variables. The Shannon limit (or channel capacity, C) is defined as the maximum possible value of this mutual information, optimized over all possible input probability distributions: $C = \max_{P(X)} I(X : Y)$. The Noisy-Channel Coding Theorem asserts that as long as the transmission rate R is less than C , there exists a coding scheme that allows the probability of error to be made arbitrarily small [160]. If $R > C$, however, the information loss becomes irreversible, leading to unavoidable data corruption regardless of the complexity of the error-correction code used.

1.3.2 von Neumann entropy

A different extension of entropy, fundamental to the field of quantum information theory, is the von Neumann entropy. It is defined for a quantum state described by a density matrix ρ as:

$$S(\rho) = -\text{Tr}(\rho \log_d \rho) = -\sum_i \lambda_i \log_d \lambda_i \quad (1.15)$$

This quantity generalizes the classical Shannon entropy within a description of a quantum system, measuring the degree of uncertainty inherent in a quantum system, while Shannon entropy captures uncertainty arising from a lack of knowledge about which state a system is in. For a pure state, where the system is in a single, well-defined quantum state, the von Neumann entropy is zero; conversely, it reaches its maximum value for a maximally mixed state, representing a total lack of information about the system's preparation. The joint von Neumann entropy (or the von Neumann entropy for a bipartite quantum state) is denoted as $S(\rho^{AB})$ and the conditional von Neumann entropy is given by:

$$S(A|B) = S(\rho^{AB}) - S(\rho^B). \quad (1.16)$$

1.3.3 Min-entropy

Another type of entropy, more often used in the context of randomness measurement, is called min-entropy. It is defined as:

$$H_\infty(X) = -\log_2(\max_{x_i \in X} P(x_i)). \quad (1.17)$$

This form of entropy reflects the unpredictability of the most probable outcome of an event. It is therefore directly linked to the probability of correctly guessing the value of a variable when an observer (e.g., an eavesdropper) guesses the most likely result [165]. In other words, it represents the minimum possible entropy value (hence the name) and serves as a lower bound for the Shannon entropy, with both measures coinciding in the case of a uniform probability distribution.

Additionally, the ϵ -smooth min-entropy, denoted as $H_\infty^\epsilon(X)$, formalizes the process of ignoring atypical sequences by maximizing the standard min-entropy over a set of alternative random variables X' whose probability distribution $\mathfrak{P}' = \{P'(x'_i)\}_{x'_i \in X'}$ are close to the actual distribution $\mathfrak{P} = \{P(x_i)\}_{x_i \in X}$. This proximity is strictly measured using the statistical distance (total variation distance), defined as

$$\delta(\mathfrak{P}, \mathfrak{P}') = \frac{1}{2} \sum_{x_i \in \mathbb{X}} |P(x_i) - P'(x_i)|,$$

where $\mathbb{X}$ is the common space over which both the random variable X and the alternative random variable X' are defined. Any distribution $\mathfrak{P}'$ that satisfies the condition $\delta(\mathfrak{P}, \mathfrak{P}') \leq \epsilon$ falls within an ϵ -ball around $\mathfrak{P}$, denoted as $\mathfrak{P}'_\epsilon(\mathfrak{P})$. Consequently, the ϵ -smooth min-entropy is formally defined as

$$H_\infty^\epsilon(X) = \max_{X': P' \in \mathfrak{P}'_\epsilon(\mathfrak{P})} H_\infty(X'). \quad (1.18)$$

Min-entropy is widely used as the metric of the randomness of generated random numbers in cryptographic applications. Its relevance arises from the fact that randomness extractors employ min-entropy to characterize the unpredictability of weak random sources, thereby ensuring that the extracted output is statistically close to a uniform distribution only when the source exhibits at least the corresponding amount of entropy. The conditional min-entropy is given by:

$$H_\infty(X|Y) = -\log_2 \left(\sum_y P(y) \max_{x \in X} P(x|y) \right). \quad (1.19)$$

The min-entropy of a quantum state, described by a density matrix ρ acting on a Hilbert space $\mathcal{H}$, is defined via the infinity norm (or spectral norm) as

$$H_\infty(\rho) = -\log_d \|\rho\|_\infty = -\log_d \lambda_{\max}, \quad (1.20)$$

where $\lambda_{\max}$ is the largest eigenvalue of the density operator ρ . The quantum min-entropy naturally lower-bounds the von Neumann entropy, $H_{\min}(\rho) \leq$

$S(\rho)$. Since $\lambda_i \leq \lambda_{\max}$ for all i , applying the strictly decreasing negative logarithm gives $-\log \lambda_i \geq -\log \lambda_{\max}$. The left side of the inequality can be multiplied by and summed over all the eigenvalues (which yields the von Neumann entropy), and the right side evaluates to the min-entropy, leading to the sequence:

$$S(\rho) = -\sum_i \lambda_i \log_d \lambda_i \geq -\log_d \lambda_{\max} = H_{\min}(\rho). \quad (1.21)$$

Remark on units of information The established inequality holds for any consistently applied logarithm base d . In the literature, the von Neumann entropy is often written using the natural logarithm ($d = e, \ln$) to yield *nats*. In cryptographic contexts, we typically employ the base-2 logarithm ($d = 2$) for Shannon and min-entropies to yield *bits*. Because a change of base simply rescales the quantities by a positive constant, the underlying bound is strictly preserved. For formal consistency, this thesis exclusively utilizes $\log_2$, expressing all evaluated entropy measures in bits.

1.3.4 Rényi entropy

While the Shannon and von Neumann entropies provide a foundational measure of uncertainty and information content, they can be viewed as specific instances of a much broader family of information measures. The generalization of the entropy function is called *Rényi entropy* [151] and is defined as:

$$H_\alpha(X) = \frac{1}{1-\alpha} \log_d \left(\sum_i P(x_i)^\alpha \right), \quad (1.22)$$

where α is the order of Rényi entropy ($\alpha \in \mathbb{R}, \alpha \neq 1$). The Shannon entropy is recovered in the limit as $\alpha \rightarrow 1$, while the min-entropy arises in the limit as $\alpha \rightarrow \infty$. The quantum Rényi entropy is:

$$S_\alpha(\rho) = \frac{1}{1-\alpha} \log_d \text{Tr}(\rho^\alpha). \quad (1.23)$$

Analogous to Shannon entropy, the von Neumann entropy arises in the limit as $\alpha \rightarrow 1$.

1.3.5 Quantum discord

Quantum discord has been identified as a fundamental measure of non-classical correlations that captures the quantum phenomena even in the

absence of entanglement [133, 75, 203]. Unlike entanglement, which relies on the non-separability of the density matrix, discord quantifies the discrepancy between total quantum correlations and the classical correlations accessible through local measurements [120].

To define this measure, let us consider a bipartite quantum system ρ^{AB} with subsystems ρ^A and ρ^B . The total correlations between these subsystems are quantified by the quantum mutual information, which is defined as:

$$I(\rho^{AB}) = S(\rho^A) + S(\rho^B) - S(\rho^{AB}). \quad (1.24)$$

While this quantity captures all correlations in the state, an alternative measure of correlations can be constructed by generalizing the classical concept of information gain (which is a reduction in uncertainty about A after knowing B). This quantity, which we denote as

$$J(\rho^{AB})_{\{\Pi_b^{1,y}\}} = S(\rho^A) - S(A|\{\Pi_b^{1,y}\}), \quad (1.25)$$

where $\{\Pi_b^{1,y}\}_b$ is the complete set of orthogonal projectors on B and

$$S(A|\{\Pi_b^{1,y}\}) = \sum_i p_i S(\rho_i^A) \quad (1.26)$$

is the conditional entropy of A given the measurement outcome on B , representing the information gained about subsystem A as the result of the measurement. These two quantities, although they are equal for the classical systems, diverge for the quantum states, due to the invasive nature of measurement, which irreversibly disturbs the state and destroys the quantum coherence that exists between subsystems. Consequently, the information accessible via local measurement J is generally strictly less than the total correlations I . The quantum discord is thus defined as the minimum difference between these two quantities over all possible measurements:

$$D(\rho^{AB}) = I(\rho^{AB}) - \max_{\{\Pi_b^{1,y}\}} J(\rho^{AB}). \quad (1.27)$$

In evaluating quantum discord, entropic calculations are typically constrained to qubit systems ($d = 2$) out of strict computational necessity. Quantifying the classical correlation of a bipartite state requires an optimization over all possible local measurements; for dimensions $d > 2$, this optimization is highly non-convex. As established by [82], computing quantum discord for arbitrary bipartite states is inherently NP-complete, with computational complexity scaling exponentially with the dimension of the

Hilbert space. Given the intractability of exact analytical and numerical evaluations for general qudit systems, this thesis restricts all subsequent calculations of quantum discord to qubits.

The usability of quantum discord lies in its ability to capture quantum advantages in information processing tasks where entanglement is either absent or insufficient [169]. It has been identified as the figure of merit for mixed-state protocols such as remote state preparation [45]. In this task, separable (non-entangled) states possessing non-zero discord can outperform certain entangled states, with the process's efficiency being bounded from below by the geometric measure of discord [45]. Similarly, in entanglement distribution, the amount of entanglement that can be successfully transferred between parties is strictly limited by the relative entropy of discord of the carrier particle [170]. In the transmission of correlations, discord represents the unavoidable loss of information when a quantum system is transmitted via classical measurement outcomes; perfect classical transmission is only possible if the initial state has zero discord [171]. It also serves as a method for considering quantum correlations for mixed states [26]. It has been also shown, using quantum discord, that separable states can still possess a quantum advantage, manifested in protocols such as deterministic quantum computation with one qubit [46].

1.4 Numerical methods

This section introduces basic concepts related to numerical optimization, as well as the method that has been strictly utilized in this thesis. We begin by introducing the fundamental concepts and definitions behind the numerical optimization process. We introduce the basic non-linear optimization algorithms utilized by various solvers. Furthermore, we introduce the basics behind the semidefinite programming, as well as the Navascués-Pironio-Acín (NPA) hierarchy, which is the core method used to characterize quantum correlations.

1.4.1 Non-linear optimization

Optimization is the study of extremal points and values of mathematical functions. It aims at minimizing (or maximizing) a real-valued function f , referred to as the *objective function*, within a given set of points $\Omega \subseteq \mathbb{R}^n$, referred to as the *feasible set*. A point $x \in \Omega$ is considered an optimal solution if it yields the best possible value of f according to the criteria

of the problem. In most engineering and economic contexts, optimization focuses on minimization, as any maximization problem can be converted by considering the negative of the objective function, $-f$.

A fundamental distinction in optimization theory is the classification of these optimal points based on the scope of their optimality. A local solution x^* is a point that provides the minimum value of f within a small, immediate neighborhood of the feasible space; that is, $f(x^*) \leq f(x)$ for all x in some neighborhood $B(x^*, \epsilon) \cap \Omega$. In contrast, a global solution x^{**} is the absolute minimum over the entire feasible set Ω , satisfying $f(x^{**}) \leq f(x)$ for every $x \in \Omega$. In convex optimization, any local minimum is guaranteed to be a global minimum, a property that greatly simplifies the search for an optimal solution. However, for non-convex functions, an algorithm may converge to a local minimum, requiring more complex global search strategies to find the absolute minimum. We say that the optimization is *constrained* when the feasible set Ω is strictly constrained, typically by detailed equations and inequalities (often in the form of a matrix). In an unconstrained problem, however, the objective function f is minimized over the entire space $\mathbb{R}^n$, meaning there are no restrictions on the values the decision variables can take.

When the objective function f or any of the constraints defining the feasible set Ω exhibit non-linear behavior, we can utilize *non-linear programming* (NLP) for optimization. Formally, an NLP problem involves search for a vector $x \in \mathbb{R}^n$ that minimizes $f(x)$ subject to:

$$\begin{aligned} g_i(x) &\leq 0, & i &= 1, \dots, m \\ h_j(x) &= 0, & j &= 1, \dots, p \end{aligned}$$

where at least one of the functions f, g_i , or h_j is non-linear. Unlike linear models, where the search space is a flat-sided polytope, the boundaries of Ω in non-linear optimization can be curved or even disconnected. This complexity introduces significant numerical challenges, as the curvature of the functions can create multiple local minima, making it difficult for standard descent-based algorithms to guarantee that a solution will indeed reach the global minimum x^{**} .

An algorithm is classified as *derivative-free* if it is aimed to solve an optimization problem without utilizing the first-order (gradient) or second-order (Hessian) derivatives of the objective and constraint functions, which means that these methods rely exclusively on function evaluations f rather than information from the tangent space or curvature. The utilization of such methods is required when the function is non-differentiable, discontin-

uous, or computationally expensive to evaluate, such as in simulation-based optimization, where an expression for the derivative does not exist.

1.4.2 Solvers

The practical implementation of the optimization theory relies on specialized computational tools known as solvers. These software engines execute numerical algorithms to converge toward an optimal solution iteratively. The choice of solver is dictated by the problem's mathematical structure – depending on the linearity or non-linearity of the objective and constraints, the convexity of the search space, the differentiability of the functions, the sparsity and scale of the constraint matrix, the presence of stochastic elements, among others.

One of the most prominent frameworks for addressing non-linear constrained problems is *Sequential Quadratic Programming* (SQP) [127]. Rather than relying on simple linear approximations, it systematically replaces the original non-linear problem with a sequence of localized *Quadratic Programming* (QP) sub-problems. At each iteration k , the algorithm formulates a quadratic metamodel representing the system's curvature, solving for a step direction d_k by minimizing:

$$\min_d \frac{1}{2} d^T B_k d + \nabla f(x_k)^T d \quad (1.28)$$

subject to the linearized constraints $A_k d + c(x_k) \leq 0$, where B_k is a symmetric matrix capturing the second-order sensitivity of the system, A_k denotes the Jacobian matrix of the constraints, and ∇f is the function gradient. The solver then repeatedly solves this structured sub-problem and advances $x_{k+1} = x_k + \alpha_k d_k$ (where α_k is the step length ensuring sufficient decrease) to navigate complex topographies, offering superlinear convergence for continuous systems, where the variables are interdependent.

When the required derivative matrices ∇f or A_k are unavailable or mathematically undefined, solvers must pivot to derivative-free architectures such as *COBYQA* [148]. This algorithm bypasses analytical differentiation entirely by constructing a local quadratic metamodel $Q_k(x)$ through multi-dimensional interpolation. The solver maintains a discrete set of sampling points $Y = \{y_1, y_2, \dots, y_m\}$ and determines the coefficients of $Q_k(x)$ such that the model matches the actual optimized function evaluations:

$$Q_k(y_i) = f(y_i), \quad \forall i \in \{1, \dots, m\} \quad (1.29)$$

The search for the next optimal point is confined within a boundary $\|x - x_k\| \leq \Delta_k$, known as a *trust-region*. As the algorithm progresses, it continuously updates both the trust-region radius Δ_k and the geometry of the interpolation set Y to strictly retain the set bounds. Because this algorithm carefully maintains a well-spaced geometric arrangement of its sample points, it doesn't rely on calculating exact local slopes. This makes it highly reliable for optimizing complex functions, where tiny noise would normally confuse and break standard gradient-based solvers.

1.4.3 Semidefinite programming

Regarding the topic of linear optimization (*linear programming* (LP)) and linear problems, they are formulated as the optimization of a linear objective function over a feasible set defined by a finite intersection of closed half-spaces. Formally, the LP seeks a vector $x \in \mathbb{R}^n$ that minimizes the inner product $c^T x$, subject to the affine equality constraints $Ax = b$ and the non-negativity constraint $x \geq 0$, where $c \in \mathbb{R}^n$ is an objective coefficient vector (or cost vector), which components define the weights of the decision variables within the linear objective function being optimized, $b \in \mathbb{R}^m$, and $A \in \mathbb{R}^{m \times n}$. The resulting feasible set, $\Omega = \{x \in \mathbb{R}^n \mid Ax = b, x \geq 0\}$, geometrically constitutes a convex polyhedron. Because the objective function is purely linear, its gradient is constant, meaning the contour lines of the objective form parallel hyperplanes. By the *Fundamental Theorem of LP* [23], if a bounded optimal solution exists, it is mathematically guaranteed to lie on at least one vertex of this polyhedral set, allowing algorithms to isolate the global minimum by either traversing the boundary edges or bisecting the interior space. This form of the LP problem definition is called a *primal LP*. While the primal LP minimizes the primary operational cost $c^T x$ over the column space of the decision variables, the corresponding dual LP maximizes the total implicit value of the bounded resources $b^T y$ over the orthogonal row space by optimizing a vector of dual variables $y \in \mathbb{R}^m$ that quantify the marginal change in the optimal objective value.

In this respect, *semidefinite programming* (SDP) [184] represents a strict algebraic generalization of LP, extending the optimization domain to the non-polyhedral cone of symmetric positive semidefinite matrices, denoted as $\mathbb{S}_+^n$. Formally, the standard primal SDP seeks a matrix $X \in \mathbb{S}^n$ to minimize the trace inner product $\text{Tr}(CX)$, subject to a set of affine equality constraints $\text{Tr}(A_i X) = b_i$ for $i = 1, \dots, m$, and the generalized matrix inequality $X \succeq 0$. Here, C and A_i are given symmetric matrices, and the positive semidefinite condition $X \succeq 0$ enforces that all eigenvalues of

X must be non-negative. The standard primal formulation of the SDP problem is therefore:

$$\begin{aligned} & \min_{X \in \mathbb{S}^n} \quad \text{Tr}(CX) \\ & \text{subject to} \quad \text{Tr}(A_i X) = b_i, \quad i = 1, \dots, m \\ & \quad \quad \quad X \succeq 0. \end{aligned} \tag{1.30}$$

On the other hand, the dual formulation constructs a strict mathematical lower bound on the primal objective by optimizing over a multiplier vector $y \in \mathbb{R}^m$ and a positive semidefinite slack matrix $S \in \mathbb{S}_+^n$, defined as:

$$\begin{aligned} & \max_{y \in \mathbb{R}^m, S \in \mathbb{S}^n} \quad b^T y \\ & \text{subject to} \quad \sum_{i=1}^m y_i A_i + S = C, \quad S \succeq 0. \end{aligned} \tag{1.31}$$

The values of $\text{Tr}(CX)$ and $b^T \cdot y$ are called the values of the primal and dual solution, and they satisfy the relation $\text{Tr}(CX) \geq b^T \cdot y$. For $C = \mathbf{0}$ or $b = 0$, we seek to verify if any solution, regardless if primal or dual, exists. We call it a *feasibility problem*.

The feasible set in an SDP is the intersection of the set of all positive semidefinite matrices X (a cone) that satisfy a set of linear affine constraints. This geometric structure allows SDP to natively encode complex non-linear quadratic constraints into strict linear matrix inequalities, while entirely preserving the convexity required to guarantee global optimality.

The practical utility of SDP extends across a broad spectrum of engineering and applied mathematics. For example, in combinatorial optimization, SDP relaxations provide mathematically rigorous approximation algorithms for NP-hard problems, most notably the Goemans-Williamson algorithm for the Max-Cut problem [71], which famously guarantees a solution within 87.8% of the true global optimum. Furthermore, SDPs have found critical applications in quantum information theory, as the physical requirement for quantum states to be represented by positive semidefinite density matrices perfectly aligns with the core geometry of the semidefinite cone.

1.4.4 Navascués-Pironio-Acín hierarchy

Introduced in [125, 126], the Navascués-Pironio-Acín (NPA) hierarchy establishes an infinite, convergent sequence of necessary conditions to characterize the set of quantum correlations. To circumvent direct optimization over

potentially infinite-dimensional Hilbert spaces, the hierarchy constructs a systematic series of outer approximations to the quantum set. At each discrete level k , the physical constraints are encoded into a moment matrix $\mathbf{\Gamma}$, formulated from the expectation values of measurement operator sequences. Because quantum mechanics requires any valid physical state to possess a positive semidefinite density matrix ($\rho \succeq 0$), the corresponding moment matrix must inherently satisfy $\mathbf{\Gamma} \succeq 0$. This algebraic condition allows each level of the hierarchy to be strictly formulated as an SDP relaxation. As $k \rightarrow \infty$, these relaxations asymptotically converge to the exact quantum set.

While the most general description of a quantum measurement utilizes Positive Operator-Valued Measures (POVMs), the NPA hierarchy structurally simplifies this requirement by optimizing exclusively over projection operators; because any POVM can be mathematically dilated into a standard projective measurement acting on a larger dimensional system without imposing upper bounds on the dimension of the joint Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$, this assumption incurs absolutely no loss of physical generality.

Although general quantum measurements are described by POVMs, the NPA hierarchy is restricted to projective operators without loss of generality. By Naimark's dilation theorem, any POVM can be written as $E_k = V^\dagger \Pi_k V$ with projectors Π_k where there exists an ancillary space $\mathcal{H}_{\text{anc}}$ and an isometry $V : \mathcal{H} \rightarrow \mathcal{H} \otimes \mathcal{H}_{\text{anc}}$. In the bipartite setting, this corresponds to embedding measurements into enlarged local Hilbert spaces $\mathcal{H}_A, \mathcal{H}_B$ (absorbing ancillas). Since the hierarchy allows finite but unbounded dimensions, this preserves all correlation statistics and leaves $\mathcal{Q}$ invariant. Consequently, the underlying local projection operators, denoted as $\Pi_i^{0,x}$ and $\Pi_j^{1,y}$, are strictly forced to satisfy fundamental algebraic properties mentioned in Section 1.1.2 and Definition 1.2.2. Because the hierarchy fundamentally probes spatial correlations across unspecified, finite-but-unbounded dimensions, the shift from POVMs to the projectors alters neither the observable trace statistics nor the boundary of the quantum correlation set $\mathcal{Q}$.

The hierarchical structure of the method is systematically defined by the maximum sequence length of the projectors: the first level derives from the set $\mathcal{T}_1 = \{\Pi_\mu\}$, the second from $\mathcal{T}_2 = \{\Pi_\mu \Pi_\nu\}$, and generally, the n -th level utilizes the set $\mathcal{T}_n$ comprising all products of n projectors. At any chosen level n , given the constructed set of operator sequences $\mathcal{T}_n = \{O_1, \dots, O_N\}$ (where each individual element O_j is explicitly defined as a product of measurement projectors, $O_j = \Pi_{\mu_1} \Pi_{\mu_2} \dots \Pi_{\mu_m}$, with sequence length $m \leq n$) the corresponding moment matrix $\mathbf{\Gamma}^n$ is defined entry-by-

entry via the expectation value $\mathbf{\Gamma}_{jk}^n = \langle \psi | O_j^\dagger O_k | \psi \rangle$. Crucially, this matrix is algebraically guaranteed to be positive semidefinite ($\mathbf{\Gamma}^n \geq 0$) because, for any complex vector $v \in \mathbb{C}^N$, the quadratic form $v^\dagger \mathbf{\Gamma}^n v$ expands to $\langle \psi | V^\dagger V | \psi \rangle$, where $V = \sum_j v_j O_j$. Since the inner product of the state $V|\psi\rangle$ with itself is mathematically non-negative, this evaluates to a non-negative value. This inherent non-negativity enforces the fundamental linear matrix inequality required by SDP solvers to compute the approximations.

Finally, $\mathcal{Q}_i$ is the set of probability distributions $\mathfrak{P}$ that admit a positive semidefinite i -th order moment matrix $\mathbf{\Gamma}^i$ over operator sequences $\mathcal{T}_i$. Enforcing quantum projector algebra and exact reproduction of $\mathfrak{P}$ yields a nested hierarchy $\mathcal{Q}_1 \supseteq \mathcal{Q}_2 \supseteq \dots \supseteq \mathcal{Q}$, where each successive level is mathematically at least as constraining as its predecessor since any lower-level set $\mathcal{T}_{n-1}$ can be fully reconstructed via linear combinations of elements within $\mathcal{T}_n$.

Physical statistics are encoded directly in moment matrices where the operator product reduces to a joint measurement projector; explicitly, for all index pairs (i, j) such that $O_i^\dagger O_j = \Pi_a^{0,x} \Pi_b^{1,y}$, whether arising from primitive generators (e.g., $O_i = \Pi_a^{0,x}$, $O_j = \Pi_b^{1,y}$) or composite monomials (e.g., $O_i = \mathbb{1}$, $O_j = \Pi_a^{0,x} \Pi_b^{1,y}$), the constraint $\mathbf{\Gamma}_{ij} = P(ab|xy)$ is imposed, thereby fixing specific entries of $\mathbf{\Gamma}$ to observed probabilities and restricting the feasible set of the associated semidefinite program to moment matrices consistent with the nonlocal correlations.

Because standard interior-point SDP solvers evaluating moment matrix $\mathbf{\Gamma}^i \succeq 0$ scale between $O(d^4)$ and $O(d^6)$, where d is the total number of elements (operator sequences) contained within your chosen set $\mathcal{T}_n$. The global time complexity therefore reaches an exponential $O(m^{4n})$ to $O(m^{6n})$ [89, 123], where m represents the total number of elemental, independent projectors required to fully describe your specific Bell scenario. This causes severe memory and floating-point limitations [143]. Consequently, while level $\mathcal{T}_1$ is computationally trivial but yields excessively loose bounds, levels $\mathcal{T}_2$ and $\mathcal{T}_3$ remain tractable only for minimal setups like bipartite CHSH, and level $\mathcal{T}_4$ and above are strictly intractable on standard hardware. To manage this, intermediate hierarchies, e.g. $\mathcal{T}_{1+AB} = \mathcal{T}_1 \cup \{\Pi_{\mu_A} \Pi_{\mu_B} \mid \Pi_{\mu_A} \in \mathcal{T}_1^A, \Pi_{\mu_B} \in \mathcal{T}_1^B\}$, which limit higher-order terms to inter-party products, are used to balance tighter constraints with computational feasibility [84].

The NPA framework is a primary numerical tool for quantifying quantum correlations and randomness, making it essential for device-independent quantum information processing. For instance, it provides rigorous security proofs in device-independent quantum key distribution [6, 141], explained

more in Chapter 5. Additionally, NPA is central to self-testing protocols [174], allowing researchers to certify specific quantum states and measurements based solely on observed input-output statistics.

As an outer convex relaxation of the quantum set, the hierarchy provides rigorous numerical bounds on quantum behavior rather than exact analytical solutions. This can be used to obtain, for example, tight lower bounds for both min-entropy [116] and conditional von Neumann entropy [94]. It is also the standard method for calculating the Tsirelson bound of arbitrary Bell inequalities [126]. Finally, its matrix-based formulation easily adapts to higher-dimensional systems; for models using qutrits or qudits, the framework simply scales its moment matrices to capture the additional measurement outcomes.

Chapter 2

Quantum cryptography

This chapter investigates the application of quantum information principles to cryptographic security, focusing on two central pillars: the distribution of secret keys and the generation of certified randomness. We first describe the framework of quantum key distribution (QKD) for establishing classical keys, contrasting standard implementation-dependent models with the device-independent (DI) approach, and reviewing specific protocol architectures. Subsequently, the chapter addresses the critical role of entropy as a resource, detailing the information-theoretic procedures of randomness extraction, expansion, and amplification required to transform raw quantum measurement outcomes into uniform and secure random strings.

2.1 Key distribution

The most fundamental goal of cryptography is the establishment of a secure communication channel between two distant parties, in a way that even if the eavesdropper knows the encrypted message that is being transferred, it is impossible for them to know the content. In history, many different types of basic ciphers have been used. In antiquity, people realized that to successfully cover the message, a different alphabet, or better yet, the shifting of the same alphabet, may be a sufficient disturbance. One of the first ciphers of this type for which we have historical records was used in the Bible, and it maps the alphabet (or syllabary) with its reverse. It has been present, for example, in Book of Jeremiah 25:26, where the word for Babylon has been changed to Sheshach (בבל → ששך) [101]. To decode this information, the reader has to have information about two details: what is the procedure that the reader has to use to return to the original

information (encryption method, in this case, alphabet substitution), and what the exact input to the method is, which can be changed for every word. In this case, it is the reversed original alphabet, but it can also be, e.g., just a partial shift of the original alphabet. We call this information a *cryptographic key*.

For most of human history, the cryptographic key could either be a physical element (like e.g., a rod in a skytale cipher in ancient Sparta or rotor position in Enigma) or some alphanumeric information that nevertheless could not be too complicated, as most encryption methods had to be calculated manually.

The introduction of modern computing fundamentally shifted the cryptographic landscape. Computational advancements facilitated the rapid analysis of classical manual encryption techniques (even through exhaustive brute-force attacks), while simultaneously enabling the development of more complex, computationally intensive encryption methods.

Around the same time, the formalization of information theory [160] provided a rigorous mathematical framework for the field. This transition established the precise constraints required for cryptographic security, centered on the concept of perfect secrecy. Shannon demonstrated that absolute secrecy is attainable only when the entropy of the key $H(K)$ is greater than or equal to the entropy of the message $H(M)$. This proof mathematically validated the One-Time Pad (OTP) as the only provably unbreakable system, contingent upon the key being truly random, equal in length to the plaintext, and never reused [161].

Furthermore, this era solidified Kerckhoffs's principle (or Shannon's maxim), which dictates that a system's security must reside solely in the secrecy of the key rather than the algorithm itself. Formally, this principle asserts that one should design cryptographic systems under the assumption that an adversary will eventually achieve full knowledge of the underlying method [161].

In modern cryptography, two types of encryption are often distinguished: *symmetric-key* and *asymmetric-key*. Symmetric encryption relies on a single shared secret to both lock and unlock data, often offering high-speed performance ideal for large files, though it suffers from the logistical hurdle of securely sharing that secret key between parties. In contrast, asymmetric encryption (or public-key cryptography) utilizes a mathematically linked pair consisting of a public key for encryption and a private key for decryption. While this approach is often more computationally demanding, it eliminates the need for a secure initial exchange, allowing anyone to send

an encrypted message that only the specific recipient can open.

The security of asymmetric cryptographic primitives is based on one-way functions (operations that are easy to compute but extremely difficult to reverse without additional information). These methods are linked to problems in the NP class: legitimate users can encrypt data and verify the results quickly, while attackers would need impractical time and resources to break the ciphertext. In practice, modern asymmetric algorithms rely on well-studied mathematical problems. The RSA algorithm depends on the difficulty of integer factorization, specifically recovering prime factors from a large composite number [152]. Elliptic Curve Cryptography (ECC) instead uses the elliptic curve discrete logarithm problem, achieving strong security with smaller key sizes due to the complex algebra of elliptic curves over finite fields [91]. Another example is ElGamal, which is an asymmetric scheme derived from the Diffie–Hellman key distribution protocol, based on the discrete logarithm problem in a cyclic group [58]. It is probabilistic (achieving semantic security – ciphertext reveals no information about the initial text), but incurs ciphertext expansion, with its output size two times longer than the plaintext.

This makes the current and future security of the information in asymmetric encryption reliant on persistence in the absence of solutions that could significantly accelerate the algorithms for certain problems. Regardless of the final solution for the $P \neq NP$ conundrum or the increase in the computational power (which can be omitted for sufficiently long cryptographic keys, it still makes plenty of messages exchanged in the past vulnerable if their encrypted forms were ever saved), there exist a class of problems that can be solved in a polynomial time, using a processing paradigm different from classical computers. One machine that, in principle, can solve such problems is a quantum computer. We denote this class of problems by BQP , and since 1995, it has been known that it includes the factorization problem [163], which is the safety condition for the widely used RSA protocol.

To mitigate this vulnerability, the cryptographic community has pivoted toward post-quantum cryptography (PQC): a class of algorithms designed to remain secure against both classical and quantum adversaries. PQC primitives are constructed upon mathematical foundations currently believed to be resistant to quantum speedup; they are not reliant on problems that are known to be in the BQP class. However, they still do not present *perfect forward secrecy*, it is not proven that the problems that constitute safety conditions for these protocols will not, in the future, be

vulnerable to other quantum algorithms. In principle, no public-key protocol can guarantee that.

The fundamental challenge in symmetric cryptography is the secure exchange of a secret key between two spatially separated parties, in the presence of an adversary. While the OTP method (which is one of the examples of the symmetric-key method) provides proven information-theoretic security, guaranteeing that the ciphertext yields no information regarding the message, it imposes a strict requirement: the key must be random, used only once, and have a length at least equal to that of the message. It rewards us, however, with the security against an eavesdropper that has unbounded computational power available. Consequently, the security of the communication reduces entirely to the security of the key distribution mechanism.

2.1.1 Quantum cryptography with classical keys

Classical methods for key distribution rely on computational complexity assumptions, such as the hardness of factoring large integers or computing discrete logarithms (e.g., Diffie-Hellman). These methods are vulnerable to advances in algorithmic efficiency and, crucially, to the potential emergence of fault-tolerant quantum computers.

In contrast, QKD offers a solution rooted in the laws of physics. QKD protocols ensure that any attempt by an eavesdropper to measure or copy the key carriers introduces detectable disturbances, thereby alerting the legitimate users to the breach before the key is used for encryption.

2.1.2 Protocols

The BB84 protocol [19], introduced in 1984, remains the foundational method for QKD. The first party, Alice, generates, using an unbiased random number generator, a string of bits. The string corresponds to the bits that should be transmitted to the second party, Bob, in the key exchange process. Additionally, for every bit transmitted, Alice should randomly choose a defined, orthonormal base (computational or Hadamard) and depending on that choice, prepare a qubit that corresponds to the value of the random transmitted bit ($|0\rangle$ and $|+\rangle$ often correspond to key bit zero and $|1\rangle$ and $|-\rangle$ to key bit one). This qubit is subsequently transferred to Bob using a quantum channel. The transmission can be potentially manipulated by an eavesdropper or disturbed by the noise. Later on, Bob randomly picks a measurement basis and performs a measurement. The

observable corresponds to one of the binary values.

However, the basis he used for the measurement can be different than Alice's. In this case, the probability distribution for measurement results will be uniform, and no meaningful information will be obtained. This is caused by the fact that they use mutually unbiased bases [54]. Strictly speaking, Bob is choosing his measurement basis y completely independently from Alice's preparation base x . When he conducts a measurement, he receives the result according to the conditional probability distribution $P(b|x, y)$, which, for this protocol, in a noiseless scenario with no eavesdropping, equals:

$$P(b = a|x = y) = 1, \quad P(b = a|x \neq y) = P(b = \neg a|x \neq y) = 1/2. \quad (2.1)$$

This repeats for n qubit transmissions. After this, both parties announce their basis choices in a form of strings x_n and y_n , they compare where $x_i = y_i$ and keep only these results a_i and b_i for which this is true. Statistically speaking, the more qubit transmissions they conduct, the closer the length of a_i and b_i should be to $n/2$.

In practice, the effective key length is significantly attenuated by intrinsic decoherence within the transmission channel and the perturbative effects of eavesdropping. For the least elaborate eavesdropper, who intercepts every qubit, measures it, prepares a new one according to the measurement, and sends this new qubit to Bob, the quantum bit error rate (QBER) will equal 25% (as she chooses the wrong basis 50% of the time, and a wrong-basis measurement yields a random result (50% error)) [70].

Beyond the basic intercept-resend model, more advanced man-in-the-middle strategies necessitate a more nuanced evaluation of the information-disturbance tradeoff, particularly when considering individual and coherent attacks. As demonstrated in [105], the security of realistic QKD implementations is not merely a binary state of interception but a gradient defined by the eavesdropper's optimization of her measurement probes to maximize information gain while minimizing the induced QBER to remain below the critical threshold. This relationship is fundamentally bounded by the Shor-Preskill security proof [164], which establishes that if the QBER exceeds approximately 11%, the information leaked to the eavesdropper potentially surpasses the information shared between the legitimate parties. Inspired by BB84, other protocols of this kind have been established since 1984. We call this class *prepare-and-measure*, as its security is based upon the prohibition of cloning of the unknown quantum state and the state collapse during the quantum measurement.

Another class of QKD protocols is based on entanglement and was established in 1991, by Artur Ekert [57]. Instead of Alice sending individual

states to Bob as in BB84, an untrusted central source distributes pairs of entangled particles, such as EPR pairs in the singlet state $\frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$. Each party randomly and independently selects a measurement basis from a predefined set of orientations to measure their respective particles. After the measurements are completed, the parties communicate over a public classical channel to identify the instances where their chosen bases coincided or were specifically correlated to extract the raw key bits. Security is verified by testing Bell's inequality on a subset of the measurement results; any eavesdropping attempt would reduce the entanglement, leading to a decrease in the Bell value that reveals the presence of a third party.

2.2 Device-independence

Information processing traditionally rests upon the fundamental assumption that the underlying hardware functions exactly as specified. In classical frameworks, any deviation from expected behavior is treated as a characterizable error to be calibrated or corrected. However, quantum information processing allows for a different approach, in which this requirement is relaxed. The user of the device does not have to trust the producer of the device or even know the details of how it was constructed. In a so-called *device-independent* approach (DI), the user can validate the correctness of the obtained results by only analyzing the output of the device, given the established input, provided that the operations made by the hardware are limited by quantum mechanics (which, in this universe, is a rather universal assumption).

DI was first introduced in [109], where the authors proposed the concept of a *self-checking source* to remove the assumption that the apparatus used to produce photons must be perfect. Their guarantee stems from a main structural theorem demonstrating that if certain EPR-type equations [11] are satisfied, the underlying quantum state must essentially be the orthogonal sum of EPR pairs.

DI QKD is conceptually rooted in the E91 protocol, as it employs an untrusted central source that distributes entangled photon pairs to two parties, typically Alice and Bob. The security of the quantum channel is certified through the loophole-free [16] violation of a Bell inequality. A *loophole-free* Bell test [76] ensures that observed correlations are strictly quantum and cannot be explained by classical, local theories with hidden variables. This requires closing two key experimental flaws. First, the locality loophole demands that one party's measurement choice cannot physi-

cally influence another party's outcome, and that all measurement settings are independent, free choices. If unclosed, a Bell violation could admit a local, classical description. Second, the detection loophole [68, 55] addresses unavoidable signal loss caused by channel absorption or device inefficiencies. If lost signals are simply rejected, an eavesdropper could exploit this data rejection to artificially manufacture a Bell violation using a locally deterministic strategy. While a Bell value exceeding the classical local bound $|\mathfrak{B}|_{\mathcal{L}}$ certifies the presence of non-local correlations and strictly bounds an eavesdropper's predictive power, it does not guarantee robust self-testing; therefore, it cannot completely rule out partially deterministic strategies and requires extensive privacy amplification to ensure secure outcomes.

Operationally, a CHSH-based DI QKD protocol runs sequentially by randomly alternating between *key rounds* and *test rounds*. In key rounds, the parties measure their shared states in fixed correlated bases to generate raw key material, whereas in test rounds, they execute the CHSH game to quantify the adversary's information regarding the key round outcomes.

For the prepare-and-measure type of QKD protocol, including BB84, it is, however, fundamentally not possible to achieve full DI. For that, no assumptions can be made regarding the internal workings or the dimensionality of the quantum devices used. However, this total lack of assumptions is fatal for one-way schemes because any observed data table can be perfectly reproduced using classical systems, provided those systems are of a sufficiently high dimension [135]. If an eavesdropper swaps the quantum systems for these high-dimensional classical states, they can extract full information about the key without ever being detected. The entire BB84 can be perfectly simulated by the parties simply exchanging a single classical bit, as long as their uncharacterized devices share some randomness [67].

To establish security for one-way protocols, we must rely on a *semi-device-independent* framework where the devices themselves remain uncharacterized, relying instead on a strict mathematical upper bound on the Hilbert space dimension of the communicated quantum systems. For example [135], like in a regular BB84, Alice operates a state preparation process that takes a classical input a and emits an unknown quantum state ρ_a , where only the dimensionality d is trusted. It is strictly assumed that these preparations are unentangled with any system held by the eavesdropper. Bob operates a corresponding measurement device that receives the system and, based on a classical input y , applies an unknown observable $M^{1,y}$ which yields an outcome b . The devices may possess shared classical variables λ , which are accessible to Eve but must remain strictly

uncorrelated from Alice and Bob’s input choices. We also assume the standard assumption of an isolated and shielded laboratory. By estimating the purely classical data table, represented by the probability distribution $\mathfrak{P}(B|A, Y) = \{P(b|a, y)\}_{a \in A, b \in B, y \in Y}$ over many iterations, the legitimate parties can bound the eavesdropper’s information and establish security against individual attacks, where Eve applies the same strategy to independently target each system sent by Alice, performing her measurements before the classical post-processing phase [154].

2.3 Randomness

Generating truly random numbers remains a persistent challenge within computer science and information technology. The capacity to produce strictly nondeterministic values is paramount for the security of modern cryptographic systems [157, 100, 146], as well as for physical and biological simulations [37], machine learning [92, 8], and various other advanced applications.

At present, the prevailing methodology relies entirely on the predictable mathematical manipulation of an initial integer seed. Because this process is inherently deterministic, it merely simulates randomness, functioning as what is formally known as a pseudo-random number generator (PRNG). Although a diverse array of PRNG algorithms exists, offering varying degrees of statistical quality in their output [185, 180, 61], they fundamentally cannot produce true randomness or a genuinely nondeterministic stream of bits. Given knowledge of the algorithm and its initial input (or seed), one can reproduce the entire output sequence, even if the output of such an algorithm presents high entropy. The generation of true randomness necessitates access to a fundamentally non-deterministic process.

Some solutions leverage physical processes characterized by inherent chaotic properties, such as atmospheric noise [3] or radioactive decay [1]. However, although these phenomena typically exhibit high entropy, they are not mathematically provably random. This theoretical vulnerability introduces the potential for partial predictability, which inherently degrades the final entropy of the generated values.

For example, predictable environmental noise exposes randomness generators to *state compromise extension attacks* [90], allowing an adversary who knows the previous state to exhaustively search the low-entropy refresh data to easily deduce the new internal state. Additionally, attackers can actively manipulate automated entropy estimators to force refreshes

with guessable data or entirely block secure refreshes, or they can flood the system with zero-entropy events [14]. Finally, predictable noise breaks complex pooling heuristics like Fortuna [62] – by testing minimal possibilities, an attacker can maintain complete knowledge of all entropy pools, permanently preventing the system from recovering to a secure state.

These methods can also be manipulated by a potential eavesdropper. For example, in [64], the authors investigate the vulnerability of using ambient radio frequency and atmospheric noise as an entropy source. Because the noise is gathered via a radio receiver, an attacker can intentionally inject a stronger, deterministic, and highly structured radio signal into the environment. The receiver locks onto the artificial signal instead of the chaotic atmospheric noise, allowing the attacker to control the output.

Furthermore, extracting data from such sources frequently necessitates reliance on specialized applications or third-party web services like [1, 3, 4]. These platforms process the physical phenomena often without providing verifiable proof that the claimed entropy source was genuinely utilized or remained immune to external manipulation. Consequently, users are forced to either implicitly trust these third-party providers or invest heavily in constructing their own sophisticated hardware infrastructure.

The proliferation of both RNG and PRNG methodologies necessitates a robust framework for their verification and comparative analysis. To address this, the National Institute of Standards and Technology (NIST) established a comprehensive suite of statistical tests designed to characterize and evaluate the suitability of various (P)RNG solutions [17]. However, as the authors explicitly caution, these statistical evaluations serve merely as a preliminary diagnostic tool to determine general fitness. Passing these tests does not substitute for rigorous cryptanalysis, nor does it replace the comprehensive certification methods required to conclusively validate randomness.

The efficacy of randomness generation is fundamentally tied to the non-deterministic nature of its entropy sources. Consequently, the probabilistic characteristics of quantum phenomena serve as an ideal foundation for entropy extraction, owing to their inherent unpredictability. To date, a diverse array of Quantum Random Number Generators (QRNGs) has been proposed [78], including, but not limiting to, entanglement-based [195, 96, 196, 121, 85], based on photon-number statistics [65, 150] or on binary measurement of coherent states [190, 119]. The existence of QRNG is crucial for the security of other means of quantum cryptography [70, 139], such as quantum key distribution (QKD) [19, 57, 128] or quantum digital

signatures [73]. Also in classical cryptography, an inadequate source of randomness can compromise any cryptographic protocol [72].

2.3.1 Extraction and amplification of randomness

In practical applications, even when a randomness protocol successfully generates entropy, the raw output rarely follows a perfectly uniform distribution. Instead, the source often yields biased results that, despite potentially possessing high min-entropy, remain statistically skewed. To mitigate this, randomness extractors are employed to process these biased raw bits into shorter sequences that are cryptographically near-uniform [173].

When dealing with QRNG, this bias typically stems from quantum signals being inevitably mixed with classical noise, such as electronic fluctuations or background detection.

An adversary might theoretically control this classical noise to gain partial information. For example, in systems relying on Single-Photon Avalanche Diodes (SPADs), an attacker with knowledge of or influence over the device's thermal and physical environment could exploit deterministic memory effects introduced by detector dead time, dark counts, and afterpulsing, which collectively degrade entropy and introduce sequential predictability into the raw bitstream [110, 87]. Similarly, in quantum random number generators based on laser phase reconstruction, the macroscopic hardware is inherently sensitive to environmental drift – an adversary could potentially introduce or monitor local acoustic vibrations and thermal changes to track the classical phase fluctuations that become inextricably mixed with the pure quantum signal [86].

Given that, a quantum extractor is required to distill the provable randomness from these deterministic classical components. By evaluating the min-entropy of the source, protocols like the Toeplitz-hashing extractor [34] can be applied to generate a final output that is ϵ -close to a uniform distribution. Trevisan's extractor is also notable in this context, as it is secure against quantum adversaries and allows weakly random seeds [48].

In contrast, randomness amplification is the more stringent task of taking a source of partially random bits and converting it into a source of fully random bits. While classical extractors can refine a single biased source, it is mathematically impossible to perform randomness amplification using only classical resources [153].

An example of the amplification protocol is the DI framework proposed by [149], which leverages the non-local correlations of quantum mechanics to map a partially deterministic source to a fully random output using the

minimal configuration of two spatially separated components. The protocol exploits the algebraic violation of a specific bipartite Bell inequality (structured as a modified Kochen-Specker pseudotelepathy game [9]) to certify entropy against the most general class of no-signaling adversaries.

2.3.2 Certification

If a user wants to certify randomness, they seek a rigorous, DI guarantee that a generated sequence of numbers possesses genuine, private randomness, independent of any assumptions about the internal workings, potential flaws, or adversarial preparation of the generating hardware. The certification process itself is grounded in the fundamental link between the non-local correlations of entangled quantum states and the inherent unpredictability of quantum measurement outcomes.

The idea of the DI randomness certification based on the Bell inequality violation was first conceptualized in [142]. The certification process calculates a strict lower bound on the min-entropy of the generated output string based on the observed Bell value $|\mathfrak{B}|$ [142, 116, 181, 20, 182, 134, 85]. Specifically, over n consecutive trials, the generated randomness is mathematically bounded by the inequality $H_\infty(R|S) \geq nf(|\mathfrak{B}| - \epsilon)$, where $|\mathfrak{B}|$ is the statistically estimated value of the CHSH expression derived from the observed data, R is the final out string, S represents the input string of randomly chosen measurement settings, $f(|\mathfrak{B}|)$ represents a theoretical bound on the min-entropy produced per single use of the system for a given Bell value. This can be estimated using NPA, or calculated exactly using a closed-form analytical expression. For the standard CHSH scenario, the minimum extractable randomness per trial as a function of the observed Bell violation $\mathfrak{B}$ is given by the formula [142, 5]:

$$f(|\mathfrak{B}|) = 1 - \log_2 \left(1 + \sqrt{2 - \frac{|\mathfrak{B}|^2}{4}} \right) \quad (2.2)$$

The total value of entropy generated is sometimes called *amount of randomness*. This certification method holds even if the abstract devices possess an internal memory, meaning the i -th measurement could theoretically depend on previous results and settings. Thus, the observed Bell violation provides a mathematical guarantee, under the assumptions provided, confirming that the apparent randomness is an undeniable product of intrinsic quantum unpredictability rather than an artifact of classical noise or preestablished entropy. To guarantee the validity of the bound, the sys-

tems must remain separated and strictly non-interacting during each individual measurement step. The technical details of quantum randomness certification are further explained in Chapter 5.

Chapter 3

Quantum Darwinism

The enigmatic nature of quantum mechanics is underscored by the measurement problem [156, 99], a fundamental quandary concerning the irreconcilable disparity between the unitary, reversible evolution of quantum states and the irreversible nature of measurement [155]. Wigner’s friend paradox encapsulates this conundrum, highlighting the profound philosophical implications of quantum measurement theory [191, 51].

The significance of this problem arises from a fundamental tension between quantum formalism and macroscopic reality. While the principle of superposition asserts that any linear combination of states is a valid configuration, our empirical observations are strictly confined to a classical world of localized, robust objects. In the quantum domain, states are characterized by extreme fragility; the traditional act of measurement appears to abruptly terminate a superposition, forcing the system into a single eigenstate. This disparity raises a foundational paradox: how can the enduring, stable macroscopic reality of our daily experience emerge from the inherently volatile and coherent building blocks of quantum mechanics?

In seeking to address the mysteries surrounding quantum measurement, the theory of quantum Darwinism (QD) [206] has garnered significant attention as a framework for understanding the transition from the quantum to the classical [200, 201]. QD posits that the role of the environment surrounding a quantum system is crucial, not merely as a source of noise, but as an active witness. In this chapter, we provide a brief introduction and overview to the topic of QD and the requisites of the state interaction that this theory provides. First, the description of the measurement model, which is the cornerstone of the theory, is provided. Subsequently, the phenomenon resulting from this model, environment-induced selection, and its

effects on our understanding of decoherence are briefly explained. Finally, we discuss how these phenomena lead to the emergence of the classical object, as seen by the QD.

3.1 Model of measurement

In [200] Wojciech Żurek elucidated the process occurring between certain parts of an interacting ensemble, aiming to explain how the basis of a particular measurement is formed. The quantum *system* ($\mathcal{S}$) that is a point of interest of a particular observation or measurement is here examined via an *apparatus* ($\mathcal{A}$), which establishes a nonseparable correlation with the initial system. The process in which the observed system interacts with the measuring apparatus, causing the system to become entangled with its degrees of freedom, is called *premeasurement* [77]. The third subsystem is called the environment ($\mathcal{E}$).

Two specific assumptions that ensure the premeasurement is physically consistent and mathematically tractable have been introduced [200]. First, the quantum system $\mathcal{S}$ is assumed to be perfectly isolated from the environment ($H^{(\mathcal{SE})} = 0$), ensuring that any decoherence of the system must occur through its interaction with the apparatus. Second, a temporal hierarchy is established: the premeasurement interaction between the system and the apparatus ($H^{(\mathcal{SA})}$) must be brief and dominate over any environmental coupling, allowing a nonseparable correlation to form before the environment begins to interact with our apparatus and share the state with it.

Finally, to avoid the complexities of energy exchange, it is assumed [200] that all vectors in the basis correspond to the same degenerate energy eigenstate of the apparatus Hamiltonian ($H^{(\mathcal{A})}|A_p\rangle = E|A_p\rangle$, where A_p is the apparatus eigenstate), satisfying the requirement that the premeasurement should not lead to an exchange of energy between the system and the apparatus. These constraints allow the analysis to focus purely on the information transfer and the resulting density matrix.

While the ($\mathcal{SAE}$) model relies on the idealized isolation of the system ($H^{(\mathcal{SE})} = 0$), it has been later suggested [204] that the ($\mathcal{SE}$) model represents the ubiquitous process of environmental monitoring. In this form, the environment is not a distant observer of an apparatus, but an immediate and ubiquitous monitor of the system itself. By allowing $H^{(\mathcal{SE})} \neq 0$, the requirement for a formal apparatus is bypassed; the environment's degrees of freedom, such as ambient photons or thermal fluctuations, directly intercept information from the system. This direct ($\mathcal{SE}$) coupling performs

a continuous, non-selective measurement that enforces einselection without the need for the premeasurement.

Consequently, the $(\mathcal{SE})$ interaction shifts the focus from controlled laboratory premeasurements toward the unconstrained dissipation of information into the environment. While the $(\mathcal{SAE})$ chain is designed to simulate the standard measurement process and amplify specific observables, the $(\mathcal{SE})$ model describes the mechanism by which a preferred basis is established by the environment. In the broader context of QD, this $(\mathcal{SE})$ model serves as the primary engine for generating the vast redundancy of information characteristic of objective classical reality.

In general, the $(\mathcal{SE})$ model provides the mechanism for state selection, but the $(\mathcal{SAE})$ model provides the architecture for observability. A detailed comparison allows for a better understanding of how *objectivity* emerges: a state is objective only if it can be found out by many independent observers who intercept different fragments of the environment. By analyzing the $(\mathcal{SAE})$ process, we can formally define how the environment transitions from being a source of noise to becoming a witness, thereby providing a comprehensive account of how the quantum-to-classical transition is completed.

It was established in [200] that during this natural process, the resultant classical state is determined by the *pointer basis* defined as the eigenvectors of the complete set of observables that commute with the Hamiltonian operator describing the apparatus-environment interaction. However, this strict condition defines the preferred states under idealized circumstances where the apparatus self-Hamiltonian is negligible, and its evolution is entirely dominated by the environment. In more realistic scenarios where the system exhibits non-trivial internal dynamics, this strict commutation requirement is generalized by the predictability sieve, which identifies the classical states as those most robust against decoherence.

The selection of the pointer basis is technically governed by the commutation relations between the system Hamiltonian $H^{(S)}$ and the interaction Hamiltonian $H^{(SE)}$. In the strong-coupling, the pointer states emerge as the eigenstates of the system observable $M^{(S)}$ within the interaction term $H^{(SE)} = \sum_i M^{(S)} \otimes \mathcal{E}_i$. Here, $M^{(S)}$ denotes the specific operator (such as position or spin) being monitored, while $\mathcal{E}_i$ represents the operators acting on the i -th degree of freedom of the environment, such as individual photons or air molecules. In this regime, the environment effectively performs a selective measurement of M , causing any state outside this basis to undergo rapid decoherence. However, when the internal dynamics $H^{(S)}$ are compa-

able to $H^{(\mathcal{SE})}$, the pointer basis must satisfy a more complex requirement: it must minimize the entanglement generated by the environment. For a standard harmonic oscillator, this process favors coherent states, as they remain uniquely localized in phase space under the simultaneous influence of internal evolution and environmental monitoring [204].

Since coherence is a quantum phenomenon, whenever a measurement, which is a process of transiting from quantum to classical data, occurs, it is also necessary that the decoherence takes place [206].

3.2 Environment-induced selection

Decoherence, a phenomenon arising from the interaction between a quantum system and its environment, lies at the heart of QD [206]. This process is essential for the emergence of classical behavior, as it results in the suppression of off-diagonal terms in the reduced density matrix between quantum states and the establishment of stable, *einselected* pointer states [200, 201].

In the QD, the environment is further recognized as a collection of subenvironments, which is modeled as a tensor product $\mathcal{H}^{(\mathcal{E})} = \bigotimes_k \mathcal{H}^{(\mathcal{E}_k)}$. This enables redundant encoding of pointer states across many fragments. The environment acts as a distributed information channel: system observables are independently imprinted onto subsystems. This redundancy allows multiple observers to access disjoint fragments and infer consistent system states, establishing effective objectivity [204].

The *environment-induced superselection*, or *einselection*, is the process of designating this specific preferred basis. The basis is stable under the interaction Hamiltonian, making it robustly encoded in the environment. As a result, the system performs effectively classically, exhibiting distinct qualities that are stable and easily observable without major disturbance. This is achieved by suppressing the coherence between different states of the pointer basis. *Einselection* contributes to the understanding of why, although being essentially made up of quantum particles, macroscopic objects seem to have clearly defined classical features [202, 203].

This designation of the preferred basis is formalized through the *predictability sieve*, a conceptual and mathematical tool used to identify the states most resilient to environmental monitoring. It treats the einselection as a selective pressure that probes the Hilbert space of the system. While a general quantum superposition is highly unstable, the pointer states are identified by their ability to minimize the loss of information to the envi-

ronment.

Mathematically, it operates by sifting through all possible initial pure states $|\psi\rangle$ and ordering them according to how well they retain their purity over time despite being monitored by their environment. Technically, this is achieved by maximizing a predictability functional, typically the von Neumann entropy or purity, where a state is deemed more classical if it minimizes entropy production or minimizes purity loss over a specific timescale [204].

By identifying these states, the predictability sieve provides a physical foundation for the emergence of objective reality. In most macroscopic interactions, such as those governed by the position-dependent coupling of collisions or thermal radiation, the sieve favors states localized in phase space. This provides a model of how we observe a world of distinct positions and momenta rather than the superpositions permitted by the Schrödinger equation.

Furthermore, this selection process serves as the necessary precursor to QD – only the states that pass through the sieve with their integrity intact are robust enough to redundantly evolve in the surrounding environment. Without this process, the environment would contain only incoherent noise rather than the structured and redundant information that allows multiple observers to reach a consensus on the state of a system.

3.3 Information redundancy

To this day, we need to recognize that the environment’s involvement in quantum measurement is a fundamental prerequisite for the operation of quantum devices. The emergence of classicality and the manifestation of measurement outcomes are driven by the proliferation of information into the environment [137, 205, 132]. This process, while essential for the objectivity of pointer states, renders quantum devices inherently susceptible to external manipulation and unauthorized access; the same redundancy that allows for independent observation also permits potential eavesdroppers to intercept fragments of the environmental witnessing without perturbing the system. Consequently, ensuring the security and integrity of quantum communication requires robust measures to safeguard against potential threats arising from environmental interactions and the dissemination of quantum information.

Information becomes intersubjective and effectively classical through its widespread dissemination, or proliferation, throughout the environment [7,

118]. In this capacity, the environment functions as a communication channel that encodes the eigenvalues of the system's pointer states across its numerous, disjoint degrees of freedom. This process is described as *information plateau* and is related to the behavior of the mutual information $I(\mathcal{S} : \mathcal{E}_f)$ between the system and a fraction f of the environment. It rises sharply for very small f and then flattens into a broad plateau at the level of the system's von Neumann entropy. We visualize this phenomenon in Figure 3.1. This indicates that nearly all classical information regarding the pointer states is contained within a tiny fragment of the environment, meaning an observer gains almost no additional knowledge by intercepting more of the environment, as the state of $\mathcal{S}$ has already been redundantly spread.

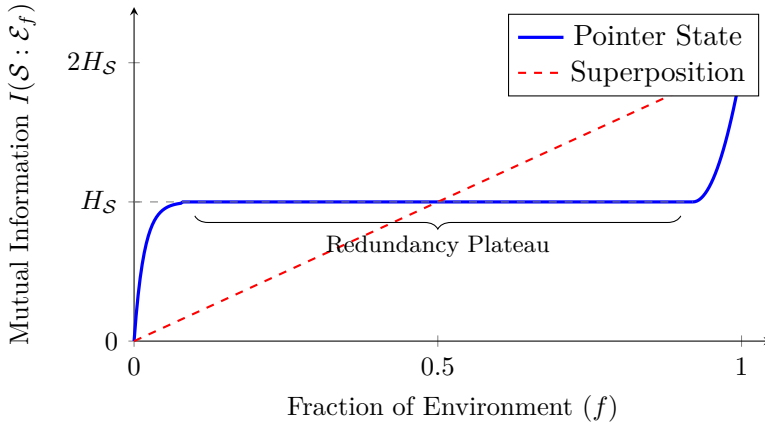


Figure 3.1: The Information Plateau in Quantum Darwinism. For pointer states, mutual information $I(\mathcal{S} : \mathcal{E}_f)$ quickly reaches the system's entropy $H_{\mathcal{S}}$, creating a plateau where additional environment fragments provide no new information. The superposition curve lacks a redundancy plateau, as information about non-selected states is not proliferated throughout the environment and can only be recovered by measuring nearly the entire global state.

The information plateau denotes a precise point in the fraction of the environment f available, independent of the size of the environmental portions under consideration, at which the mutual information between the system and various environmental components achieves a constant value. This constant number indicates that there is classical objectivity because the system's information is redundantly encoded across the envi-

ronment. [22, 206, 32, 112, 28]

The existence of this plateau provides the physical basis for objectivity and the consensus required for a classical world. While the total information shared between the system and the entire environment includes both classical records and quantum correlations, the plateau effectively bounds the information available to local observers. The quantum correlations are hidden in global entanglements that require the interception of almost the entire environment ($f \approx 1$) to recover. For the macroscopic observer, who only ever accesses a small fraction $f \ll 1$, the only available information is the redundant, classical variety. The length of this plateau determines the redundancy factor $1/f_\delta$, quantifying how many independent observers can simultaneously and non-invasively witness the same state.

The existence of these redundant records serves as the physical bedrock for the consensus required to perceive a classical world. Because information is encoded across numerous, disjoint subsystems of the environment, a multitude of independent observers can reach a consensus about the system's state simply by measuring their own local environmental samples. Recognizing the environment as a witness necessitates a fundamental shift in how we view the observer, leading to a different philosophical understanding of quantum mechanics. It suggests that *objective existence* is not an intrinsic property of an isolated quantum system, but rather a consequence of a state's ability to leave multiple, redundant imprints of itself throughout the environment. Because individual quantum states are considered "mostly information" and are too fragile to objectively exist until they are widely spread, reality itself becomes inextricably tied to the environment's capacity to act as a witness. This raises profound epistemological and existential questions about history: if the universe has a finite memory and old events are eventually overwritten by new ones, one must ask whether an event without a surviving environmental record truly happened at all [206].

Decoherence factor

The level of decoherence within a central system, resulting from its interaction with an N -partite environment, can be quantified using the collective decoherence factor, $\Gamma(t)$. To analyze the state of the system and a specific observed portion of the environment, we partition the M environmental subsystems. We focus on a fraction fM (where $f \in [0, 1]$) and discard the remaining $(1-f)M$ unobserved part through partial tracing. The collective decoherence factor is defined as the sum of the norms of the off-diagonal

terms remaining after this tracing process [200, 117]:

$$\Gamma = \sum_{i \neq j} \left(|\sigma_{ij}| \left| \prod_{k=1}^{fM} \gamma_{i,j}^{(k)} \right| \right), \quad (3.1)$$

where $\sigma_{ij} = \langle i | \rho_0 | j \rangle$ and $\gamma_{i,j}^{(k)} = \text{Tr} \left(\rho_{i,j}^{(k)} \right) = \text{Tr} \left(U_i^{(k)} \rho_0^{(k)} U_j^{(k)\dagger} \right)$, where $U_i^{(k)}$ is a unitary evolution operator on the subsystem k conditioned upon the observed system; $|i\rangle, |j\rangle$ are pointer states; $\gamma_{i,j}^{(k)}$ is an individual decoherence factor coming from the interaction with a single, k -th environmental subsystem; and ρ_0 is the initial state ($\rho_0^{(k)}$ is one of the subsystems of ρ_0).

The value of $\Gamma(t)$ monitors the transition from quantum to classical. When $\Gamma(t) = 0$, it indicates that full decoherence has occurred. The density matrix off-diagonal terms have vanished, and the system's state has effectively been reduced to a classical probability distribution over the pointer states. For $\Gamma(t) = 1$, it indicates that decoherence has not yet occurred, and the system maintains its original quantum coherences. In the context of QD, reaching $\Gamma(t) = 0$ is a necessary condition [117] for the emergence of objectivity, as it ensures the pointer states are the only ones that persist and can be redundantly imprinted across the environment. As the number of observed parts fM increases, it becomes easier for different observers to gain the same information about the system.

Chapter 4

Decoherence and QKD

The recognition of the environment's critical role in quantum measurement and decoherence opens the door to novel security threats that have not been thoroughly explored [115]. Analogous to the so-called van Eck attacks in classical computer science and networks, where electromagnetic emanations from electronic devices are intercepted to glean sensitive information, quantum systems may be susceptible to similar vulnerabilities [183]. In other words, the eavesdropper can pick up side-channel information – the attacks exploit unintended emissions from electronic devices, such as computer monitors and other equipment, to reconstruct the concealed information remotely using uncontrolled side-channels [166], which are often easily omitted in the security analysis of protocols [111, 104, 95, 175, 49, 106, 122, 124, 97, 98]. Thus, it is important in the context of quantum devices to investigate whether the vulnerabilities stemming from environmental interactions could be exploited to extract quantum information and thus compromise cryptographic protocols, posing security risks in quantum communication.

This chapter covers one of the main results of this thesis, which has been published in [129]. All the figures in this chapter are taken from this work. We investigated how the form of measurements provided by quantum Darwinism allows for the leakage of information in the standard BB84 QKD protocol. We analyzed the extent to which critical cryptographic key data is leaked during quantum measurement and evaluated the potential for an eavesdropper to recover this information via Van Eck side-channel attacks. The chapter is structured as follows: first, in Section 4.1, the methodology of the modelling of the measurement process in BB84 protocol is presented. We also introduce the generalization of a unified environment model, which

we call the layered-model. In Section 4.2, we present the analytical discussion, where we derive the explicit form of a key-rate for a simplified model of a single-qubit layered environment. Finally, in Section 4.3, we present the numerical analysis of distinguishability that is available to the eavesdropper.

4.1 Measurement and Decoherence in BB84

This section examines the quantum measurement process within the framework of the BB84 protocol. To isolate the fundamental mechanics of measurement, we model the physical exchange as a sequence of independent qubit-by-qubit transmissions, an approach that intentionally sets aside potential device memory effects [108]. This abstraction allows for a granular decomposition of the process into its constituent physical operations. While the complete measurement process traditionally encompasses both decoherence and orthogonalization [117], our analysis focuses exclusively on the decoherence phase. We also assume the ideal distinguishability of states at the receiver, as the impact of channel noise lies outside the current scope of this investigation. These considerations utilize the $(\mathcal{SAE})$ decoherence model.

In BB84, the state of a transmitted photon is based on two variables, randomly chosen by Alice – the measurement basis (either computational or Hadamard), which we denote as a binary value a and the key bit t . After Bob's measurement, the eavesdropper, Eve, knows which basis has been used (as it is shared publicly by the parties), but the key bit value is unknown. Therefore, she has to distinguish between two situations – when Alice sent a qubit corresponding to the bit value $t = 0$ or a qubit corresponding to the bit value $t = 1$:

$$|\phi\rangle_t^{(\mathcal{SAE})} = |\psi_{gen}\rangle_t^{(S)} \otimes |\psi_0\rangle^{(A)} \otimes \bigotimes_{l=1}^{N_l} \bigotimes_{e=1}^{N_{\mathcal{E}}} |\psi_0\rangle^{(\mathcal{E}_{l,e})}, \quad (4.1)$$

where in case of $t = 0$, $|\psi_{gen}\rangle_t^{(S)} = |0\rangle$ for $a = 0$ or $|\psi_{gen}\rangle_t^{(S)} = |+\rangle$ for $a = 1$ and in case of $t = 1$, $|\psi_{gen}\rangle_t^{(S)} = |1\rangle$ for $a = 0$ or $|\psi_{gen}\rangle_t^{(S)} = |-\rangle$ for $a = 1$. The form of ψ_0 depends on the measurement basis of Bob (denoted as b) and it also partly implies a form of interaction operator (which has to operate in the same orthonormal basis). For $b = 0$, we use $|\psi_0\rangle^{(A)} = |0\rangle$ and for $b = 1$ we use $|\psi_0\rangle^{(A)} = |+\rangle$. The environment consists of N_l separated layers, each with $N_{\mathcal{E}}$ qubits. The form of $|\psi_0\rangle^{(\mathcal{E}_{l,e})}$ is also dependent on

the form of the interaction between every single layer of the environment, as well as on the form of premeasurement. In our model, we consider that $|\psi_0\rangle^{(\mathcal{E}_{l,e})} = |\psi_0\rangle^{(\mathcal{A})}$ and construct the interaction operators accordingly.

The interaction between the system and the apparatus is modeled based on specific rank-1 projectors and a c-not operation, following the approach established in [115]. Consideration is also given to the fact that premeasurement may be performed using two mutually unbiased observables with projectors $\{P_0^{(\mathcal{S})}, P_1^{(\mathcal{S})}\}$ or $\{P_+^{(\mathcal{S})}, P_-^{(\mathcal{S})}\}$. Furthermore, the c-not operation is defined in connection with the specific measurement basis employed. Consequently, the premeasurement interaction is formulated in the following terms of unitary operators:

$$U_{b=0}^{(\mathcal{SA})} = P_0^{(\mathcal{S})} \otimes \mathbb{1}_2^{(\mathcal{A})} + P_1^{(\mathcal{S})} \otimes C_X^{(\mathcal{A})}(\alpha), \quad (4.2)$$

$$U_{b=1}^{(\mathcal{SA})} = P_+^{(\mathcal{S})} \otimes \mathbb{1}_2^{(\mathcal{A})} + P_-^{(\mathcal{S})} \otimes C_Z^{(\mathcal{A})}(\alpha), \quad (4.3)$$

where C_X and C_Z operations are defined as:

$$C_X = \begin{bmatrix} \sin(\alpha) & \cos(\alpha) \\ \cos(\alpha) & -\sin(\alpha) \end{bmatrix}, \quad (4.4)$$

$$C_Z = HC_X H, \quad (4.5)$$

with α set as a constant value. These operations constitute a generalization of the *c-not* quantum gate, which is known as *c-maybe* [178]. In our considerations, we use $\alpha = 0$. A correlation between the observed state and the apparatus is established by this model, which dictates the fundamental progression of the measurement process. If no information transfer occurred between $\mathcal{S}$ and $\mathcal{A}$, the acquisition of results by the receiver would be rendered impossible. This process is defined in relation to the type of measurement that Bob conducts; nevertheless, we only analyze the situations in which $a = b$, as these are allowed by the BB84 protocol. The interaction between the apparatus and the environment in our model is defined as:

$$\begin{aligned} U^{(\mathcal{AE})} = & \left(\Pi_0^{(\mathcal{E}_{N_l-1})} \otimes U_0^{(\mathcal{E}_{N_l})} + \Pi_1^{(\mathcal{E}_{N_l-1})} \otimes U_1^{(\mathcal{E}_{N_l})} \right) \times \\ & \vdots \\ & \left(\Pi_0^{(\mathcal{E}_1)} \otimes U_0^{(\mathcal{E}_2)} + \Pi_1^{(\mathcal{E}_1)} \otimes U_1^{(\mathcal{E}_2)} \right) \times \\ & \left(\Pi_0^{(\mathcal{A})} \otimes U_0^{(\mathcal{E}_1)} + \Pi_1^{(\mathcal{A})} \otimes U_1^{(\mathcal{E}_1)} \right). \end{aligned} \quad (4.6)$$

For the sake of simplicity, these interactions are assumed to occur sequentially. Specifically, the interaction between the apparatus and the primary layer of the environment is followed by successive interactions between subsequent environmental layers. Each multiplication factor represents the interaction between adjacent pairs within this hierarchy, including the interaction between the apparatus and the first layer. The interactions are thus modeled as a linear chain, wherein $\mathcal{A}$ interacts with $\mathcal{E}_1$, $\mathcal{E}_1$ subsequently interacts with $\mathcal{E}_2$, and the process continues through each successive layer $\mathcal{E}_{N_l}$.

Every interaction in the chain causes information to propagate from the previous layer to the next one. Projectors $\Pi_0^{(X)}$ and $\Pi_1^{(X)}$ ($X \in \{\mathcal{A}, \mathcal{E}_1, \dots, \mathcal{E}_{N_l}\}$) on the state of the apparatus are regular, single-qubit projectors for Hadamard and computational bases. In the numerical simulation, the interaction between the layers is based on the Haar distributed $U_0^{(X)}$ and $U_1^{(X)}$. Projectors on the preceding layers are constructed as Hermitian matrices that are parameterized using randomly chosen real matrices to take into account the unpredictability of the free-space quantum objects interacting with each other.

The model we propose here, which we call the layered model, is a generalization of a model that treats the environment as a unified ensemble of states, where it is assumed that the interaction between states is unlimited. It is, however, still a simplified toy model. The usage of such simplifications, due to the high complexity of any quantum description of classical objects, is a standard approach, see e.g. [44, 178]. It is based on the process of determining the outcome on the apparatus in the form of an interaction Hamiltonian described in [200], as well as the description of the environment-induced transition to the classical state presented in [201]. These foundational descriptions of the decoherence process underpin QD theory, which presents the prerequisites for the state to become a stable and classical pointer state.

Given that the bases for encoding and measurement are publicly disclosed during the sifting phase, the objective of the eavesdropper is reduced to the discrimination between two binary states. These states lead to distinct final configurations of the environment; however, access is restricted to a single environmental layer.

The eavesdropper is modeled as an observer who intercepts the environmental layer most proximal to the system. This positioning is critical; should access to a preceding layer be obtained, all subsequent layers are rendered redundant, as they provide no additional advantage for state dis-

crimination. Consequently, the information available to the eavesdropper satisfies the following sequence of inequalities:

$$I(\mathcal{S} : \mathcal{E}_1) \geq I(\mathcal{S} : \mathcal{E}_2) \geq \dots \geq I(\mathcal{S} : \mathcal{E}_{N_l}), \quad (4.7)$$

where $I(\mathcal{S} : \mathcal{E}_i)$ represents the mutual information between the quantum system and the i -th layer. The spread and accessibility of the information can be further constrained by noise and shielding. Because the interaction Hamiltonian between adjacent layers typically prevents the exhaustive transfer of information, the eavesdropper's optimal strategy is confined to the earliest available point of interception to maximize the available information. Consequently, the task for the eavesdropper is to implement an optimal measurement capable of distinguishing between two states composed of $N_{\mathcal{E}}$ qubits.

Additionally, only part of that layer might be distinguishable; thus, the measurement that the eavesdropper uses on her available layer should be an arbitrary projector of a rank 2^k , where k denotes the number of qubits that the eavesdropper can distinguish using the Van Eck-type antenna [183]. In our scenario, the side information is contained in the environmental qubits.

Helstrom state discrimination The eavesdropper's main goal is to distinguish between two different resultant states procured in the process mentioned in Section 4.1. This can be achieved with Helstrom measurement [74], which is the measurement that leads to the lowest possible error in distinguishing between two states. The probability of a correct guess is given by the Holevo–Helstrom theorem [81]:

$$P_{guess} = \frac{1}{2} + \frac{1}{2} \|\lambda\rho_0 - (1 - \lambda)\rho_1\|_1, \quad (4.8)$$

where λ is the probability of appearance of the first state (for uniform probability distribution $\lambda = 0.5$) and $\|\cdot\|_1$ is the trace norm.

4.2 Single-qubit layered environment

In this section, a simplified analytical model of the process described in Section 4.1 is constructed, wherein N_l single-qubit layers are employed ($N_{\mathcal{E}} = 1$). In accordance with the BB84 protocol, consideration is limited to instances where the key bit is accepted by both parties, an event observable via the classical, unencrypted channel. The basis that was used in the communication process is similarly announced; the eavesdropping task is

reduced to determining whether the state of the final accessible environmental layer (subsystem $\mathcal{E}_{N_l}$) indicates the leak of the information about the quantum state, suggesting that the exchanged key bit was 0 or that it was 1. Therefore, the eavesdropper should make a Helstrom measurement [74], the success probability of which is defined by (4.8). Furthermore, under the common assumption that Alice uses a near-perfect random bit generator, the prior probability equals $\lambda = 0.5$.

To model the interactions constituting $U^{(\mathcal{AE})}$ as in (4.6), that involve the interaction between the apparatus and the first layer, as well as between the layers, we need first to include the noise effect between the layers into an imperfect c-not operator, with the imperfection defined as the rotation of a regular c-not operator by angle α . To achieve that, we introduce the operator $Q(\varepsilon, \alpha) = \varepsilon \cdot \mathbb{1}_2 + (1 - \varepsilon) \cdot C_X(\alpha)$ (similarly for C_Z), where coefficient ε parametrizes the interaction between the apparatus and the environment (and also between subsequent layers) that limits the degree of interaction between two subsystems. However, Q is not unitary, therefore it must be transformed into a unitary operator. One way to perform such transformation will be to use some kind of matrix factorization that as a result provides a unitary matrix (preferably as close to the original as possible) and some additional product, which we can reject. QR factorization meets the requirement, as it decomposes any real square matrix into a product $Q = Q'R$, where Q' is an orthonormal matrix and R is an upper triangular matrix, and $R = \mathbb{1}$ when Q is unitary. By factorizing the matrix according to the steps in Appendix A, we obtain:

$$Q'(\varepsilon, \alpha) = \begin{bmatrix} \frac{p}{\sqrt{p^2+q^2}} & \frac{-q}{\sqrt{p^2+q^2}} \\ \frac{q}{\sqrt{p^2+q^2}} & \frac{p}{\sqrt{p^2+q^2}} \end{bmatrix}, \quad (4.9)$$

where $p = \varepsilon + (1 - \varepsilon)\sin(\alpha)$ and $q = (1 - \varepsilon)\cos(\alpha)$. With Q' , we now define the interlayer unitary interaction operator:

$$U = \Pi_0^{(X)} \otimes \mathbb{1}_2^{(Y)} + \Pi_1^{(X)} \otimes Q'(\varepsilon, \alpha)^{(Y)}, \quad (4.10)$$

where X and Y are consecutive environmental layer subsystems, and $\Pi_0^{(X)}$ and $\Pi_1^{(X)}$ are rank-1 projectors in the orthonormal basis of the subsystem X . Subsequently, we get from direct calculations that the guessing probability for the single-layer environment is given by

$$P_{guess}^{N_l=1} = \frac{1}{2} + \frac{1}{2} \cdot \frac{q}{\sqrt{p^2 + q^2}} \quad (4.11)$$

and for the two-layer environment

$$P_{guess}^{N_l=2} = \frac{1}{2} + \frac{1}{2} \cdot \frac{q^3}{(p^2 + q^2)^2 \sqrt{p^2 + q^2}}. \quad (4.12)$$

The eavesdropper is conducting the measurement on the last layer $\mathcal{E}_{N_l}$, as this is the only layer she has access to, and we assume the worst-case scenario in which she can obtain the information that dissipated to that layer fully. Thus, the mutual information between Bob's apparatus and the last layer $I(\mathcal{A} : \mathcal{E}_{N_l})$ should be directly related to P_{guess} . For instance, when the eavesdropper receives the bit 0, it can be stated, with the probability P_{guess} , that it is the right one, and with the probability $1 - P_{guess}$ that it is the wrong one. In other words, $P(e = 0|a = 0) = P_{guess}$ and $P(e = 0|a = 1) = 1 - P_{guess}$ and similarly for bit 1. This leads to the conditional entropy $H(\mathcal{E}_{N_l}|\mathcal{A})$, which is equal to $H(\mathcal{A}|\mathcal{E}_{N_l})$, as the situations in which $a = 0$ conditioned on $e = 0$ is only possible when Eve guesses correctly, therefore $P(a = 0|e = 0) = P_{guess}$. Additionally, $H(\mathcal{A}) = 1$ in this case, because Alice is using a random number generator with an approximately uniform probability distribution. This leads to the formulation of the mutual information:

$$\begin{aligned} I(\mathcal{E}_{N_l} : \mathcal{A}) &= H(\mathcal{A}) - H(\mathcal{A}|\mathcal{E}_{N_l}) \\ &= 1 + (1 - P_{guess}) \log_2(1 - P_{guess}) + P_{guess} \log_2(P_{guess}). \end{aligned} \quad (4.13)$$

Mutual information is therefore dependent solely on the value of P_{guess} . I. Csiszar and J. Körner [43] showed that parties can obtain a secret key only if the mutual information between the parties is larger than between Alice and Eve and the key rate is the difference between these two values: $r = I(\mathcal{S} : \mathcal{A}) - I(\mathcal{S} : \mathcal{E}_{N_l})$. We are considering only the situations in which communication leads to the accepted bit of the key, therefore $I(\mathcal{S} : \mathcal{A}) = 1$ and $I(\mathcal{S} : \mathcal{E}_{N_l}) = I(\mathcal{E}_{N_l} : \mathcal{A})$, thus the formula for key rate is dependent only on the value of P_{guess} as well:

$$r = (1 - P_{guess}) \log_2(1 - P_{guess}) + P_{guess} \log_2(P_{guess}). \quad (4.14)$$

For example, the key rate for the single-qubit layer with exactly one layer environment is given as:

$$r_{N_l=1} = 1 - \frac{1}{2} \left(\log_2 \frac{q^2}{p^2 + q^2} + \frac{q}{\sqrt{p^2 + q^2}} \log_2 \frac{\sqrt{p^2 + q^2} + q}{\sqrt{p^2 + q^2} - q} \right). \quad (4.15)$$

Several additional examples for varying numbers of layers N_l have been calculated. Based on the observed forms of these results, cf. (4.11) and (4.12),

as well as the key rate formulation in (4.14), the following conjecture for single-qubit layers is proposed:

Conjecture 1. *The guessing probability value, P_{guess} , for n single-qubit layers equals*

$$P_{guess}^{N_l=n} = \frac{1}{2} + \frac{1}{2} \cdot \frac{q^{2n-1}}{(p^2 + q^2)^{(2n-1)/2}}, \quad (4.16)$$

and the key rate for n single-qubit layers equals

$$\begin{aligned} r_{N_l=n} = 1 - \frac{1}{2} \cdot \log_2 \frac{(p^2 + q^2)^{2n-1} - q^{2(2n-1)}}{(p^2 + q^2)^{2n-1}} \\ + \frac{1}{2} \cdot \frac{q^{2n-1}}{(p^2 + q^2)^{(2n-1)/2}} \log_2 \frac{(p^2 + q^2)^{(2n-1)/2} + q^{2n-1}}{(p^2 + q^2)^{(2n-1)/2} - q^{2n-1}}. \end{aligned} \quad (4.17)$$

4.3 Distinguishability analysis

In this section, the decoherence-induced information leakage is analyzed through a numerical simulation of the BB84 protocol, specifically focusing on how the distinguishability of environmental states evolves as a function of the inter-layer noise parameter ε . The simulation facilitates an evaluation of the protocol by constructing the unitary operators $U^{(\mathcal{SA})}$ and $U^{(\mathcal{AE})}$ according to the forms established in (4.2) and (4.6), which are then applied to the initial environmental states defined in (4.1). To model the physical constraints of the eavesdropper, a partial trace is performed over all subsystems except for the targeted environmental layer, $\mathcal{E}_{N_l-1}$, as the system, apparatus, and distal environmental layers are assumed to be inaccessible to the adversary. This procedure is executed for both sets of states, when the initial one is $|0\rangle$ (or $|+\rangle$), and when it is $|1\rangle$ (or $|-\rangle$), thereby enabling the determination of the optimal guessing probability P_{guess} via the Helstrom bound in (4.8).

To demonstrate the decoherence occurring in the model, numerical simulations were performed for the rejected cases of the BB84 protocol, in which encoding and measurement are conducted in different, mutually unbiased bases. The outcomes of this process, quantified by the average collective decoherence factor (3.1) [117], are presented in Figure 4.1. Two primary phenomena are observed. First, the decoherence factor is found to decrease as the dimensionality of the initial environmental layer increases; for larger environmental sizes, the system approaches a state of full decoherence. This indicates that a larger environment facilitates a more robust propagation

of information from the apparatus, thereby inducing state collapse. Simultaneously, it is observed that a higher interaction degree ε (which describes the level of noise in the interaction) results in lower decoherence. In the limit where the noise factor approaches one, the decoherence is entirely suppressed.

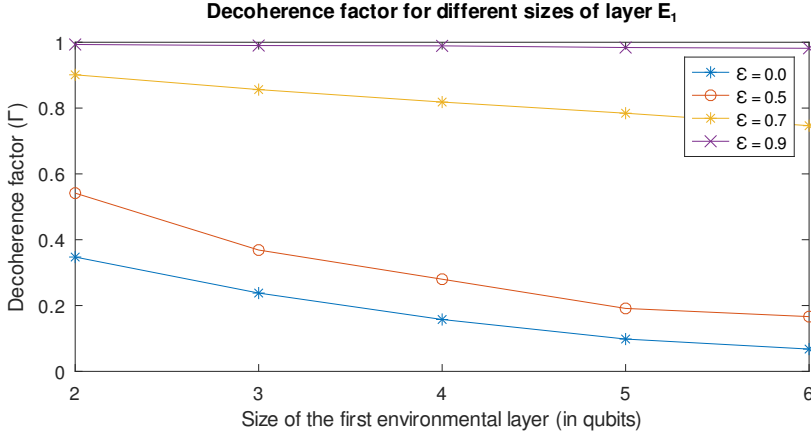


Figure 4.1: The dependence of the average decoherence factor Γ for the interaction $U^{(\mathcal{AE}_1)}$ given the size of the first environmental layer $\mathcal{E}_1$. The average is calculated over the cases rejected in BB84, for different interaction degree values (ε). Only the first decoherence interaction, between the apparatus and the first layer of the environment, is taken into consideration, as this is where the collapse of the state of the apparatus occurs.

Additionally, simulations were carried out for environmental layer sizes $N_{\mathcal{E}}$ ranging from 3 to 7 qubits. For each configuration, optimal projectors were prepared as Helstrom measurements, and the guessing probability was evaluated using the Holevo–Helstrom theorem [74, 81]. It was determined that the guessing probability varies according to the percentage of controlled and measured dimensions within the final (or the only one) environmental layer. This dimensionality increases twofold with the addition of each qubit. These results are presented in Table 4.1. Furthermore, it can be noted that the guessing probability for a corresponding degree of control increases with the total number of qubits in the layer; for instance, a 50% dimensionality control yields a probability of approximately 72% for $N_{\mathcal{E}} = 3$, whereas a value of 77% is reached for $N_{\mathcal{E}} = 7$. The observation that a larger environment is capable of accommodating more information and compensating for noise has been noted, for example, in [207, 208].

% of $\mathcal{E}$ controlled	$N_{\mathcal{E}} = 3$	$N_{\mathcal{E}} = 4$	$N_{\mathcal{E}} = 5$	$N_{\mathcal{E}} = 6$	$N_{\mathcal{E}} = 7$
1.5625	-	-	-	-	0.509
3.125	-	-	-	0.513	0.521
6.25	-	-	0.518	0.527	0.533
12.5	-	0.556	0.556	0.563	0.565
25	0.589	0.602	0.599	0.625	0.637
50	0.717	0.723	0.731	0.723	0.773
100	0.967	0.983	0.995	0.997	0.998

Table 4.1: Guessing probability of a key bit for an eavesdropper that uses Helstrom measurement on a controlled part of the environment's sole ($N_l = 1$) layer for $\varepsilon = 0$. It can be observed that the guessing probability is linearly proportional to the controlled part of the environment, counted as the percentage of dimension, and thus the control of the $N_{\mathcal{E}} - 1$ qubits leads to the guessing probability of around 75%.

The decoherence factor is zero ($\Gamma = 0$) in all cases where the key bit is successfully established. This follows from the fact that, when encoding and measurement are performed in the same basis, the state S does not undergo decoherence. From the outset, S is already a pointer state, rather than a mixture of pointer states. However, the information transfer still occurs between the apparatus and the environment, as it follows the process of subsequent interactions (4.6) between layers.

The next results are presented in Figure 4.2 and Table 4.2. First, from Figure 4.2 it can be observed that the visible loss of distinguishability i.e. the guessing probability for the eavesdropper in the considered sizes of environments, occurs for $\varepsilon \geq 0.5$, with the monotonic decrease. For $\varepsilon = 1$, there is understandably no interaction between the apparatus and the environment and thus no distinguishability, yet also no decoherence, as we noted from Figure 4.1 above. When additional layers are present, a visible decrease of distinguishability occurs between the first and the second layer, with a much smaller loss between the second and the third one, as shown in Table 4.2. That difference is also lower for higher values of ε , as P_{guess} overall decreases for higher values of ε .

The data presented in Table 4.1 and in Figure 4.2 strongly suggest that the higher number of qubits in environmental bases (including the last one, accessible to the eavesdropper) leads to a higher level of information extraction, even if the controlled percentage of the environment is the same. The guessing probability also fluctuates less for lower values of noise factor

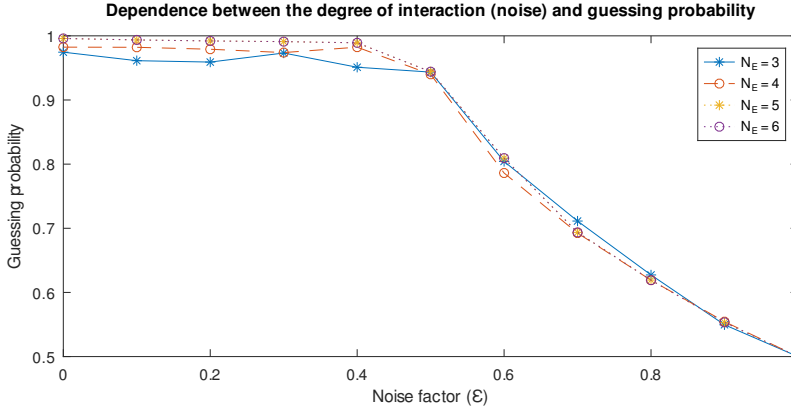


Figure 4.2: Guessing probability of a key bit for different values of ε degree of interaction (4.10) between apparatus and the environment for a single-layer environment (4.6). The eavesdropper fully controls the last (and only) layer of the environment.

ε , as seen in Figure 4.2 for $\varepsilon < 0.4$. This phenomenon is consistent with the observation of the *information plateau*, as described in Section 3.3.

N_l (number of layers)	$\varepsilon = 0.5$	$\varepsilon = 0.7$	$\varepsilon = 0.9$
1	0.871	0.658	0.549
2	0.823	0.646	0.536
3	0.818	0.645	0.536

Table 4.2: Key bit guessing probability for $N_E = 2$ and different values of ε degree of interaction between apparatus and the environment and different number of layers ($N_l = 1, 2, 3$).

The results of the numerical calculations offer insights into the dynamics of decoherence and its implications for quantum communication protocols. In particular, the findings suggest that a layered environment serves as a robust model for simulating decoherence phenomena. By examining the behavior of the decoherence factor Γ , as depicted in Figure 4.1, we infer that in real-world scenarios where Γ is expected to be on the order of 10^{-40} [210], the presence of a sufficiently large layer would likely be accessible to potential eavesdroppers.

Moreover, the analysis summarized in Table 4.1 reveals a clear trend. As the size of the environmental layer increases, the fraction of control required by an eavesdropper to improve the guessing probability decreases. Conse-

quently, the likelihood of a successful guessing attack on the BB84 protocol rises. The results for our toy-model suggest that even the interception of a minimal fraction of the total environmental Hilbert space may be sufficient to compromise the security of the protocol, facilitating a successful breach with disproportionately limited resources.

Furthermore, our investigation reveals a nuanced relationship between the size of the layer and the noise parameter ε . As illustrated in Figure 4.1, we observe that larger layers are necessitated to counterbalance higher levels of noise while keeping the same value of Γ , as evidenced by the increasing trend of ε . Conversely, as shown in Figure 4.2 and in Table 4.1 while a larger ε corresponds to a reduction in guessing probability, the presence of a larger layer confers enhanced robustness against noise, highlighting an intricate trade-off involved in optimizing layer size and noise parameters to mitigate eavesdropping risks effectively.

Consequently, these results shed light on the potential efficacy of employing multiple layers as a security measure. As indicated in Table 4.2, the utilization of multiple layers may introduce additional difficulty for eavesdroppers, thereby enhancing the difficulty of unauthorized access. This observation underscores the importance of devising sophisticated shielding mechanisms that facilitate necessary measurements while upholding stringent security standards.

Chapter 5

Randomness certification

The emergence of Bell's theorem as a cryptographic tool has revolutionized the generation of unpredictable measurement outcomes, providing a framework for randomness certification that is independent of the internal workings of the device [38]. This paradigm, initially presented in [142], leverages the violation of the CHSH inequality to provide a quantitative lower bound on the entropy produced by a quantum system. Building upon this foundation, [116] introduced a systematic method for analyzing various Bell expressions to determine their efficacy in the presence of white noise. Their work demonstrated that specific inequalities are capable of certifying up to two bits of randomness per measurement when evaluated using min-entropy.

While many Bell inequalities have been proposed and studied analytically, and the NPA provides a framework for numerical quantitative analysis, the choice of Bell tests in practical DI QRNG devices is often done without assessment and comparison, including in terms of noise requirements. This absence represents a significant gap in the transition from theoretical protocols to robust physical implementations. To address this deficit, in this work, we proposed a method for comparative analysis and certification of diverse Bell expressions, identifying the optimal configurations for entropy certification in the presence of noise. This chapter covers the set of results, which has been published in [130, 131]. All the figures and tables in this chapter are taken from these works. Specifically, we outline the potential benefits of Shannon entropy compared to traditional min-entropy measures, showing that it offers a more resilient lower bound in the presence of noise for randomness certification. Furthermore, we present a method for quantitatively analyzing Bell expressions used to certify ran-

domness in quantum systems. By means of this framework, we conducted a comprehensive analysis of more than half a million Bell expressions, which were chosen using the proposed sampling strategy. As an extension of these results, we further incorporate the concept of self-testing for boxes [12], and we utilize a similar analysis method for the certification of the randomness using three-outcome quantum states.

5.1 Device-independent randomness certification

The party that is willing to verify the unpredictable nature of the generated randomness can use the violation of any Bell inequality as a certificate of randomness [38]. This method, introduced by [142], relies on the assumption that two correlated systems are separated. It also requires an initial random seed to perform statistical tests verifying the violation of the Bell inequality. Therefore, it can be viewed as as a randomness expansion protocol [38], with randomness quantified using the entropy as the randomness measure. It was also shown that this approach to randomness certification is, in principle, DI [140]. This idea has been further investigated experimentally in e.g. [188, 103, 199, 144].

The randomness certification method established in [142] is centered on the CHSH inequality; however, as various alternatives exist, a selection must be made by the user or vendor of a QRNG device. This necessitates a comparative evaluation to determine which Bell inequality maximizes the unpredictability of the generated random bits.

In this section, a universal numerical method is described for the comparative analysis of Bell inequalities employed as randomness certificates. The primary objective of this analysis is to determine the maximal certifiable randomness, quantified here by the maximum value of the Shannon entropy. This is achieved through a sequence of numerical calculations, beginning with an examination of scenarios in which both parties perform measurements on entangled states.

To guarantee a valid DI randomness expansion, a protocol called spot-checking should be used [40, 159]. It is used to verify the integrity of quantum devices without testing every round, ensuring the observed correlations reflect true quantum behavior. Strong security comes from randomly selecting test rounds, which prevents adversaries from predicting checks and makes cheating statistically detectable. For a Bell inequality G , a trusted third party determines randomly (randomly chooses $t_i = \{0, 1\}$), with a small probability $0 < q < 1$ (the longer the output we want to obtain, the

smaller q needs to be, e.g. in [113] $q = \frac{\log^2 N}{N}$ has been used), whether a trial will be one of two options: testing the value of Bell expression or randomness generation.

5.1.1 Randomness extraction and certification

In this analysis, a bipartite scenario is considered as the source of randomness, following the standard framework for self-testing and DI QRNG [107]. To preserve device-independence, the analysis is constrained to the raw inputs and outputs of the devices.

However, certain external operational conditions are established. It is assumed that the devices are spatially separated, thereby precluding any signal transmission that could allow one party to manipulate results through the statistical imitation of entanglement. The measurement settings are chosen randomly (using a QRNG to determine), are mutually unbiased, and subsequent iterations are i.i.d. Additionally, the setup is assumed to be isolated from the external environment, with communication restricted solely to the controlled inputs and outputs defined by the QRNG protocol. Nevertheless, no other assumptions are made regarding their internal mechanisms, the execution of measurements, or the presence of potential biases.

The parties operate on binary outcomes, with the number of measurement settings restricted to a maximum of four for the first party (Alice) and three for the second party (Bob). For such a two-qubit system, the theoretical maximum for certifiable randomness is $H = 2$ for two outcomes, occurring exclusively when a uniform probability distribution ($P(a, b|x, y) = 0.25$) is achieved across all four possible measurement outcomes.

In this model, a quantum entangled Werner state of two particles is shared between Alice and Bob, which may be provided by a third party or established prior to the protocol. This state is defined as:

$$\rho = p \frac{\mathbb{1}}{4} + (1 - p) |\psi\rangle\langle\psi|, \quad (5.1)$$

where $|\psi\rangle$ represents a state that maximizes the Bell value and p denotes the noise level. The parties separately choose measurement settings and perform observations on their respective particles; however, only a specific subset of setting pairs will maximize the resulting Shannon entropy for a given Bell inequality.

We utilize a simplification of the generalized Bell operator (1.4), defined using the correlation operator (1.2), which we denote as:

$$G_\alpha = \sum_{i=1}^N \sum_{j=1}^M \alpha_{i,j} C(i, j), \quad (5.2)$$

where $-1 \leq \alpha_{i,j} \leq 1$ and N and M denote the number of measurement settings for Alice and Bob, respectively, with i and j labeling their corresponding settings. The operator in this form can be described by its coefficient matrix:

$$\alpha = \begin{bmatrix} \alpha_{1,1} & \alpha_{1,2} & \dots \\ \alpha_{2,1} & \ddots & \\ \vdots & & \alpha_{N,M} \end{bmatrix}. \quad (5.3)$$

However, in the entropy-based analysis, it is more convenient to work directly with the underlying probability distributions. Let Alice's measurement outcome be a and Bob's be b , each associated with projectors $\Pi_a^{0,x}$ and $\Pi_b^{1,y}$, respectively. The elements of the corresponding joint probability distribution $\mathfrak{P}(A, B|X, Y)$ are then

$$P(a, b|x, y) = \text{Tr} \left[\rho \left(\Pi_a^{0,x} \otimes \Pi_b^{1,y} \right) \right]. \quad (5.4)$$

In the binary case, outcomes satisfy $a, b \in \{-1, 1\}$. We define a correlator in the form of:

$$\bar{C}(x, y, \mathfrak{P}) = \sum_{a \in A} \sum_{b \in B} a \cdot b \cdot P(a, b|x, y) \quad (5.5)$$

By combining this definition with (5.4), we obtain the relation between (1.2) and (5.5) is

$$\bar{C}(x, y, \mathfrak{P}) = \text{Tr}(\rho C(x, y)). \quad (5.6)$$

Given that, the Bell expression, defined as a function of correlator and parametrized by α takes the form:

$$\mathfrak{B}_\alpha(\mathfrak{P}) = \sum_{i=1}^N \sum_{j=1}^M \alpha_{i,j} \bar{C}(i, j, P). \quad (5.7)$$

To employ this expression as an inequality-based randomness certificate, the user must also specify Tsirelson's bound $|\mathfrak{B}|_{\mathcal{Q}}$ and the pair of measurement

spot-settings (x_0, y_0) , which are selected to maximize the certified randomness. The value of the expression for a Werner state with noise level p and quantum bound is given by $|\mathfrak{B}|_p$ is given by $(1 - p)|\mathfrak{B}|_{\mathcal{Q}}$. Consequently, a single protocol R can be represented as a set:

$$R = \{\alpha, |\mathfrak{B}|_{\mathcal{Q}}, x_0, y_0\}. \quad (5.8)$$

5.1.2 Bounding the probabilities

Expressions (5.5) and (5.7) show, that to calculate the value of the Bell expression, we should use the probabilities of the quantum measurement results for the given measurement settings. Thus, we need to establish the bounds on these probabilities allowed by quantum mechanics.

This step utilizes the NPA [126, 125] to obtain the probability bounds, as a form of relaxation. It provides an infinite hierarchy of semidefinite constraints that any set of quantum correlations must satisfy. Each level of the hierarchy can be formulated as an SDP problem, allowing for efficient numerical optimization. The method analyzes probability distributions arising from projective measurements performed by two parties (5.4). In our case, the measurements are binary, thus the results for Alice and Bob are constrained to $a, b \in \{-1, 1\}$.

The most basic utilization of this technique, presented in [126], is the bounding of the maximal quantum violation ($|\mathfrak{B}|_{\mathcal{Q}}$). To obtain this value for a Bell expression $\bar{G}$, we need to solve an SDP maximization problem:

$$|\mathfrak{B}|_{\mathcal{Q}_i} = \max_{P \in \mathcal{Q}_i} \mathfrak{B}_\alpha(\mathfrak{P}). \quad (5.9)$$

Maximizing this over each level of NPA hierarchy yields an SDP with solution $\mathfrak{B}_\alpha(P)_{\mathcal{Q}_i}$ (where $\mathcal{Q}_i$ is the set of quantum behaviors for the i -level of NPA hierarchy), which serves as an upper bound to the true quantum value $\mathfrak{B}_\alpha(P)_{\mathcal{Q}}$. Increasing the level systematically tightens the bound (or keeps it unchanged), and the sequence converges to the exact quantum limit in the infinite limit.

For any Bell inequality-based protocol R , we can establish a set of linear expressions $\{L_i\}_i$:

$$L_i(P, x_0, y_0) = \sum_{a,b} c_i^{(abx_0y_0)} P(a, b|x_0, y_0), \quad (5.10)$$

where $c_i^{(abx_0y_0)}$ is a constant and (x_0, y_0) are the spot-settings, which are specified for each optimization. For every linear expression, we can now

conduct an NPA optimization. Consider the following optimization problem:

$$\begin{aligned} \max_P \quad & L_i(P, x_0, y_0) \\ \text{subject to} \quad & \mathfrak{B}_\alpha(\mathfrak{P}) - (1 - p)|\mathfrak{B}|_{\mathcal{Q}} = 0. \end{aligned} \quad (5.11)$$

Using the NPA method, we formulate (5.11) and using the SDP solver, we receive the expression's upper bound (to obtain a lower bound, we need to minimize). In our case, the optimization has been computed using a Q_2 level of the NPA hierarchy.

To be precise, we conduct the NPA-based optimization for the set of linear expressions (5.11) for the constant coefficients $c_i^{(abxy)}$ that equal:

$$c_1^{(-1,-1,x_0,y_0)}, c_2^{(-1,1,x_0,y_0)}, c_3^{(1,-1,x_0,y_0)}, c_4^{(1,1,x_0,y_0)} = 1, \quad (5.12)$$

and the remaining constants $c_i^{(abxy)} = 0$. We progress with the SDP optimization for all possible measurement outcomes ($a = -1, b = -1$; $a = 1, b = -1$, etc.) and the settings are chosen to maximize entropy with the absence of noise ($p \approx 0$ relates to $H \approx 2$). These cases can be recognized by the lower and upper bounds for each outcome, which are approximately 0.25.

5.1.3 Calculating entropy

The standard (e.g. [38, 142, 39, 116]) approach to the Bell certification is based on independent optimization of the outcomes: for a given Bell inequality, we determine its value and then maximize the probabilities of individual outcomes. However, when every outcome is maximized independently, we omit the natural constraints that result from the probability properties – all outcomes cannot be maximized at the same time, and maximization of one outcome will affect the value of the remaining.

This fact does not interfere with the certification on the value of min-entropy, as in that situation, we only utilize the highest probability. However, for the certification on the value of Shannon entropy, even if a single probability is high, the result is influenced by the total probability distribution. The quantum behavior that maximizes min-entropy might likely not be the one that maximizes the value of Shannon entropy.

Optimization (5.11) can be used to establish the bounds on probabilities allowed by quantum mechanics. These bounds can be used as constraints on the probability distribution. Essentially, we can use NPA to lower and

upper bound any linear probability equation, and these results can be used as constraints on the non-linear optimization of the Shannon entropy:

$$\begin{aligned}
 \min_{\mathfrak{P}} \quad & - \sum_{i \in \mathfrak{P}} H(\mathfrak{P}) \\
 \text{subject to} \quad & \forall_{i \in N_P}, l_i \leq P_i \leq u_i, \\
 & \sum_{P_i \in \mathfrak{P}} P_i = 1,
 \end{aligned} \tag{5.13}$$

where H is the non-convex optimized function. The elements of the quantum behavior, $\mathfrak{P} = \{P_i\}_i$ are the variables to be optimized and are bounded, with l_i denoting the lower bounds and u_i the upper bounds. In principle, this can be used for any non-convex problem that can be bounded using the NPA, which is any problem that requires the characterization of the correlations that arise from locally measuring a single part of a joint quantum system. In our certification method, the optimized function is the Shannon entropy.

We utilize the COBYQA [147, 148] solver. A key feature of it is that it always respects bound constraints throughout the optimization process, which makes it suitable for a problem bounded with NPA relaxation. However, as this problem is non-convex, it has many local minima, where the optimizer may get stuck. To avoid that, we used the basin-hopping global optimization technique [187], which performs a random perturbation of coordinates with every repetition and accepts the new coordinates based on the minimized function value. In this optimization, we have settled for 1500 iterations each, as for the lower number of iterations, the optimizer still was sometimes not able to achieve the global minimum.

The problem of reliable Shannon entropy estimation for QRNG processes has been initially studied in [79]. They have shown a memoryless semi-DI QRNG scheme, as well as a generic method for semi-DI QRNG rate computation. They have, however, made some assumptions that reduce the applicability of their method, e.g., they conduct a linearization of the entropy function and, based on that linearization, they optimize the linear constraints over the set of quantum behaviors that describe the correlations.

Our method, although also uses Shannon entropy for randomness estimation, relaxes some of these assumptions – it can be used for full DI protocols, it does not require a linearization (it relies on non-linear optimization, bounded by the SDP-obtained lower and upper bounds, instead),

and it uses a set of constraints that is based purely on the probability distribution of the correlations.

5.1.4 Shannon entropy certification

The practical usability of Shannon entropy in the extraction of quantum randomness is underlined by the existing experimental results and the implementation in real hardware. For example, in [66], Shannon entropy serves as the quantitative foundation for distinguishing quantum-mechanical effects from classical noise (including e.g. electronic noise) to ensure that their random bits is originating solely from the quantum entropy). The authors utilized Shannon entropy because it provides a direct mathematical framework to quantify the average information content in the Gaussian distribution of vacuum states. The authors partitioned the total entropy into distinct quantum and classical components. The total entropy is first evaluated, and the estimated contribution from classical effects, such as electronic noise and local oscillator imbalances, is subtracted. This allows the exact amount of genuinely quantum mechanical entropy to be determined. In this setup, it was found that even with a classical noise contribution of 1.75 bits, a significant 3.25 bits of unique quantum entropy remained per sample. Consequently, while min-entropy remains the standard for worst-case guarantees, a higher extraction rate was justified, which might have been unnecessarily penalized by a more restrictive min-entropy measure.

If the samples are produced independently, a property called the Asymptotic Equipartition Property (AEP) holds [165]. For a sequence of i.i.d. random variables $X^n = X_1, X_2, \dots, X_n$, the Asymptotic Equipartition Property (AEP) can be formulated using the ϵ -smooth min-entropy (1.18), converging to the Shannon entropy H , as $n \rightarrow \infty$:

$$\lim_{n \rightarrow \infty} \frac{1}{n} H_{\infty}^{\epsilon}(X^n) = H(X) \quad \text{for all } \epsilon \in (0, 1). \quad (5.14)$$

In essence, this property implies that as the number of samples increases (for example, when analyzing larger sets of QRNG-based values), the proper certification of Shannon entropy becomes increasingly important, as it characterizes the asymptotic rate. Indeed, for a generation of a single sample, we need to assume that the worst possible scenario can happen, and therefore, min-entropy must be considered the certified lower bound. As the number of samples grows, the likelihood that most individual sample values cluster near their respective lower bounds decreases. This implies that, for sufficiently large sample sizes, the aggregate entropy of the set will tend

<i>Variables</i>	
P	Probability of measurement outcome.
<i>Inputs</i>	
$\mathfrak{B}$	Bell expression used as a certificate.
$ \mathfrak{B} _p$	Considered Bell expression value.
L	Set of linear expressions on the probabilities of results in a form of $L_i(P, x_0, y_0) = \sum_{a,b} c_i^{(abx_0y_0)} P(a, b x_0, y_0).$
x_0, y_0	Spot-setting for measurements.
Protocol	
1.	Using NPA, establish an upper (u_i) and lower (l_i) bounds of $L_i(P, x_0, y_0)$, subject to $\mathfrak{B}(P) - \mathfrak{B} _p = 0$, where $ \mathfrak{B} _p = (1 - p) \mathfrak{B} _{\mathcal{Q}}$ for a noise level p .
2.	Using a non-linear optimization, minimize $\sum_{a,b} H(P(a, b x_0, y_0))$, where every linear expression in a form of (5.11) is constrained by l_i and u_i only and H is the objective function (in our case – Shannon entropy).

Figure 5.1: Brief description of proposed randomness certification method using Shannon entropy.

to deviate from the min-entropy-based lower bound. Min-entropy certification, therefore, becomes increasingly conservative, providing a lower bound on the amount of randomness that can be extracted from the system. For a large set of samples, the entropy of the whole set tends to converge to the average value, which is the Shannon entropy.

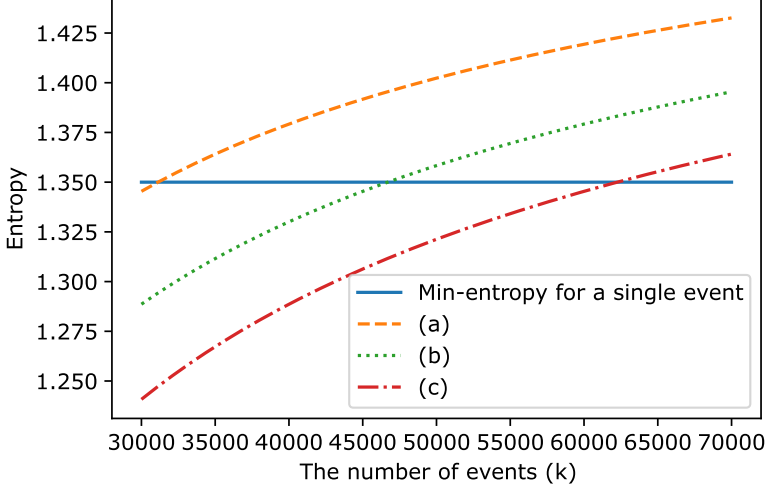


Figure 5.2: Shannon entropy-based min-entropy sequence lower bounds based on (5.15), per event in the sequence, compared to the min-entropy for a single event. Three statistical distance bounds ϵ have been analyzed: (a) $\epsilon = 10^{-8}$; (b) $\epsilon = 10^{-12}$; (c) $\epsilon = 10^{-16}$. In (a), for $k \approx 30k$ (and $k \approx 45k$ in (b), and $k \approx 62.5k$ for (c)), this lower bound (divided per event) exceeds the maximal single-event min-entropy value for CHSH.

The estimated Shannon entropy can also be used to determine the effective number of bits that can be extracted from the quantum source. Randomness extractors use the min-entropy to quantify how much true unpredictability a weak random source has, so they can guarantee that their output is close to uniform only when the source has at least that much entropy. In [80] it has been shown, however, that for several independent samples k , the conditional min-entropy of the source X^k , given the setting Y^k , is close to the Shannon entropy. For any statistical distance ϵ there exists a distribution $P(\bar{X}|\bar{Y})$, which is at most $\epsilon/2$ from (X^k, Y^k) and satisfies:

$$H_\infty(\bar{X}|\bar{Y}) \geq kH(X|Y) - 6\sqrt{k \log_2 \frac{1}{\epsilon} \log_2 |X|}. \quad (5.15)$$

This result provides a quantitative connection between Shannon entropy

and min-entropy. For sufficiently long sequences of independent samples, the conditional min-entropy of the joint distribution grows approximately linearly with the conditional Shannon entropy.

As a consequence, the total amount of extractable randomness from the sequence is more closely related to Shannon entropy, than by the min-entropy of any single event. We present this phenomenon in Figure 5.2.

Furthermore, it has also been shown in [80], that when the bound (5.15) guarantees sufficient conditional min-entropy, a standard extraction method can be applied, e.g. the Leftover Hash Lemma, where Shannon entropy determines how many bits can be extracted, as the extractor's output length is proportional to $m = kH(X|Y) - 6\sqrt{k \log_2 \frac{1}{\epsilon} \log_2 |X|}$ and thus to the value of Shannon entropy. Similar analysis has also been presented in [165], where the upper bound on bits extractable from Shannon sources has been obtained:

$$N = Hk - \Theta\left(\sqrt{\log_2(1/\epsilon)hk}\right), \quad (5.16)$$

The constant under $\Theta(\cdot)$ depends on the source, similarly to $\log_2 |X|$ in [80]. The key assumption, however, is that the source is memoryless, an assumption that also applies to our setting.

5.2 Certification for existing Bell inequalities

In this section, we address the issue of randomness certification for existing Bell inequalities. Using the protocol introduced in Section 5.1, we classified four Bell expressions for Shannon entropy-based QRNG certification, presented in Sections 5.2.1, 5.2.2, 5.2.3, and 5.2.4, according to the amount of randomness they certify as a function of the Werner white noise level p . Furthermore, both the maximal amount of certifiable randomness and the behavior of the entropy function relative to the noise level p were evaluated, with a comprehensive comparison provided in Section 5.2.5.

Additionally, the observations of the results above lead to some conclusions about the properties of the Shannon entropy in randomness certification. In Section 5.2.6, we derived and analyzed the general form of Shannon entropy constrained by NPA optimization results, computed using the ncpol2sdpa [192] framework with the MOSEK [10] solver. We were also able to achieve certain gains after applying all possible combinations of the probabilities of results in entropy calculations, which we evaluated in Section 5.2.8. Finally, the certification of randomness for a three-outcome quantum state is demonstrated in Section 5.2.9.

The values of Shannon entropy were obtained via non-linear optimization based on the scheme detailed in Section 5.1 and on Figure 5.1. Optimization was performed over three variable probabilities, denoted as $P_{a,b} = P(a, b|x_0, y_0)$ for simplicity: $P_{-1,-1}$, $P_{-1,1}$, and $P_{1,-1}$. The fourth probability, $P_{1,1}$, was defined as $1 - P_{-1,-1} - P_{-1,1} - P_{1,-1}$, with each variable corresponding to the probability of obtaining one of the allowed outcomes. In cases where measurement results are not binary, the number of variables is determined by $n^2 - 1$, where n represents the number of outcomes permitted by a local measurement. Bounds for each of these variables were calculated by solving the optimization problem (5.11) for the set of linear expressions derived from these individual probabilities.

5.2.1 Clauser-Horne-Shimony-Holt inequality

Introduced in [36], this is the first and therefore the most widely used example of the Bell inequality. The regular CHSH, however, does not certify two bits of randomness, even for the lack of noise ($p = 0$). However, the entropy function shows only a gradual decrease for $p \geq 0.1$.

By adding one correlation function $C(2, 3)$, we can obtain a different operator, which we denote as modified CHSH, or ModCHSH, introduced in [116]:

$$G_{ModCHSH} = C(1, 2) + C(1, 3) + C(2, 1) + C(2, 2) - C(2, 3). \quad (5.17)$$

The Tsirelson's bound for this Bell expression is $|\mathfrak{B}_{ModCHSH}|_{\mathcal{Q}} = 1 + 2\sqrt{2}$. We use this protocol for the pair of settings ($x = 1, y = 1$).

As shown in Figure 5.3, modified CHSH in the form of (5.17) indeed leads to the certification of two bits of randomness. However, it does not provide higher entropy over classical CHSH for the noise $p \geq 0.1325$. Above this level, the standard CHSH provides higher entropy. In other words, for higher noise, CHSH can certify a higher level of randomness, compared to (5.17).

5.2.2 Braunstein-Caves inequalities

This type of Bell inequality was introduced in [24]. It is a family of expressions, parametrized by several binary measurement settings for two parties $n \geq 2$:

$$G_{BC_n} = C(1, 1) + C(1, 2) + C(2, 2) + \dots + C(n-1, n-1) + C(n-1, n) + C(n, n) - C(n, 1). \quad (5.18)$$

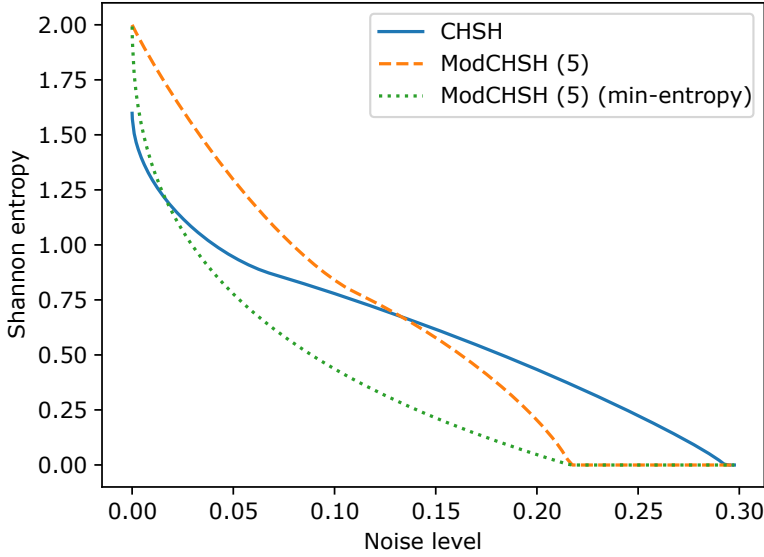


Figure 5.3: Lower bounds on Shannon entropy for randomness certification provided by CHSH inequality, as well as (5.17), as a function of the level of noise.

The Tsirelson's bound equals $|\mathfrak{B}_{BC_n}|_{\mathcal{Q}} = 2n \cos(\frac{\pi}{2n})$. We have run the optimization for three expressions that are a part of this family: BC_3 , BC_5 , and BC_7 . We have tried all twelve settings for each expression, and we have listed those for which two bits of randomness can be certified. For BC_3 these are $(x = 1, y = 3)$, for BC_5 these are $(x = 4, y = 2)$ or $(x = 1, y = 4)$ and for BC_7 these are $(x = 4, y = 1)$ or $(x = 1, y = 5)$.

The results for this family of protocols are presented in Figure 5.4. They show that the shortest Bell expression, BC_3 , provides the highest Shannon entropy, followed by BC_5 and BC_7 . However, due to the unusual change of the course of the function, for some noise levels ($p \approx 0.04$), the difference between the BC_5 and BC_7 is relatively small.

5.2.3 I_1 and I_2

In [116], two Bell expressions have been proposed:

$$\begin{aligned}
 G_{I_1} = & C(1, 2) - C(1, 3) - C(2, 1) - C(2, 2) \\
 & + C(3, 1) + C(3, 3) + C(4, 1),
 \end{aligned} \tag{5.19}$$

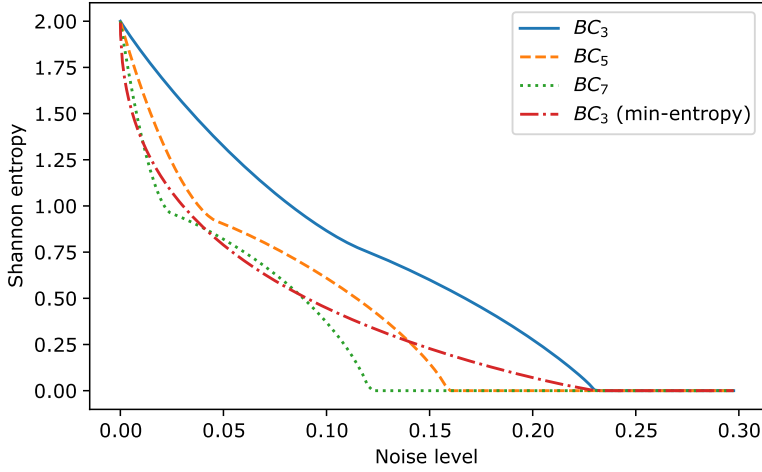


Figure 5.4: Lower bounds on Shannon entropy for randomness certification provided by the family of Braunstein-Caves inequalities, as a function of the level of noise.

and

$$\begin{aligned}
 G_{I_2} = & -C(1, 2) + C(1, 3) + C(2, 1) + C(2, 2) + C(2, 3) \\
 & + C(3, 2) - C(3, 3) + C(4, 1) + C(4, 2) + C(4, 3).
 \end{aligned} \tag{5.20}$$

The Tsirelson's bound for these are $|\mathfrak{B}_{I_1}|_{\mathcal{Q}} = 1 + 6 \cos(\pi/6)$ and $|\mathfrak{B}_{I_2}|_{\mathcal{Q}} = 2 + 4\sqrt{2}$ respectively. They represent a wider group of inequalities with 4 possible measurement settings for Alice and 3 for Bob. Their min-entropy certification has been thoroughly described in [116], but for the certification of the Shannon entropy, their usefulness has not yet been shown. We evaluate these inequalities for $(x = 1, y = 1)$ measurement settings, as these lead to the situation where two bits of randomness can be obtained.

Both plots presented in Figure 5.5 show that I_1 has a small, yet noticeable, advantage over I_2 for a smaller amount of noise, whereas this changes at the point where the convexity of the entropy as a function of noise parameter changes. Thus, for larger noise, I_2 has a visible (and more influential) advantage; it certifies more randomness.

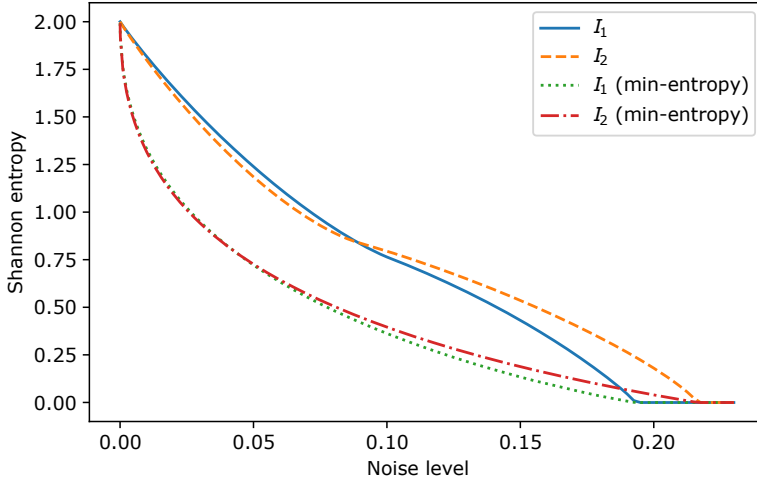


Figure 5.5: Lower bounds of Shannon entropy for randomness certification provided by the I_1 and I_2 inequalities, as a function of the level of noise.

5.2.4 Woollorton-Brown-Colbeck inequalities

The last two families of inequalities investigated in this paper were introduced in [194]. The first family, I_δ , is defined as:

$$G_{I_\delta} = C(0,0) + \frac{C(0,1) + C(1,0)}{\sin \delta} - \frac{C(1,1)}{\cos 2\delta}, \quad (5.21)$$

where $0 \leq \delta \leq \pi/6$ and Tsirelson's bound equals $|\mathfrak{B}_{I_\delta}|_Q = \frac{2\cos^3\delta}{\cos 2\delta \frac{1}{\sin \delta}}$. The second one, J_γ , is defined as:

$$G_{J_\gamma} = C(0,0) - C(1,1) + (4\cos^2 \frac{\gamma + \pi}{6} - 1)(C(0,1) + C(1,0)), \quad (5.22)$$

where $0 \leq \gamma \leq \pi/12$ and the quantum bound equals $|\mathfrak{B}_{J_\gamma}|_Q = 8\cos^3 \frac{\gamma + \pi}{6}$.

For these families of Bell inequalities, we observe that both I_δ and J_γ certify two bits of randomness for Shannon entropy. Additionally, the robustness of the certification for I_δ increases when the value of δ approaches $\delta = \pi/6$, but the decrease of the value of δ does not change the maximal certification for that protocol. This behavior has been visualized in Figure 5.6. However, in both I_δ and J_γ families, we were not able to observe a change in the convexity, which was visible in all the previous ones.

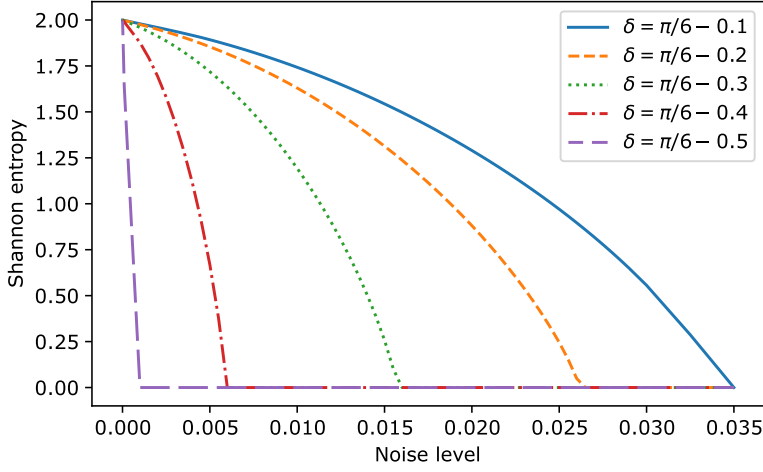


Figure 5.6: Lower bounds of Shannon entropy for randomness certification provided by the I_δ (with decreasing values of δ) inequalities, as a function of the level of noise.

noise level p	I_{δ_0}		J_{γ_0}	
	Shan.	min-ent.	Shan.	min-ent.
0.000001	1.9999784	1.9912406	1.9999784	1.9912408
0.0001	1.9978744	1.9131034	1.9978744	1.9131034
0.01	1.7656553	1.0459131	1.7656553	1.0459131
0.02	1.3794377	0.5697659	1.3794376	0.5697659
0.0275	0.9593294	0.2994331	0.9593294	0.2994330

Table 5.1: Comparison between the Shannon entropy and min-entropy lower bounds for certain values of noise, for I_δ and J_γ protocols. The parameters are chosen to maximize the amount of key certified by these protocols ($\delta = \frac{\pi}{6}$ and $\gamma = 0.0$).

5.2.5 Comparison

As noted in the preceding remarks, the amount of entropy certified varies depending on the noise levels to which the certificates are applied. As illustrated in Figure 5.7, no single certificate is identified as superior across the entire noise range. Specifically, the robustness of BC_3 is found to dominate up to a noise level of $p = 0.14$, at which point it is surpassed by the amount of randomness certified by the CHSH inequality.

In the absence of BC_3 as a candidate, the highest levels of randomness are provided by I_1 up to $p = 0.08$, where a slight advantage is then gained by I_2 . Furthermore, the CHSH inequality is observed to outperform I_1 for $p < 0.095$ and I_2 for $p < 0.11$.

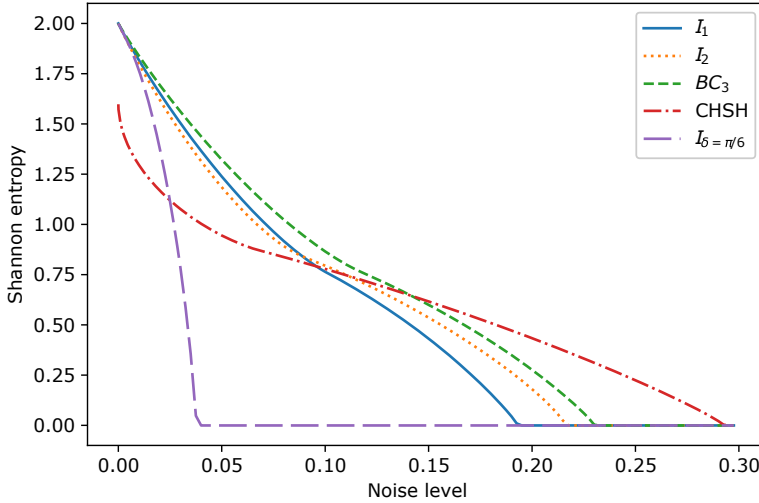


Figure 5.7: Lower bounds on Shannon entropy for different Bell inequalities used for randomness certification, as a function of noise.

5.2.6 General form for Shannon entropy

The non-linear optimization based on (5.13) yields the value of the Shannon entropy for the provided lower and upper bounds. However, it is also very time-consuming and does not allow for quick certification of Shannon entropy without the need to perform lengthy numerical calculations. Nevertheless, an analytical lower bound for this value can be established.

For $a, b \in \{-1, 1\}$ and spot-settings x_0, y_0 , the probability $P(a, b|x, y) \leq$

u_P , where as u_P we denote an upper bound for the probabilities. As

$$\sum_{a,b \in \{-1,1\}} P(a,b|x,y) = 1, \quad (5.23)$$

we can also point out that $u_P \geq \frac{1}{n}$, where n is the number of measurement results pairs (a,b) , that equals $n = 4$ in our analysis (for measurements that allow for more than two possible outcomes, this value can be higher). This follows from the normalization of quantum probabilities, which sum to unity. If the upper bound satisfies $u_P = \frac{1}{n}$, the distribution is uniform. Conversely, if the expected upper bound is smaller, $u_P < \frac{1}{n}$, at least one probability must be larger, since even if the remaining probabilities are uniformly distributed, each of them would exceed u_P .

One of the features of the Shannon entropy function (1.11) is that it is Schur-concave¹, which implies that it reaches its minimum value for the probability distribution that is the most uneven that the conditions allow. In other words, as few results as possible should appear with the likelihood related to the global probability upper bound. The lowest upper bound in this case will be $u_P = \frac{1}{n}$, where n is the number of different measurement outcomes, but the more biased the results are, the higher u_P will be, and thus entropy will be lower. The distribution that adheres to that allows us to obtain the lower bound for the value of Shannon entropy. Thus, there are going to be exactly $\lfloor 1/u_P \rfloor$ measurement results that will occur with the probability u_P , $n - \lfloor 1/u_P \rfloor - 1$ results that will not occur ($P(a,b|x,y) = 0$), and one result that will occur with the probability $1 - \lfloor 1/u_P \rfloor u_P$. This way, we can obtain a general form for the lower bound of the Shannon entropy function.

Proposition 5.2.1. *The lower bound for the value of the Shannon entropy function is*

$$H(P) \geq - \left\lfloor \frac{1}{u_P} \right\rfloor u_P \log_2(u_P) - \left(1 - \left\lfloor \frac{1}{u_P} \right\rfloor u_P\right) \log_2 \left(1 - \left\lfloor \frac{1}{u_P} \right\rfloor u_P\right), \quad (5.24)$$

¹A function $f : \mathbb{R}^n \rightarrow \mathbb{R}$ is *Schur-concave* if for all $x, y \in \mathbb{R}^n$ such that x is majorized by y (the components of both vectors are sorted in non-increasing order), it holds that $f(x) \geq f(y)$. Equivalently, f is symmetric and satisfies

$$(x_i - x_j) \left(\frac{\partial f}{\partial x_i} - \frac{\partial f}{\partial x_j} \right) \leq 0 \quad \text{for all } i, j.$$

Intuitively, a Schur-concave function decreases as its arguments become more unequal, meaning it prefers more balanced distributions of components.

where u_P is the upper bound for a single probability in the probability distribution P .

Following [142], we employ the relation between the observed CHSH violation value $|\mathfrak{B}_{CHSH}|$ and the adversary's optimal guessing probability:

$$P_{\text{guess}}(a|x) \leq \frac{1 + \sqrt{2 - |\mathfrak{B}_{CHSH}|^2/4}}{2}. \quad (5.25)$$

It has been also shown, that there exists a tight min-entropy bound for local min-entropy $H_\infty(A|X)$, which also constitutes the lower bound for global min-entropy, since $H_\infty(AB|XY) \geq H_\infty(A|X)$ and match: $H_\infty(A|X) \geq 1 - \log_2 \left(1 + \sqrt{2 - |\mathfrak{B}_{CHSH}|^2/4} \right)$.

Any observed violation above the classical limit guarantees randomness and thus DI security. Based on that, we can establish the lower bound for the value of Shannon entropy of a local measurement for CHSH as:

$$\begin{aligned} H(A|X)_{CHSH} \geq & -\frac{1 + \sqrt{2 - |\mathfrak{B}_{CHSH}|^2/4}}{2} \log_2 \left(\frac{1 + \sqrt{2 - |\mathfrak{B}_{CHSH}|^2/4}}{2} \right) \\ & - \left(\frac{1 - \sqrt{2 - |\mathfrak{B}_{CHSH}|^2/4}}{2} \right) \log_2 \left(\frac{1 - \sqrt{2 - |\mathfrak{B}_{CHSH}|^2/4}}{2} \right), \end{aligned} \quad (5.26)$$

In Figure 5.8, we present how the bounds (5.26) and (5.24) for comparison change depending on the noise level.

However, as mentioned, the bound based on (5.25) only describes local measurements of the global state. In [193], a tight, analytical guessing probability upper bound for a scenario for three-partite (two honest communication parties and an eavesdropper) Mermin-Bell inequality is presented:

$$P_{\text{guess}}(ab|xy) \leq \begin{cases} \frac{3}{4} - \frac{|\mathfrak{B}_M|}{8} + \sqrt{3} \sqrt{\frac{|\mathfrak{B}_M|}{8} \left(\frac{1}{2} - \frac{|\mathfrak{B}_M|}{8} \right)} & \text{if } |\mathfrak{B}_M| \geq 3 \\ \frac{3}{2} - \frac{|\mathfrak{B}_M|}{4} & \text{if } |\mathfrak{B}_M| \leq 3, \end{cases}$$

where $2 \leq |\mathfrak{B}_M| \leq 4$ is the value of the Mermin-Bell inequality achieved in the measurement process. The lower bound applies to every pair of measurement settings (x, y) . We plot the Shannon entropy lower bound based on (5.27) and Proposition 5.2.1, as well as the min-entropy lower bound based on the same guessing probability upper bound on Figure 5.9.

Notably, Shannon entropy and min-entropy converge to the same value at two distinct points, specifically where $|\mathfrak{B}_M| \approx 3.75$ and $|\mathfrak{B}_M| \approx 3.96$.

In the interval between $|\mathfrak{B}_M| = 2$ and $|\mathfrak{B}_M| = 3.75$, the upper bound $u_P > 1/2$. This implies a probability distribution of $P = [u_P, 1 - u_P, 0, 0]$ consisting of only two possible outcomes until $|\mathfrak{B}_M| = 3.75$, at which point $u_P = 1/2$ and the Shannon and min-entropy measures coincide.

Between $|\mathfrak{B}_M| = 3.75$ and $|\mathfrak{B}_M| = 3.94$, the distribution expands to three possible outcomes; at $|\mathfrak{B}_M| = 3.94$, a uniform probability distribution of $1/3$ is reached, again resulting in equal entropy values. For $|\mathfrak{B}_M| > 3.94$, the number of possible outcomes must increase to four. In contrast, for the Shannon entropy values obtained via the numerical method in Section 5.1, no such common points with min-entropy are observed. This discrepancy is attributed to the fact that we use not just upper, but also lower bounds.

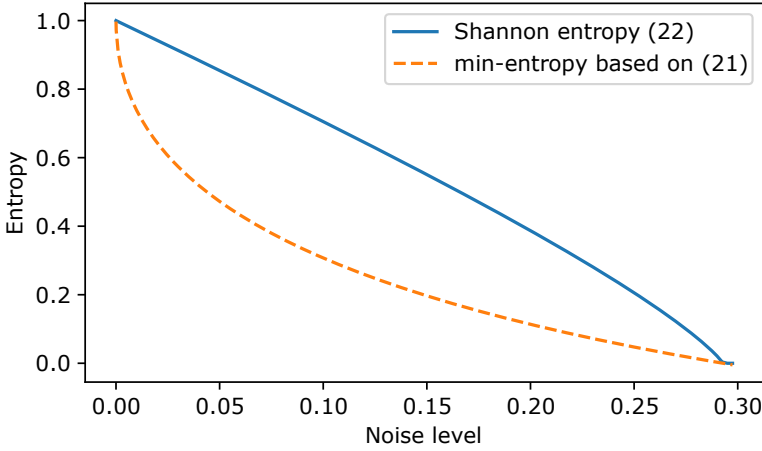


Figure 5.8: Shannon and min-entropy lower bounds for CHSH for different levels of noise, based on (5.25) and (5.26).

Additionally, we can also make a direct observation considering the probability distributions obtained in the optimization process. We have observed for every analyzed case that a particular probability distribution maximizes the value of Shannon entropy:

Observation 5.2.1. *The probability distribution that maximizes the value of Shannon entropy and therefore maximizes the randomness for a given certificate is (up to a permutation)*

$$P_H = [l_{-1,-1}, l_{-1,1}, u_{1,-1}, 1 - l_{-1,-1} - l_{-1,1} - u_{1,-1}], \quad (5.27)$$

where $l_{-1,-1}$ is the lower bound for result $a = -1, b = -1$, $l_{-1,1}$ is the lower bound for result $a = -1, b = 1$ and $u_{1,-1}$ is the upper bound for result $a = 1, b = -1$.

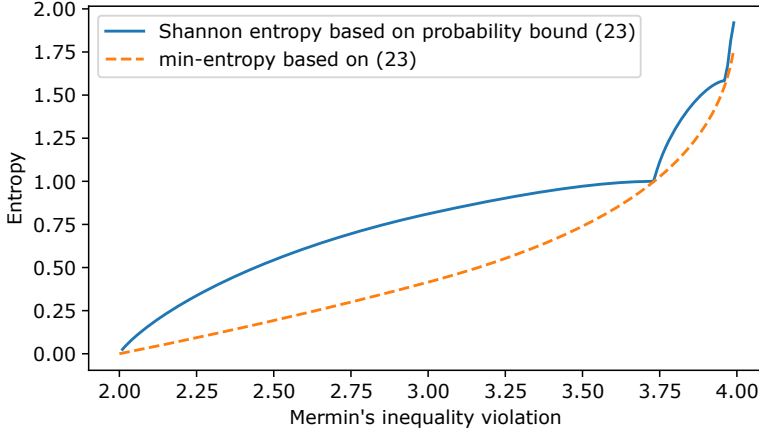


Figure 5.9: Shannon and min-entropy lower bounds for CHSH for different Mermin values $2 \leq |\mathfrak{B}_M| \leq 4$, based on (5.27).

This observation has not been proven for every family of Bell inequalities; however, for the analyzed examples in Sections 5.2.1, 5.2.2, 5.2.3, and 5.2.4, the observation-based entropy value agrees with the value obtained using nonlinear optimization to 6th digit.

5.2.7 Entropy as a composite function

In Sections 5.2.1, 5.2.2, and 5.2.3, a change in the convexity of the function is noticeable. Shannon entropy is not a function defined on a sequence of intervals; therefore, this behavior may be caused by a different course of the functions that make up the Shannon entropy, especially the course of the NPA-calculated lower and upper probability bounds. To investigate this issue, we have calculated the second derivative of the Shannon entropy (the process is shown in Appendix B):

$$\begin{aligned} \frac{\partial^2 H}{\partial p^2} = & \frac{\partial H}{\partial l_{-1,-1}} \frac{d^2 l_{-1,-1}}{dp^2} - \frac{1}{\ln 2} \left(\beta_1 \left(\frac{dl_{-1,-1}}{dp} \right)^2 \right. \\ & \left. + \alpha \frac{dl_{-1,-1}}{dp} \left(\frac{dl_{-1,1}}{dp} + \frac{du_{1,-1}}{dp} \right) \right) + \dots \end{aligned} \quad (5.28)$$

For these calculations, we were allowed to use the probability distribution from the Observation 5.2.1, as it is valid for the inequalities described in previous subsections, which include BC_n .

The other coefficients are composed likewise, but with different lower or upper bounds used for derivation. It can be noticed that this derivation is essentially constructed with two addition terms – one positive and one negative. As shown in Figure 5.10, on the range of values corresponding to the part with a lower entropy level, the value of the second derivation is lower than 0 (this part of the function is concave), whereas, on the range of values corresponding to the part with higher entropy level, the value of the second derivation is higher than 0 (this part of the function is convex).

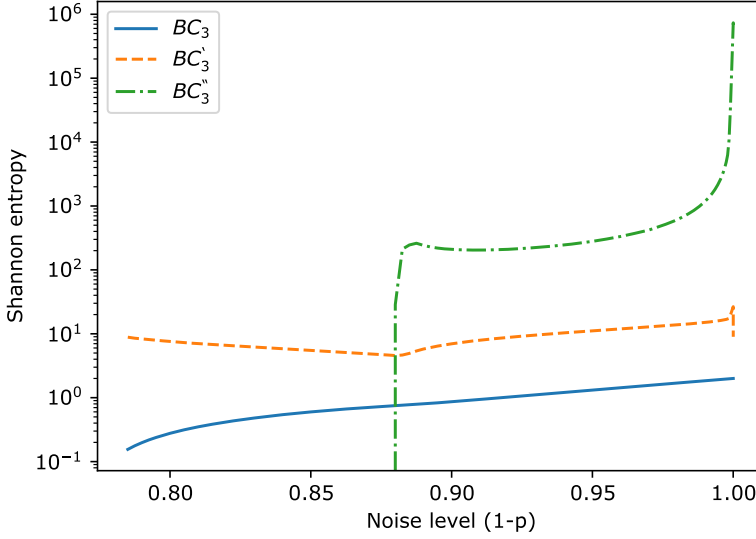


Figure 5.10: BC_3 function calculated based on Observation 5.2.1 compared with its first and second derivative (as described in Appendix B).

This change in convexity can be essentially explained by the fact that different quantum strategies (in this case, as the measurement settings are fixed – different measured quantum states) are optimal for different quantum bounds and different noise levels $((1-p)|\mathfrak{B}|_{\mathcal{Q}})$. A similar issue has been presented in [13] for optimized guessing probability, where the authors pointed out that mixtures of strategies can achieve higher average guessing probability than any single-strategy curve between those points.

However, this also means that the adversary that is aware of the course of the certified randomness can mix their strategies to exploit the non-convexity to devise a more effective attack. It has also been shown in [13] that if the function of entropy over the Bell inequality violation is not necessarily concave, then for the case with different quantum strategies, the

entropy could actually be lower. To ensure that the bound is valid for any mixture of quantum behaviors, a convex hull of the entropy function should be used as the final bound.

Additionally, it is noted that in (5.13), each value of l_i and u_i is obtained from a separate NPA optimization for a fixed noise level and Bell inequality, and thus corresponds to different quantum behavior. While the consideration of a single, fixed quantum behavior would be more convenient for computing Shannon entropy, to the best of our knowledge, a method for minimizing Shannon entropy over the entire set of such behaviors currently does not exist.

Let us also note that by considering l_i and u_i from separate optimizations, the resulting constraints are necessarily relaxed and, consequently, more pessimistic. Furthermore, the use of the NPA method itself introduces an additional relaxation, as it accounts not only for all quantum-mechanically possible attacks but also for certain super-quantum behaviors. Consequently, the proposed method determines a conservative estimate of the Shannon entropy. Because (5.11) represents a relaxation, the entire framework is likewise characterized as a relaxation in which optimization is limited to the imposition of upper and lower bound constraints without further restrictions on the probability distribution $\{P_i\}$. Under the restriction to strictly allowed quantum behaviors, the entropy would only increase.

5.2.8 Additional constraints

Overall, the NPA calculations were focused on determining the direct lower and upper bounds on the individual measurement result probabilities, as defined for each Bell inequality. However, this does not exhaust the scope of linear combinations that can be bounded via (5.11) to further constrain the non-linear optimization in (5.13).

The bounded probabilities can thus be combined into 12 other additive linear combinations (as for four different pairs of measurement outcomes, there are exactly $2^4 = 16$ additive linear combinations, and we already used four of them). Two of these, the null combination and the sum of all components, provide no additional information as their values are known a priori. Consequently, ten linear combinations remain that may yield tighter bounds on the probability sums:

$$\left\{ \sum_{(i,j) \in A} P_{i,j} \mid A \subseteq \{-1, 1\}^2, |A| \in \{2, 3\} \right\}. \quad (5.29)$$

Additional constraints for the modified CHSH expression (5.17) were calculated and subsequently integrated into the non-linear optimization for Shannon entropy. For the resulting linear expressions, both lower and upper bounds were established. Regarding the computational performance, it was found that only 100 iterations of the basin-hopping technique were required to reliably avoid local minima, a significant reduction compared to the 1500 repetitions necessitated by previous calculations.

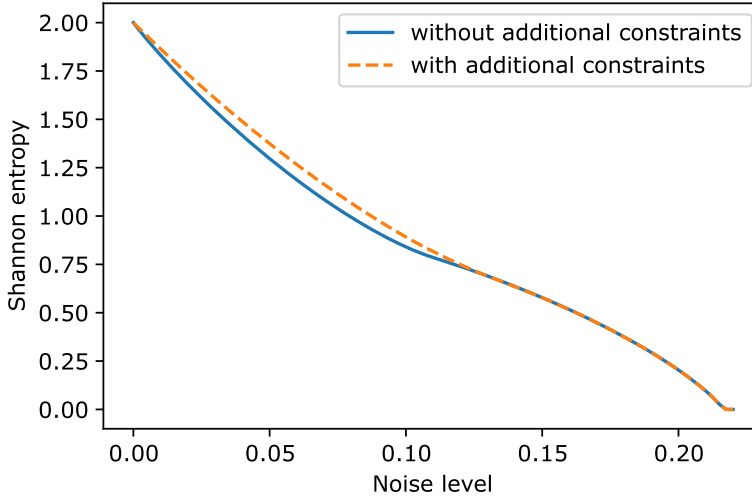


Figure 5.11: Lower bounds on Shannon entropy for modified CHSH Bell inequality with and without additional constraints.

The results show that with additional constraints, we were able to obtain a moderate improvement. However, the advantage ends for the same noise level, where CHSH starts to have an advantage over the modified CHSH, which is also the moment when the function changes its convexity, as described in Section 5.2.7.

5.2.9 Three-outcome scenario

To further investigate the topic of DI randomness certification, we have also pursued a three-outcome protocol based on the d -outcome Bell expressions family proposed in [88]. This family constitutes a generalisation of the CHSH for d -outcome measurements. It also has an interesting property, that the maximal quantum violation is achieved by the maximally entangled states, measured using the projectors that correspond to mutually unbiased bases. Their results are based on the functional due to Buhrman and Massar

(BM functional) [27]. The available number of outcomes d and the number of settings are constrained to odd primes, and the quantum bound can be algebraically calculated using a sum-of-squares decomposition of the Bell expression. More specifically, we use a Bell operator in the form of [88]:

$$G_d = \frac{1}{d^3} \sum_{n=1}^d \lambda_n \sum_{jk} \omega^{njk} \Pi_n^{0,j} \otimes \Pi_n^{1,k}, \quad (5.30)$$

where λ_n are complex numbers of unit modulus, ω are the d -th root of unity and $M^{0,j}$ and $M^{1,k}$ are the observables. The quantum bound we used for the optimization of this inequality is $|\mathfrak{B}|_{\mathcal{Q}} = 1.718233$, and the settings are $x = d + 1 = 4$ and $y = 2$.

The certification method described in Sections 5.1.2 and 5.1.3 was utilized for this analysis. However, given that nine possible pairs of outcomes exist for the three-outcome quantum state, additional linear-expression constraints were incorporated to account for all available outcomes. Optimization was performed over eight independent variables, each representing the probability of a specific outcome pair, while the ninth probability was defined as the difference between one and the sum of the other variables. The results of this numerical optimization are presented in Figure 5.12.

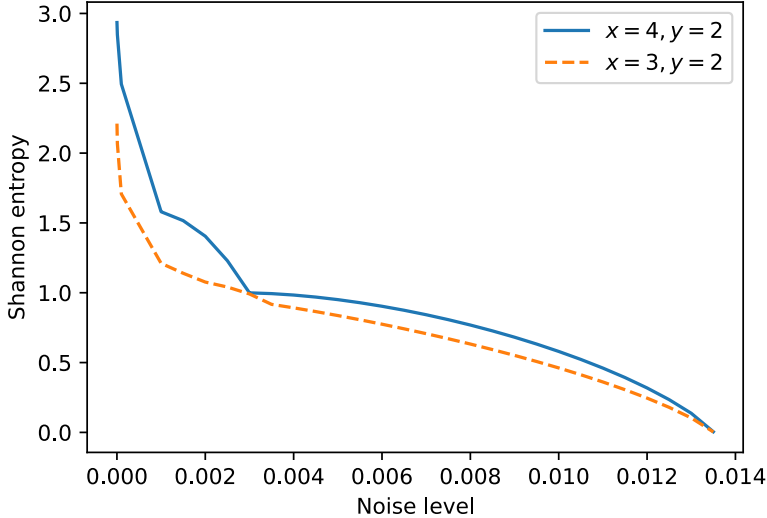


Figure 5.12: Shannon certification of randomness using the Bell inequality proposed in [88], for $d = 3$ Werner state, quantum bound $|\mathfrak{B}|_{\mathcal{Q}} = 1.718233$, settings $(x = 4, y = 2)$ and $(x = 3, y = 2)$ for comparison.

Characteristics similar to the previously investigated two-dimensional Bell certificates were observed in the results, particularly regarding a change in the concavity of the entropy function. This transition is identified at approximately $p = 0.0055$, where an entropy value of $H^{p=0.0055} = 1$ is achieved. At the minimum noise level of $p = 1\text{e-}6$, corresponding to a Bell value of $|\mathfrak{B}|_{p=1\text{e-}6} = 1.718231$, nearly three bits of randomness are attainable ($H^{p=1\text{e-}6} = 2.93$).

However, a significant caveat is noted regarding noise tolerance, which is found to be substantially lower than that of two-dimensional quantum systems. Entropy is observed to converge to zero at a noise level of approximately $p = 0.014$ (Bell violation value $|\mathfrak{B}|_{p=0.014} = 1.694178$), which is a markedly worse robustness in comparison to two-dimensional counterparts.

5.3 Extensive search for certification protocols

In this section, we present an extensive numerical investigation and comparative analysis of Bell certificates for configurations with four measurement settings on one side and three on the other, conducted using the proposed quantitative procedure. Section 5.3.1 shows the global results and the distribution of the Bell certificates, based on the certifiable Shannon entropy. In Section 5.3.2, we focus on identifying Bell certificates with particularly favorable properties for DI randomness certification by examining representative protocols, comparing their entropy behavior under varying noise levels, and assessing the accuracy of entropy estimates obtained from the analytical distribution (5.27) relative to nonlinear optimization results. Finally, Section 5.3.3 investigates the self-testing properties of the identified Bell certificates within the framework of self-testing for boxes introduced in [12].

5.3.1 General analysis

Building on the definition of the coefficient matrix in (5.3) and the general form of the Bell operator in (5.2), we first quantify the size of the search space considered in our analysis, corresponding to all possible Bell expressions constructed from discrete unit coefficients. In other words, for this analysis, the coefficient matrix elements are constrained to these values: $\alpha_{i,j} \in \{-1, 0, 1\}$. Otherwise, the number of possible Bell expressions would be infinite.

For $N = 4$ measurement settings on Alice's side and $M = 3$ on Bob's,

the total number of distinct expressions with coefficients $\alpha_{ij} \in \{-1, 0, 1\}$ is $3^{NM} - 1 = 531,440$, excluding the trivial zero matrix. With $N \cdot M = 12$ measurement spot-setting combinations (x_0, y_0) , this yields $12 \times (3^{NM} - 1) = 6,377,280$ distinct certification protocols R^2 . For each protocol, (5.9) was used to compute Tsirelson's bound and, using the optimization problem defined in (5.11), performed the probability bounding. These bounds were then used to estimate the corresponding measure of randomness, quantified using Shannon entropy.

The noise levels p must be carefully selected, since each requires an independent SDP optimization. Selected noise levels should allow for a consistent comparison of the entropy function across protocols and reveal which protocol is most robust to noise. Following the findings in [116] and in Section 5.2, the noise rules out reliable entanglement-based randomness generation for $p > 0.2$ (because the lower bounds on Shannon and min-entropy drop sharply across all tested Bell inequalities, meaning the device's outputs can no longer be certified as reliably random). Therefore, for this analysis, we put forward three levels of noise: $p = 1\text{e-}6$, $p = 0.1$, and $p = 0.2$.

Typically, the estimation of entropy for the bounded quantum behaviors is based on the NPA optimization of guessing probability [116], but for Shannon entropy, the accurate estimation requires nonlinear optimization over the feasible set of probability distributions consistent with the observed statistics, as presented in Section 5.2. Furthermore, it demands a high number of iterations to avoid local entropy minima. This limitation motivates the search for analytic or semi-analytic methods that can provide accurate entropy bounds without resorting to full nonlinear optimization. In this thesis, two complementary approaches towards this goal are presented. First, in Section 5.2.6, a rigorous analytical lower bound on the Shannon entropy is provided, albeit only on the assumption that limited information about the distribution is available (5.24).

However, the empirical ansatz from Observation 5.2.1 in the form of a probability distribution (5.27) provides a semi-analytic formula that fully utilizes the lower and upper bounds established using the optimization prob-

²In principle, if a certificate used with the spot-setting pair (x_0, y_0) includes a non-zero correlator $\tilde{C}(x_0, y_0)$, this correlator should be omitted from the Bell expression. During the randomness certification, the goal is to maximize the uncertainty of the results and thus maximize randomness. However, a correlator that is measured using observables that correspond to its (x_0, y_0) settings will always maximize the correlation between two parties. Therefore, such a correlator should be removed from the Bell expression when deployed.

lem defined in (5.11), which makes it suitable for this analysis.

The distribution of Bell certificates, grouped by the value of their associated randomness measure (Shannon entropy), for low noise ($p = 1e-6$), is shown in Figure 5.13. Approximately 1.4 million certificates exhibit zero entropy, indicating that they cannot certify any randomness and therefore correspond to Bell values that do not exceed the local bound. Hence, they do not exhibit the Bell's violation. Among the remaining certificates, none certifies less than one bit of randomness. Additionally, at $p = 0.2$, the maximum observed entropy is $H_{\max}^{p=0.2}(P_H) = 1.0724$, while for $p = 0.1$, it reaches $H_{\max}^{p=0.1}(P_H) = 1.4773$. We have also compared these results with the distribution for min-entropy of the Bell certificates. In this case, more than 2 million certificates exhibit zero entropy.

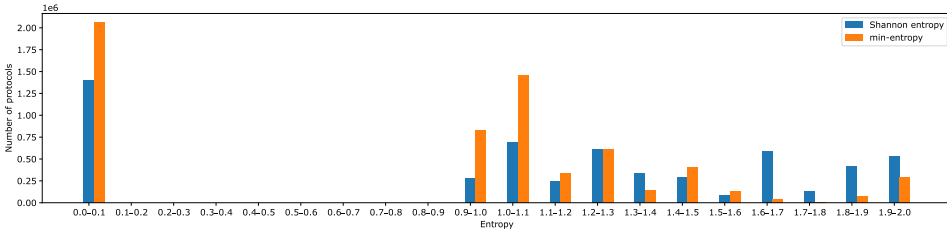


Figure 5.13: A distribution of the Bell certificates, as defined by (5.8). The certificates are classified based on the value of the measure of randomness (Shannon entropy) that the certificate yields. The histograms are presented for the white noise value $p = 1e-6$, for both Shannon and min-entropy.

5.3.2 Selected protocols

The primary objective of this investigation is to introduce new Bell certificates for use in quantum DI randomness certification. We explored several protocols exhibiting distinct characteristics in the computed data points. Specifically, we analyzed: protocols that maximize $H^{p=0.2}(P_H)$ among those satisfying $H^{p=1e-6}(P_H) \approx 2.0$ (5.1.2); protocols that maximize $H^{p=0.1}(P_H)$ under the same condition, $H^{p=1e-6}(P_H) \approx 2.0$ (5.1.5); protocols exhibiting the smoothest behavior – i.e., minimal variation in the entropy function across different noise levels – at various values of $H^{p=1e-6}(P_H)$ (5.1.3), (5.1.4); and finally the protocol in (5.1.1), where the constraint from (5.1.2) was relaxed to $H^{p=1e-6}(P_H) > 1.7$ instead of $H^{p=1e-6}(P_H) \approx 2.0$. All of the chosen protocols are presented in Table 5.2.

For the selected protocols, Shannon entropy was computed using the

$\mathbb{N}^\circ$	α	B
5.1.1	$(0, 1, 0; -1, -1, 0; -1, -1, 0; -1, 1, 0)$	5.472136
5.1.2	$(-1, -1, -1; 1, -1, 0; 0, 0, 0; -1, 1, 1)$	6.146067
5.1.3	$(-1, -1, 1; -1, -1, 0; 1, 0, 1; 1, 0, -1)$	6.569963
5.1.4	$(1, -1, 0; 1, 0, -1; 0, 0, 0; 0, -1, 1)$	5.196152
5.1.5	$(0, 1, -1; 1, 1, 1; -1, 0, -1; 1, 1, -1)$	7.534802

Table 5.2: Protocols chosen for the further analysis, in the form of (5.8). All spot-settings equal $(x_0, y_0) = (0, 0)$.

distribution defined in (5.27) over the range $p \in (1\text{e-}6, 0.3)$, with the results illustrated in Figure 5.15. To further investigate these characteristics, the Shannon entropy was also calculated (Figure 5.16) via the non-linear optimization protocol.

The analysis indicates that entropy values derived from the distribution in (5.27) are consistently higher than those obtained for optimized quantum behavior across all analyzed certificates. It is further demonstrated that (5.27) may lead to entropy estimations that paradoxically increase with higher levels of white noise, as observed for (5.1.4). These findings suggest that entropy calculated via the distribution in (5.27) should, at most, be considered an upper bound.

This interpretation is supported by the discrepancies between the two distinct methods of establishing quantum behavior, as illustrated in Figure 5.14. Notably, for a noise level of $p \approx 1\text{e-}6$, the quantum behavior defined in (5.27) yields the same value as for optimization-based Shannon entropy calculation. Furthermore, for every Bell expression, the difference is observed to peak within the range $p \in (0.05, 0.1)$ before decreasing and reaching a minimum only when the entropy is equal to zero.

These results corroborate the assumption that the Shannon entropy based on the probability distribution (5.27) can be considered an upper bound for the Shannon entropy obtained using nonlinear optimization.

An investigation was conducted to determine if any certificate from the full set that maximizes entropy at the highest noise levels could achieve two bits of randomness at $p = 1\text{e-}6$. We have observed that under this assumption, the optimal certificate does not exceed $H^{p=1\text{e-}6}(P_H) = 1.6$, a value equivalent to the standard CHSH inequality. A comparison between the CHSH inequality and the expressions defined in Table 5.2 is presented in Figure 5.16.

Additionally, we have computed the min-entropy using the method that

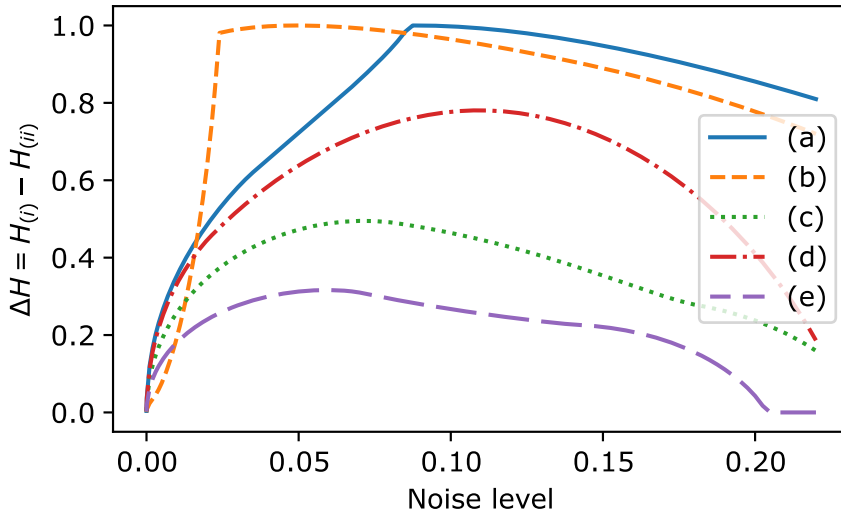


Figure 5.14: Difference between the Shannon entropy values obtained from (5.27) and those derived from nonlinear optimization, illustrating the over-estimation of entropy by (5.27) at higher noise levels.

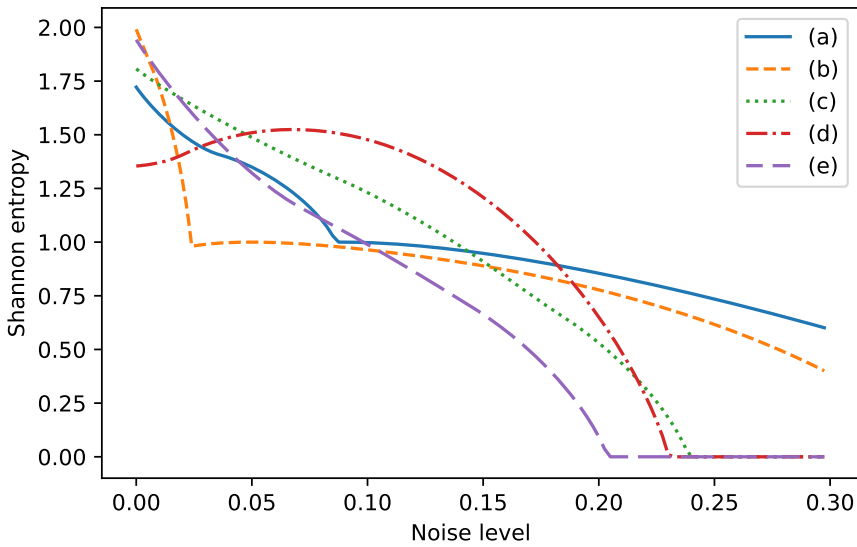


Figure 5.15: Certification of randomness using the Bell inequalities defined in Table 5.2, for two measures of randomness. The measure is Shannon entropy based on (5.27).

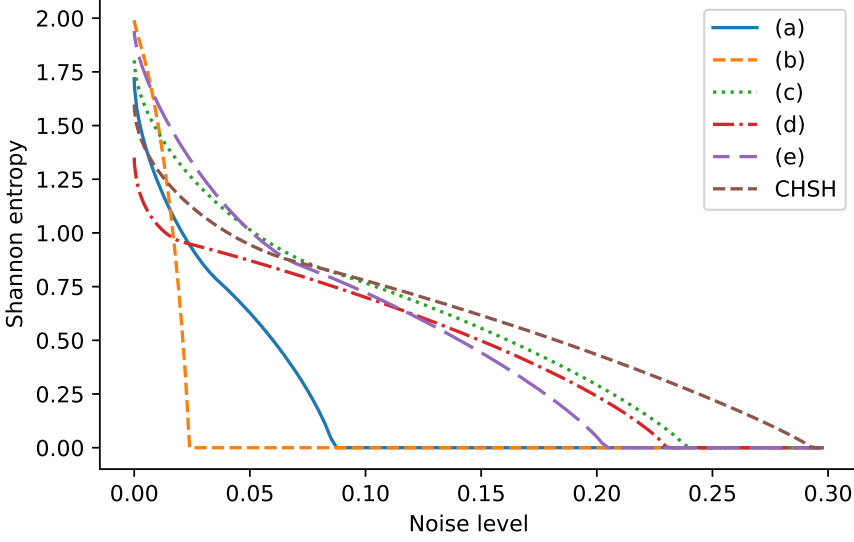


Figure 5.16: Certification of randomness using the Bell inequalities defined in Table 5.2, for two measures of randomness. The measure is Shannon entropy. The values are obtained using the standard certification approach, which relies on the nonlinear optimization, constrained by the NPA-obtained bounds, as opposed to (5.27).

utilizes non-linear optimization; it is visualized in Figure 5.17. The maximum amount of entropy certified by the protocols from Table 5.2 does not exceed $H_{max}^{p=1e-6}(P_{opt}) = 1.8396$, which is achieved for (5.1.2).

5.3.3 Boxes self-testing

In [12], an additional form of self-testing, named *self-testing for boxes*, has been introduced. For a given protocol $R = \{\alpha, |\mathfrak{B}|_{\mathcal{Q}}, x_0, y_0\}$ and Bell expression $\mathfrak{B}_{\alpha}(P)$, let $Boxes(\alpha, |\mathfrak{B}|_{\mathcal{Q}})$ denote the set of all boxes for the Bell inequality with expression $\mathfrak{B}_{\alpha}(P)$ and quantum bound $|\mathfrak{B}|_{\mathcal{Q}}$. In this context, *boxes* refer to sets of probability distributions $\{P(a, b|x, y) : a, b \in \{-1, 1\}, x \in \{1, 2, 3, 4\}, y \in \{1, 2, 3\}\}$, for which the value of the operator defined by the Bell expression, denoted by $\mathfrak{B}_{\alpha}(P)$, attains at least the Tsirelson bound $|\mathfrak{B}|_{\mathcal{Q}}$. For a given Bell expression $\mathfrak{B}_{\alpha}(P)$, a corresponding quantity $Flex(\alpha, |\mathfrak{B}|_{\mathcal{Q}})$ is introduced [12]:

$$Flex(\alpha, |\mathfrak{B}|_{\mathcal{Q}}) = \frac{1}{NM} \sum_{a,b,x,y} \max_{p \in Boxes(\alpha, |\mathfrak{B}|_{\mathcal{Q}})} p(a, b|x, y). \quad (5.31)$$

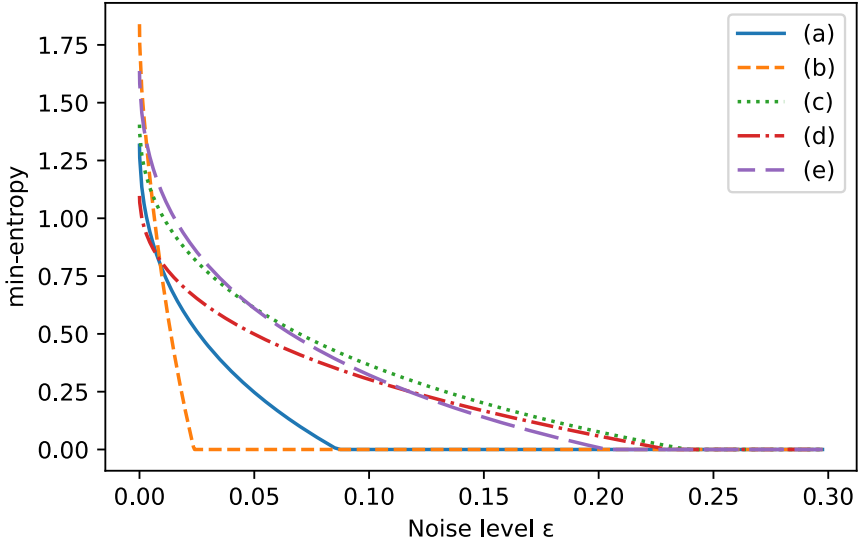


Figure 5.17: Certification of randomness using the Bell inequalities defined in Table 5.2, for two measures of randomness. The measure is min-entropy. The values are obtained using the standard certification approach, which relies on the nonlinear optimization, constrained by the NPA-obtained bounds, as opposed to (5.27).

Given that, the operator defined by Bell's expression $\mathfrak{B}_\alpha(P)$ is self-tested for boxes iff the set $\text{Boxes}(\alpha, |\mathfrak{B}|_{\mathcal{Q}})$ has $\text{Flex}(\alpha, |\mathfrak{B}|_{\mathcal{Q}}) = 1$, which means that the box attaining Tsirelson's bound $|\mathfrak{B}|_{\mathcal{Q}}$ is unique.

For every certificate, we have tested the flex value for the probability distribution based on the NPA obtained upper bounds for the outcomes. There are 12 probability distributions in this form, one for every pair of settings. We have verified if the certificates listed in Table 5.2 are self-tested for boxes. We have observed two protocols, (5.1.3) and (5.1.5), which presented (for $p = 1e-6$) the flex that equals 1.0, whereas for the other protocols from the list it falls within the vicinity of 1.3.

The minimum flex for $p = 0.1$ is 2.4, and for $p = 0.2$, it is 2.8. A normalized flex of at least 2.0 implies the existence of at least two distinct boxes for which the Bell expression yields the maximal value, $|\mathfrak{B}|_p$. This degeneracy, however, leads to the conclusion that infinitely many boxes can produce this specific Bell expression value. Because the set of valid boxes is convex, given any two optimal boxes, $\text{Box}(\alpha, |\mathfrak{B}|_p)_1$ and $\text{Box}(\alpha, |\mathfrak{B}|_p)_2$, we can mathematically construct a third box as their convex combination:

Bell expression	Flex for $p = 1\text{e-}6$	Flex for $p = 0.1$
(5.1.1)	1.338003	3.325855
(5.1.2)	1.255119	3.058927
(5.1.3)	1.003841	2.648911
(5.1.4)	1.253785	2.829320
(5.1.5)	1.003749	2.663294

Table 5.3: Comparison between different certificates presented in Table 5.2. Only two of the presented protocols show flex that equals exactly 1, i.e., when the box attaining Tsirelson’s bound is unique.

$\text{Box}(\alpha, |\mathfrak{B}|_p)_3 = \beta_1 \text{Box}(\alpha, |\mathfrak{B}|_p)_1 + \beta_2 \text{Box}(\alpha, |\mathfrak{B}|_p)_2$, where $0 < \beta_1, \beta_2 < 1$ and $\beta_1 + \beta_2 = 1$. Since this continuous mixture means the configuration lacks a unique extremal point, the statistics alone cannot isolate a single physical realization. Thus, there are no box-certifiable certificates for either $p = 0.1$ or $p = 0.2$.

Chapter 6

Dependence between quantum discord and non-locality

Quantum discord provides a rigorous information-theoretic measure of non-classical bipartite correlations beyond the entanglement paradigm. States with identically zero discord occupy a measure-zero subset with respect to the Hilbert–Schmidt measure, within the state space of finite-dimensional open systems, implying that almost all mixed quantum states natively possess non-zero discord [63]. Furthermore, these correlations typically exhibit asymptotic decay [172, 198] rather than sudden death under Markovian noise, avoiding the sudden death characteristic of entanglement. This widespread presence invites further investigation into its operational utility; since discord is nearly universal, its role as a specialized resource requires careful qualification to maintain its discriminatory power in mapping the specific boundaries of quantum advantage within distributed tasks.

Nevertheless, quantum discord possesses concrete operational interpretations within information-theoretic and thermodynamic protocols. Specifically, discord quantifies the exact markup in entanglement consumption required during quantum state merging when local operations and classical communication are restricted [31]. This identifies discord as a physical resource whose asymmetry directly dictates performance imbalances in dense coding scenarios. Furthermore, recent derivations of analytical lower bounds for geometric quantum discord and extended partial transpose criteria facilitate the practical detection of these correlations in higher-dimensional systems [197].

The meaning of quantum discord also extends to thermodynamics, where it determines the efficiency discrepancy between quantum and classical

Maxwell’s demons during work extraction [209], and to information theory, where it drives the non-classical locking of correlations, a phenomenon where minimal classical communication unlocks vast amounts of hidden information, even in the absence of entanglement [53]. These roles are linked by a single geometric measurement through comprehensive state-space boundary evaluations [120]. Physically, in solid-state architectures like coupled double quantum dots, geometric discord demonstrates superior robustness against thermal and Coulomb noise compared to standard entanglement [189].

The discovery of quantum discord revealed that non-locality and entanglement do not exhaust the diversity of quantum correlations [133]. Discord quantifies correlations that persist even in the absence of entanglement, arising from the discrepancy between two classically equivalent forms of mutual information [169]. Understanding the intricate dependence between different quantum characterizations is essential for mapping the boundaries of quantum advantage in distributed tasks.

This chapter addresses the aforementioned challenges by introducing a numerical framework for the certification and systematic analysis of the relationship between Bell nonlocality and quantum discord. Specifically, we investigate the lower bounds of discord by determining the minimum value required for a bipartite state to manifest a given Bell violation. Through this mechanism, we characterize six distinct Bell inequalities, comparing their performance through the minimal discord values observed under varying intensities of white noise. The results presented herein are previously unpublished and offer new insights into the interplay between different forms of quantum correlations.

The chapter is structured as follows: Section 6.1 details the numerical methodology, including the parametrization of bipartite states, the selection of Bell inequalities, and the computational protocol for discord calculation; Section 6.2 then presents the findings of our analysis, including the aforementioned certification of the minimal discord values, as well as the discussion on a potential method for classifying states based on their discord.

6.1 Characterization for entangled states

In this analysis, we again consider a bipartite quantum scenario in which two parties, Alice and Bob, share a general two-qubit mixed state. We employ a generic parametrization scheme that constructs the state through

a purification approach, treating the mixed state as the reduced density matrix of a pure state in a larger system. This formulation characterizes the full fifteen-dimensional $SU(4)$ space of two-qubit mixed states [93].

To establish the density matrix, first, the basis has to be set. We use a basis constructed from single-qubit unitary transformations, which are parameterized by local rotation angles, as follows:

$$\begin{aligned} |d_0\rangle &\equiv |\phi\phi'\rangle, & |d_1\rangle &\equiv |\phi_\perp\phi'_\perp\rangle, \\ |d_2\rangle &\equiv |\phi\phi'_\perp\rangle, & |d_3\rangle &\equiv |\phi_\perp\phi'\rangle; \end{aligned} \quad (6.1)$$

where

$$\begin{aligned} |\phi\rangle &= \cos\left(\frac{\theta}{2}\right) e^{-i\frac{\psi}{2}} |0\rangle + \sin\left(\frac{\theta}{2}\right) e^{i\frac{\psi}{2}} |1\rangle, \\ |\phi_\perp\rangle &= -\sin\left(\frac{\theta}{2}\right) e^{-i\frac{\psi}{2}} |0\rangle + \cos\left(\frac{\theta}{2}\right) e^{i\frac{\psi}{2}} |1\rangle, \\ |\phi'\rangle &= \cos\left(\frac{\theta'}{2}\right) e^{-i\frac{\psi'}{2}} |0\rangle + \sin\left(\frac{\theta'}{2}\right) e^{i\frac{\psi'}{2}} |1\rangle, \\ |\phi'_\perp\rangle &= -\sin\left(\frac{\theta'}{2}\right) e^{-i\frac{\psi'}{2}} |0\rangle + \cos\left(\frac{\theta'}{2}\right) e^{i\frac{\psi'}{2}} |1\rangle; \end{aligned} \quad (6.2)$$

which are parametrized by the angles $\theta, \psi, \theta', \psi'$.

The density matrix is formed by an orthonormal set of entangled basis vectors $\{|e_k\rangle\}$. The primary vector, $|e_0\rangle$, is parameterized by the entanglement angle χ and phase ζ ($\chi, \zeta \in [0, 2\pi)$). The remaining vectors $|e_k\rangle$ are explicitly derived by mixing the orthogonal complement $|\Psi_\perp\rangle = -e^{-i\zeta}q_-|d_0\rangle + q_+|d_1\rangle$ with the basis states (6.1):

$$|e_0\rangle = q_+|d_0\rangle + e^{i\zeta}q_-|d_1\rangle, \quad (6.3a)$$

$$|e_1\rangle = c_{21}|\Psi_\perp\rangle + s_{21}(c_{32}|d_2\rangle + s_{32}|d_3\rangle), \quad (6.3b)$$

$$\begin{aligned} |e_2\rangle &= -c_0\bar{s}_{21}|\Psi_\perp\rangle + (c_0\bar{c}_{21}c_{32} - s_0\bar{s}_{32})|d_2\rangle \\ &\quad + (c_0\bar{c}_{21}s_{32} + s_0\bar{c}_{32})|d_3\rangle, \end{aligned} \quad (6.3c)$$

$$\begin{aligned} |e_3\rangle &= \bar{s}_0\bar{s}_{21}|\Psi_\perp\rangle - (\bar{s}_0\bar{c}_{21}c_{32} + \bar{c}_0\bar{s}_{32})|d_2\rangle \\ &\quad - (\bar{s}_0\bar{c}_{21}s_{32} - \bar{c}_0\bar{c}_{32})|d_3\rangle. \end{aligned} \quad (6.3d)$$

The parameters c_{ij}, s_{ij} equal:

$$c_{ij} = \cos\left(\frac{\theta_{ij}}{2}\right) e^{-\frac{i\psi_{ij}}{2}}, \quad s_{ij} = \sin\left(\frac{\theta_{ij}}{2}\right) e^{\frac{i\psi_{ij}}{2}}, \quad (6.4)$$

where $\theta_{ij} \in [0, 2\pi)$ and $\psi_{ij} \in [0, 2\pi)$ are the rotation angles parameterizing the unitary transformations. The entanglement coefficients for the Schmidt decomposition are given by:

$$q_+ = \cos \chi, \quad q_- = \sin \chi, \quad (6.5)$$

with χ determining the initial entanglement of the pure state core $|e_0\rangle$.

Finally, the mixed state ρ is assembled as the weighted sum of the projectors of these entangled basis vectors:

$$\rho = \sum_{k=0}^3 \mu_k |e_k\rangle \langle e_k|, \quad (6.6)$$

where the coefficients μ_k correspond to the eigenvalues of the density matrix and satisfy the normalization condition $\sum \mu_k = 1$, which allows us to parametrize only 3 out of four μ_k values, while the fourth one is a value derived from (6.6). Consequently, $\mu_k \in [0, 1]$.

The full quantum state is therefore parametrized using 15 separate optimization variables: $\mu_0, \mu_1, \mu_2, \theta, \psi, \theta', \psi', \theta_0, \psi_0, \theta_{21}, \psi_{21}, \theta_{32}, \psi_{32}, \chi, \zeta$.

An input vector $x \in \mathbb{R}^{N_D}$, $\{x_i\}_{i=0}^{N_D-1}$ is defined such that the first fifteen components, $\{x_i\}_{i=0}^{14}$, uniquely determine the density matrix ρ according to the described purification scheme.

6.1.1 Parametrization of the measurement

To investigate the non-local properties of the generated states, we perform a non-linear optimization over the joint space of state configurations and local measurement settings, where the value of various Bell expressions is used as a constraint. We need, therefore, to parametrize not just the quantum state, but also the measurement settings. The remaining components of $\{x_i\}_{i=15}^{N_D-1}$ characterize the local measurement settings for Alice and Bob.

We consider generalized bipartite scenarios where Alice chooses from N_A settings $\{M^{0,k}\}_{k=0}^{N_A-1}$ and Bob from N_B settings $\{M^{1,l}\}_{l=0}^{N_B-1}$. To eliminate redundant degrees of freedom associated with rotational invariance, we fix Alice's first measurement setting to the Pauli operator $M^{0,0} \equiv \sigma_z$. The remaining observables are fully variational. Each setting $O \in \{M^{0,k>0}, M^{1,l}\}$ is an observable parameterized by polar and azimuthal angles (θ, ϕ) ; $\theta, \phi \in [0, 2\pi)$ on the Bloch sphere:

$$O(\theta, \phi) = \begin{pmatrix} \cos \theta & e^{-i\phi} \sin \theta \\ e^{i\phi} \sin \theta & -\cos \theta \end{pmatrix}. \quad (6.7)$$

6.1.2 Discord calculation

To evaluate (1.27), we must maximize the classical correlations over all possible local measurements on subsystem B . Since the local entropy $S(\rho^A)$ is invariant under operations on B , this optimization is equivalent to finding the measurement basis that minimizes the conditional entropy $S(A|\{\Pi_i^{1,y}\})$.

For our bi-partite case, we optimize over the set of measurements $\{\Pi_i^{1,y}\}$: they are parameterized by the angles $\theta_d \in [0, \pi]$ and $\phi_d \in [0, 2\pi)$ on the Bloch sphere. The orthogonal basis states defining these measurements are given by:

$$|u\rangle = \begin{pmatrix} \cos \frac{\theta_d}{2} \\ e^{i\phi_d} \sin \frac{\theta_d}{2} \end{pmatrix}, \quad |v\rangle = \begin{pmatrix} \sin \frac{\theta_d}{2} \\ -e^{i\phi_d} \cos \frac{\theta_d}{2} \end{pmatrix}. \quad (6.8)$$

The corresponding projectors acting on subsystem B are $\Pi_0^{1,(\theta_d, \phi_d)} = |u\rangle\langle u|$ and $\Pi_1^{1,(\theta_d, \phi_d)} = |v\rangle\langle v|$. The conditional entropy is calculated using (1.26).

Finally, we implement a numerical optimization strategy to find the minimum conditional entropy. We include these two parameters, θ_d and ϕ_d , in the global non-linear optimization problem described in Section 6.1.1. This increases the total dimension of the search space, which in the end equals $N_D = 15 + 2(N_A - 1) + 2N_B + 2$.

6.2 Results

To characterize the boundary between non-classical correlations and Bell non-locality, we perform a numerical minimization of the quantum discord for two-qubit systems under a strict constraint of a Bell value $|\mathfrak{B}|_{\bar{p}} = \bar{p}|\mathfrak{B}|_{\mathcal{Q}}$, where $\bar{p} \in (0, 1]$ parametrizes the constraint by the fraction of the maximal quantum Bell value, Tsirelson's bound. For example, for CHSH and for $\bar{p} = \frac{1}{\sqrt{2}}$, the value comes down to the local bound $|\mathfrak{B}_{CHSH}|^{\bar{p}=1/\sqrt{2}} = \frac{1}{\sqrt{2}}|\mathfrak{B}_{CHSH}|_{\mathcal{Q}} = \frac{1}{\sqrt{2}} \cdot 2\sqrt{2} = 2 = |\mathfrak{B}_{CHSH}|_{\mathcal{L}}$. One of the constraints is thus that the Bell value for the optimized state and measurements $|\mathfrak{B}|_{opt}$ needs to stay very close to the Bell value for a given $\bar{p}$:

$$|\mathfrak{B}|_{\bar{p}} - \epsilon \leq |\mathfrak{B}|_{opt} \leq |\mathfrak{B}|_{\bar{p}} + \epsilon, \quad (6.9)$$

where ϵ is a small tolerance for a deviation. For our considerations, deviation tolerance equals $\epsilon = 10^{-3}$. The fraction $\bar{p}$ of the maximal quantum Bell value is related to the Werner state noise p : $\bar{p}|\mathfrak{B}|_{\mathcal{Q}} = (1 - p)|\mathfrak{B}|_{\mathcal{Q}}$.

To ensure that the minimization algorithm respects the restrictions mentioned, especially the normalization condition $\sum \mu_k = 1$, we employ the

COBYQA [148] algorithm. In this analysis, the defining property of this routine is its strict confinement to user-prescribed bounds, rendering it particularly suitable for optimization problems involving functions that are undefined outside the specified domain.

For complex regimes where local minima may emerge, we utilize a basin-hopping [187] global optimization routine. This, however, could lead to a problem with maintaining strict bounds. The basin-hopping method performs a perturbation of the optimized vector, without paying attention to the bounds defined in the minimization. If these bounds and constraints are exceeded, the minimization will be started in the range of states that are not valid quantum states (especially if the normalization condition $\sum \mu_k = 1$ is violated), leading to the possibility of negative discord, which is not allowed by quantum physics. To counter that, we have introduced two separate solutions: first, a reimplementaion of the step function has been provided, which does not allow exceeding the defined bounds and the normalization condition. Additionally, we have introduced a step rejection function that, after the minimization for a single basin-hopping step, verifies the correctness of the quantum state, rejecting the result in case of exceeding the bounds.

6.2.1 Discord for canonical Bell inequalities

In this section, we present the results of the non-linear discord function optimization for the three groups of Bell expressions: Clauser-Horne-Shimony-Holt inequality and modified CHSH (described in Section 5.2.1), Braunstein-Caves BC_3 and BC_5 inequalities (described in Section 5.2.2) and I_1/I_2 family (described in Section 5.2.3).

For CHSH and (5.17), the results of the optimization are presented in Figure 6.1. Consistent with the randomness certification in Section 5.2.1, for the modified CHSH expression (5.17), it is visible that all quantum correlations, including those measured by quantum discord, are not certified under the classical limit $|\mathfrak{B}|_{\mathcal{L}}$. This phenomenon is also present for CHSH and for other Bell expressions presented. As for the relation between CHSH and (5.17), it can be noticed that the shape of the discord function is the same for both; however, due to ModCHSH reaching $|\mathfrak{B}|_{\mathcal{L}}$ for higher fractions $\bar{p}$, the function is compressed along the X axis.

For the Braunstein-Caves family of chained Bell expressions, the results of the optimization are presented in Figure 6.2. For the higher fractions $\bar{p}$, it can be noticed that for both expressions, discord stays very close; any differences are likely attributable to numerical optimization errors of non-

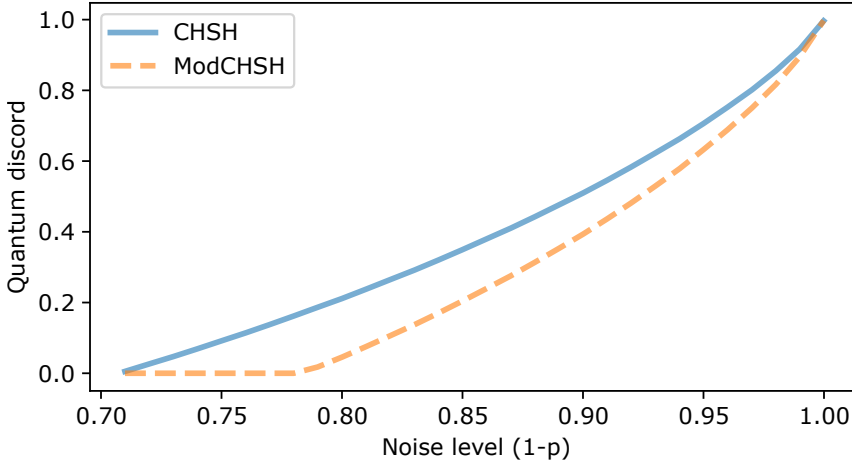


Figure 6.1: Lower bounds on quantum discord for CHSH inequality, as well as (5.17), as a function of the fraction $\bar{p}$ of the quantum bounds $|\mathfrak{B}_{CHSH}|_{\mathcal{Q}}$ or $|\mathfrak{B}_{Mod}|_{\mathcal{Q}}$, respectively.

linear optimization. After $\bar{p} = 0.95$ however, the graphs clearly deviate, with the BC_5 achieving lower discord values and losing any correlation for the noise level close to $\bar{p} = 0.85$, which corresponds to the local bound $|\mathfrak{B}_{BC_5}|_{\mathcal{L}}$ for this expression. This phenomenon is almost identical to the one presented by CHSH and (5.17).

For the I_n family of chained Bell expressions, the results of the optimization are presented in Figure 6.3. It can be noticed that for these expressions, the minimized discord plots for both I_1 and I_2 are very close, and they almost overlap to some extent. For certain noise fractions $\bar{p}$ I_2 , even overtakes I_1 . At high fractions ($\bar{p} > 0.95$), this behavior mirrors the phenomenon observed in the Braunstein-Caves family, where the discord values are so nearly identical that discrepancies likely arise from non-linear optimization limits. However, for $\bar{p} < 0.88$, the higher discord values for I_2 appear to be an intrinsic feature of the expression itself. The I_2 expression achieves its local bound $|\mathfrak{B}|_{\mathcal{L}}$ for higher noise, around $\bar{p} \approx 0.78$. Thus, it shows some level of quantum correlation (in this case, entanglement) also for noise values for which I_1 is entirely classical. Furthermore, these results are consistent with the randomness certification shown in Section 5.2.3, where I_2 started to certify more randomness around $p = 0.09$.

In Figure 6.4, we present the comparison of discord values optimized for all six Bell expressions analyzed. The highest minimal discord value

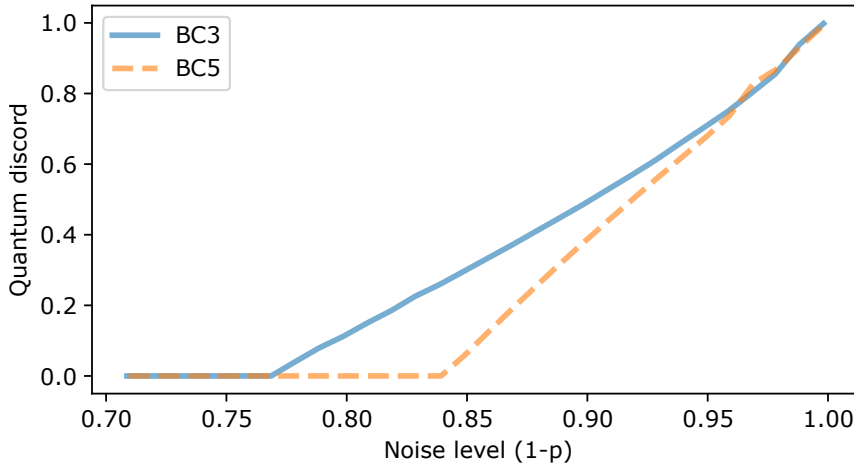


Figure 6.2: Lower bounds on quantum discord for the family of Braunstein-Caves inequalities, as a function of the fraction $\bar{p}$ of the quantum bounds $|\mathfrak{B}_{BC_n}|_{\mathcal{Q}}$.

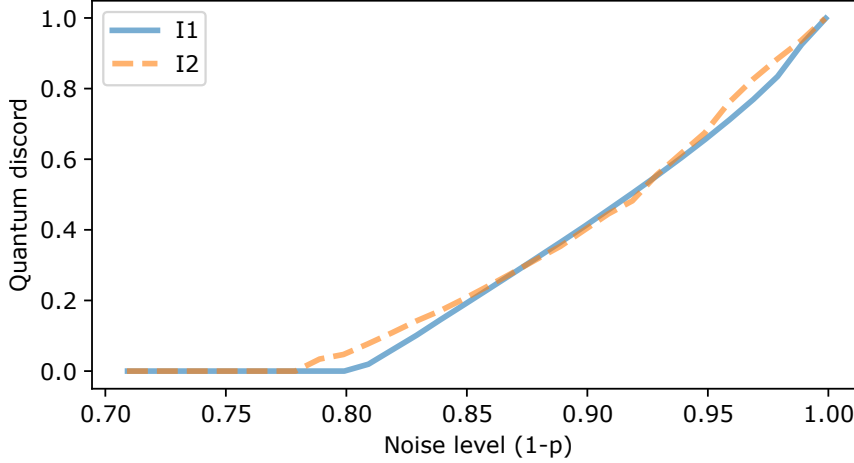


Figure 6.3: Lower bounds on quantum discord for the I_1 and I_2 inequalities, a function of the fraction $\bar{p}$ of the quantum bounds $|\mathfrak{B}_{I_1}|_{\mathcal{Q}}$ or $|\mathfrak{B}_{I_2}|_{\mathcal{Q}}$, respectively.

can be observed for CHSH for the whole spectrum of noise values, whereas the lowest minimal discord is represented by BC_5 . In general, for a larger number of measurement settings available for the parties, our discord lower bound decreases. Within the groups of expressions that represent the same number of settings (e.g., I_1 and I_2), the differences are minimal – they represent roughly the same level of quantum correlation. However, it can be noticed that (5.17) shows a level of quantum correlations close to the I_n family, while it allows two fewer settings for Alice and the same number for Bob.

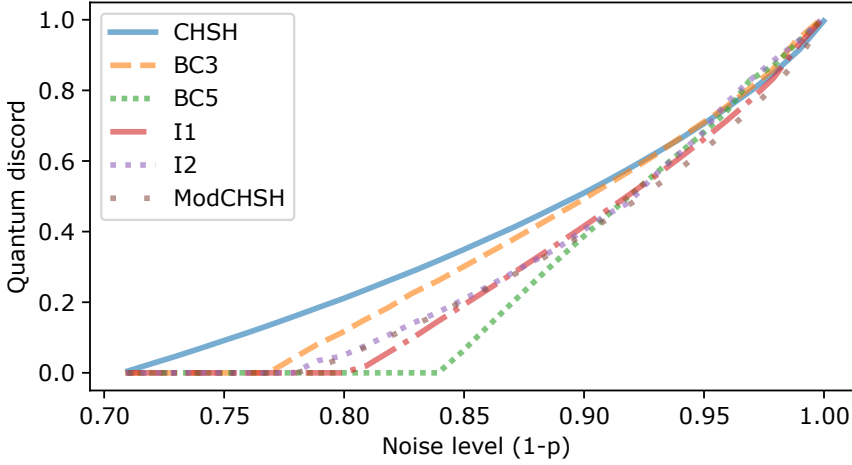


Figure 6.4: The summary of discord optimization results for all analyzed Bell expressions, as a function of the fraction $\hat{p}$ of the quantum bound $|\mathfrak{B}|_{\mathcal{Q}}$.

6.2.2 Structural Patterns in Discord Minimization

For the purpose of this analysis, around fifty numerical experiments were performed for each of the Bell expressions, with different optimization parameters such as: initial vector (fully randomized, established for a state with $|\mathfrak{B}|_{\mathcal{Q}}$ or with an initial vector taken from the state optimized for a previous fraction p), number of basin-hopping iterations, step size, and if it uses the default stepping method or our custom made.

The functions presented in Section 6.2.1 represent the minimal value obtained across all of the experiments, separately for every fraction $\hat{p}$ of the quantum bound $|\mathfrak{B}|_{\mathcal{Q}}$. However, by overlaying all results on a single plot, we can observe additional features of the experiments performed, revealing structural features of the optimization landscape.

In Figure 6.5, we present the aforementioned combined graph for the numerical experiments performed to minimize the discord function for the CHSH expression. A distinct pattern emerges, with most of the obtained quantum discord results bounded by two clear curves. One is the minimization curve used in the previous analysis, and the other is its symmetric counterpart (up to optimization error): a concave upper boundary that appears approximately symmetric to the lower convex curve to enclose the data. These two lines suggest the presence of two dominant classes of local minima, which may correspond to two distinct classes of quantum states.

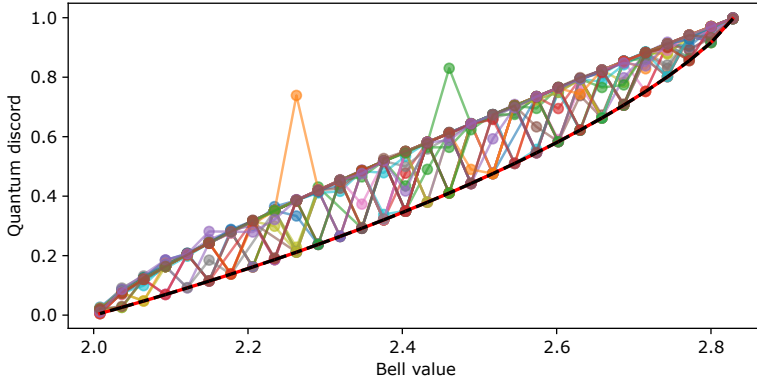


Figure 6.5: Combination of the results of numerical experiments undertaken to minimize the discord function for the CHSH expression, as a function of the value of the expression (Bell value).

In Figure 6.6, we combine the plots for the numerical experiments performed to minimize the discord function for the I_1 expression. Here, the two classes of states that we have mentioned before are also visible; however, additional observations can also be made. First, the greater number of deviations from the two classes of results suggests a more complex optimization landscape with additional local minima. Furthermore, there is a distinct subset of solutions that converges to a straight line and has slightly higher discord values than strict minimization. This suggests the possible presence of an additional local minimum in the vicinity of the optimal value.

In Figure 6.7, we combine the plots for the numerical experiments performed to minimize the discord function for the BC_5 expression. Here, the convexity of the minimum function is very close to a straight line, which deviates from the results presented in Figure 6.5, may indicate that the optimization frequently converged to a nearby local minimum observed in Figure 6.6. Nevertheless, this result might also be caused by other features

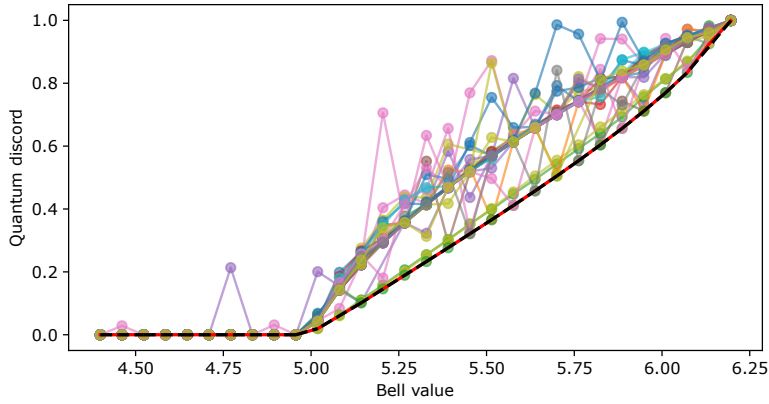


Figure 6.6: Combination of the results of numerical experiments undertaken to minimize the discord function for the I_1 expression, as a function of the value of the expression (Bell value).

resulting from the form of the expression. Without a full characterization of the function, it is not possible to state with certainty that values below the optimized ones are achievable.

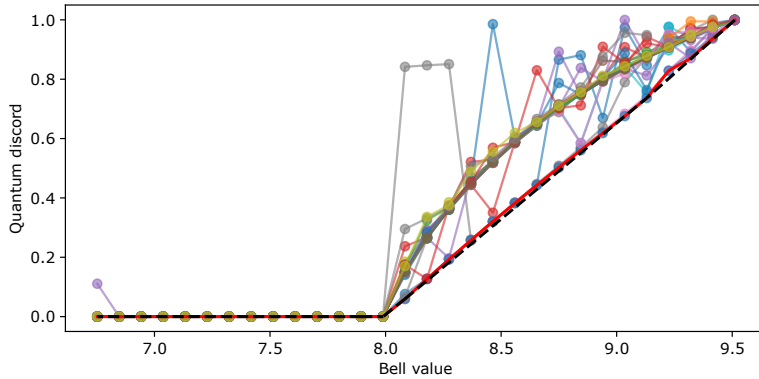


Figure 6.7: Combination of the results of numerical experiments undertaken to minimize the discord function for the BC_5 expression, as a function of the value of the expression (Bell value).

Concluding remarks

In this dissertation, we have explored the boundaries of quantum security and randomness through three main research directions: the vulnerabilities introduced by environmental decoherence, the development of robust certification methods for DI entropy, and the relationship between the description of the quantum correlations provided by quantum discord and Bell non-locality.

In Section 4, we evaluated the extent of eavesdropping facilitated by decoherence. We demonstrated how the process of information propagation, which is, according to the theory of QD, required during the decoherence of the measured state, inherently increases an eavesdropper's probability of correctly intercepting the accepted key bits. To model more sophisticated scenarios of this phenomenon, we introduce the concept of environmental layers. In our model, joint interactions between successive layers introduce stochastic noise, governed by a constant operator interaction noise factor ε . By utilizing this layered framework, we characterize the interaction dynamics and derive analytical expressions for both mutual information and the final key rate, expressed as functions of the guessing probability. Furthermore, we provide a generalized formula for interactions spanning an arbitrary number of single-qubit layers.

Through independent numerical analysis, we demonstrated how the distinguishability of environmental states produced by the BB84 transmission process changes depending on the level of noise present in the information dissipation process. Specifically, distinguishability declines significantly when the noise factor ε exceeds 0.5. Our numerical analysis indicated that a layered environmental model effectively captures decoherence dynamics; however, we find that larger layers render quantum communication protocols, such as BB84, more susceptible to eavesdropping. A delicate balance exists between layer dimensionality and noise parameters: while larger layers are required to mitigate higher noise levels (for larger layers and constant ε , P_{guess} is visibly lower), they simultaneously exacerbate vulnerability to

eavesdropping. Furthermore, while the complexity of multiple layers may hinder simplistic eavesdropping attempts, our results underscore the necessity of robust shielding mechanisms to maintain both measurement feasibility and cryptographic integrity. While our model primarily addresses vulnerabilities arising during the measurement phase, state preparation may also introduce security risks depending on the specific implementation. If the preparation method requires Alice to generate a state and subsequently measure it to verify its integrity, effectively forcing a collapse into the desired eigenstate, the process becomes functionally equivalent to the Bob's measurement dynamics analyzed herein.

Our results underscore the critical importance of robust shielding against information leakage facilitated by fundamental quantum processes. An adversary could potentially extract non-negligible information to compromise the communication channel by simply exploiting the natural decoherence of the system. Although it might be currently difficult to use this vulnerability in practical QKD communication, it is nonetheless a real theoretical threat, and given technological advances, it might be possible to execute this scheme.

It might be challenging to distinguish the states that contain the imprint of the BB84 state; however, it cannot be deemed inconceivable. The experimental feasibility of the QD scenario has been considered in, for example, [35]. Distinguishing environmental states that carry the imprint of a BB84 transmission presents a significant technical challenge; however, such a feat remains well within the realm of physical possibility. The experimental feasibility of QD has been explored in existing literature, notably in [35], where researchers demonstrated information transfer between a specific photonic quantum state and a multi-qubit photonic environment.

Critically, that study successfully quantified mutual information as a function of the noise interface between the system and its environment. This mechanism of information propagation mirrors the interaction between the consecutive layers proposed in our model, providing empirical evidence that such dynamics are not only theoretically sound but also experimentally observable.

In Chapter 5, we introduced a novel randomness certification framework utilizing the NPA hierarchy to establish rigorous bounds on probability distributions and their linear combinations. These bounds serve as the fundamental constraints for a non-linear optimization, allowing us to determine the Shannon entropy and subsequently perform the certification. Beyond this specific application, our methodology is extensible to any non-convex

optimization problem requiring the characterization of correlations derived from local measurements on a composite quantum system. This highlights the utility of our approach in broader contexts where the underlying set of quantum correlations must be precisely bounded.

Utilizing our framework, we conducted a comparative analysis of four distinct families of Bell inequalities as witnesses for randomness certification: the CHSH (including a modified variant), the Braunstein-Caves inequalities, the I_1/I_2 expressions, and the Woollorton-Brown-Colbeck inequalities. Our results identify the certificates for maintaining the robustness of a QRNG across varying noise thresholds. We highlighted significant discrepancies in the certification process when employing Shannon entropy, as opposed to the more conventionally utilized min-entropy, revealing critical implications for security bounds. In the process, we derived the analytical form of the Shannon entropy when constrained by the lower and upper probability bounds obtained via the NPA hierarchy. Furthermore, we introduced an analytical lower bound for the Shannon entropy, providing a computationally efficient alternative that bypasses the need for intensive non-linear optimization. Additionally, in Section 5.2.9, we have presented the Shannon entropy certification for a three-outcome scenario, showing a potential application for randomness extraction for qudits.

Furthermore, we developed and implemented a quantitative framework for the systematic evaluation of Bell expressions within the context of device-independent (DI) quantum randomness certification. We performed a high-throughput analysis of over 500 thousand Bell expressions and identified five prominent candidates distinguished by their entropy performance under varying levels of white noise. The comparison between analytical estimates and nonlinear optimization results revealed that the analytical entropy values act as upper bounds, underscoring the importance of non-linear refinement for precise quantification of certifiable randomness. We have also further investigated the self-testing properties of these selected Bell certificates by employing the self-testing for boxes formalism [12].

Our findings establish a connection between quantum entropy sources and classical cryptographic standards. While classical cryptography uses Shannon entropy to define theoretical secrecy limits, quantum protocols typically rely on min-entropy to address hardware biases. By strictly certifying Shannon entropy, we enable a rigorous, direct comparison between quantum sources and conventional randomness-generation methods.

In Chapter 6, we conducted a comprehensive numerical analysis of quantum discord by performing several dozen non-linear optimization experi-

ments for several Bell expressions to identify the global minimum across a spectrum of noise levels. The optimization of non-linear discord functions across diverse Bell inequalities reveals a consistent trend wherein quantum correlations, even those quantified by discord, vanish entirely as the system reaches its classical limit. Across all analyzed Bell expressions, quantum discord consistently vanishes at their respective classical limits. Furthermore, an increased number of measurement settings generally lowers the minimal discord bound, with CHSH maintaining the highest correlations. Furthermore, optimized quantum discord is visibly bounded by symmetric convex and concave curves, indicating two probable classes of quantum states. Nevertheless, much remains to be discovered regarding the link between quantum discord, Bell violations, and universal discord characterization. This study demonstrates that classifying quantum states by their discord values might uncover compelling new properties within these classes.

Open questions

The topics presented in this thesis can be further explored in a plethora of interesting directions. For example, future research on the intersection of QD and quantum cryptography can prioritize the development of security verification methods, specifically exploring semi-DI protocols [135] to mitigate the inherent risks of information spreading in the decoherence process.

Furthermore, the analysis of the entanglement-based QKD protocols in relation to the decoherence process and QD is the obvious next step in exploring the threats to widespread quantum communication.

Finally, the relationship between quantum discord and Bell violations, as well as more universal discord characterization, still holds many potential discoveries. The results presented in Chapter 6 clearly suggest that, by examining the further optimization process, we can discover interesting properties of classes of quantum states.

References

- [1] HotBits: Genuine random numbers, generated by radioactive decay. <https://www.fourmilab.ch/hotbits/>, 1996.
- [2] *Quantum Error Correction*. Cambridge University Press, 2013.
- [3] RANDOM.ORG - True Random Number Service. <https://www.random.org/>, 2024.
- [4] NIST Randomness Beacon (Version 2.0 Beta). <https://csrc.nist.gov/Projects/interoperable-randomness-beacons/beacon-20>, 2025.
- [5] Antonio Acín, Serge Massar, and Stefano Pironio. Randomness versus nonlocality and entanglement. *Physical Review Letters*, 108:100402, March 2012. doi: 10.1103/PhysRevLett.108.100402.
- [6] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani. Device-Independent Security of Quantum Cryptography against Collective Attacks. *Physical Review Letters*, 98(23), June 2007. doi: 10.1103/physrevlett.98.230501.
- [7] Kazimierz Ajdukiewicz. *The Scientific World-Perspective and Other Essays, 1931–1963*. Synthese Library. 1 edition, 1977. ISBN 978-90-277-0527-3. doi: 10.1007/978-94-010-1120-4.
- [8] Mohammed Ghaith Altarabichi, Sławomir Nowaczyk, Sepideh Pashami, Peyman Sheikholharam Mashhadi, and Julia Handl. Rolling the dice for better deep learning performance: A study of randomness techniques in deep neural networks. *Information Sciences*, 667: 120500, 2024. doi: 10.1016/j.ins.2024.120500.
- [9] Leandro Aolita, Rodrigo Gallego, Antonio Acín, Andrea Chiuri, Giuseppe Vallone, Paolo Mataloni, and Adán Cabello. Fully non-local quantum correlations. *Physical Review A*, 85:032107, March 2012. doi: 10.1103/PhysRevA.85.032107.
- [10] MOSEK ApS. *MOSEK Optimizer API for Python manual. Version 10.2.11.*, 2024. URL <https://docs.mosek.com/10.2/pythonapi/index.html>.

- [11] A. Aspect and P. Grangier. Experiments on einstein-podolsky-rosen correlations with pairs of visible photons. In Roger Penrose and C. J. Isham, editors, *Quantum concepts in space and time*. Oxford University Press, 1986. ISBN 9780198519720.
- [12] Michał Banacki, Piotr Mironowicz, Ravishankar Ramanathan, and Paweł Horodecki. Hybrid no-signaling-quantum correlations. *New Journal of Physics*, 24(8):083003, August 2022. ISSN 1367-2630. doi: 10.1088/1367-2630/ac7fb3.
- [13] Jean-Daniel Bancal, Lana Sheridan, and Valerio Scarani. More Randomness from the Same Data. *New Journal of Physics*, 16:033011, 2014. doi: 10.1088/1367-2630/16/3/033011.
- [14] Boaz Barak and Shai Halevi. A model and architecture for pseudo-random generation with applications to /dev/random. Technical report, Princeton University and IBM, September 2005.
- [15] Jonathan Barrett and Stefano Pironio. Popescu-Rohrlich Correlations as a Unit of Nonlocality. *Physical Review Letters*, 95(14), September 2005. ISSN 1079-7114. doi: 10.1103/physrevlett.95.140401.
- [16] Jonathan Barrett, Daniel Collins, Lucien Hardy, Adrian Kent, and Sandu Popescu. Quantum nonlocality, bell inequalities, and the memory loophole. *Physical Review A*, 66:042111, October 2002. doi: 10.1103/PhysRevA.66.042111.
- [17] Lawrence E. Bassham, Andrew L. Rukhin, Juan Soto, James R. Nechvatal, Miles E. Smid, Elaine B. Barker, Stefan D. Leigh, Mark Levenson, Mark Vangel, David L. Banks, Nathanael Alan Heckert, James F. Dray, and San Vo. SP 800-22 Rev. 1a. A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications. 2010. doi: 10.5555/2206233.
- [18] John Stewart Bell. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1:195–200, November 1964. doi: 10.1103/PhysicsPhysiqueFizika.1.195.
- [19] Charles H. Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560:7–11, December 2014. doi: 10.1016/j.tcs.2014.05.025.
- [20] Mario Berta, Omar Fawzi, and Stephanie Wehner. Quantum to Classical Randomness Extractors. *IEEE Transactions on Information Theory*, 60(2):1168–1192, February 2014. doi: 10.1109/tit.2013.2291780.
- [21] Jacob Biamonte, Peter Wittek, Nicola Pancotti, Patrick Rebentrost, Nathan Wiebe, and Seth Lloyd. Quantum machine learning. *Nature*, 549(7671):195–202, September 2017. ISSN 1476-4687. doi: 10.1038/

- nature23474.
- [22] Robin Blume-Kohout and Wojciech H. Żurek. A simple example of Quantum Darwinism: Redundant information storage in many-spin environments. *Foundations of Physics*, 35:1857–1876, 2005. doi: 10.1007/s10701-005-7352-5.
 - [23] Stephen Boyd, Laurent El Ghaoui, Eric Feron, and Venkataramanan Balakrishnan. *Linear matrix inequalities in system and control theory*, volume 15. SIAM, 1994.
 - [24] Samuel L. Braunstein and Carlton M. Caves. Information-theoretic Bell Inequalities. *Physical Review Letters*, 61:662–665, August 1988. doi: 10.1103/PhysRevLett.61.662.
 - [25] Stephen Brierley, Miguel Navascues, and Tamas Vertesi. Convex separation from convex optimization for large-scale problems. 2017. arXiv: 1609.05011.
 - [26] Aharon Brodutch and Daniel Terno. Why Should We Care About Quantum Discord? In *Quantum Science and Technology*, pages 183–199. Springer International Publishing, 2017. doi: 10.1007/978-3-319-53412-1_8.
 - [27] Harry Buhrman and Serge Massar. Causality and Tsirelson’s bounds. *Physical Review A*, 72:052103, November 2005. doi: 10.1103/PhysRevA.72.052103.
 - [28] Barış Çakmak, Özgür E. Müstecaplıoğlu, Mauro Paternostro, Bassano Vacchini, and Steve Campbell. Quantum Darwinism in a composite system: Objectivity versus classicality. *Entropy*, 23(8):995, 2021. doi: 10.3390/e23080995.
 - [29] A. Robert Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Physical Review A*, 54(2):1098–1105, August 1996. ISSN 1094-1622. doi: 10.1103/physreva.54.1098.
 - [30] Edwin Cartlidge. Quantum keys sent along fiber and into space. Accessed: 2026-04-04.
 - [31] D. Cavalcanti, L. Aolita, S. Boixo, K. Modi, M. Piani, and A. Winter. Operational interpretations of quantum discord. *Physical Review A*, 83(3):032324, 2011.
 - [32] Ming-Cheng Chen, Han-Sen Zhong, Yuan Li, Dian Wu, Xi-Lin Wang, Li Li, Nai-Le Liu, Chao-Yang Lu, and Jian-Wei Pan. Emergence of classical objectivity of quantum Darwinism in a photonic quantum simulator. *Science Bulletin*, 64(9):580–585, 2019. doi: 10.1016/j.scib.2019.03.032.
 - [33] Yu-Ao Chen, Qiang Zhang, Teng-Yun Chen, Wen-Qi Cai, Sheng-Kai

- Liao, Jun Zhang, Kai Chen, Juan Yin, Ji-Gang Ren, Zhu Chen, et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature*, 589(7841):214–219, 2021. doi: 10.1038/s41586-020-03093-8.
- [34] Shubham Chouhan, K. S. V. Anurag, G. Raghavan, and P Kanaka Raju. FPGA-based Toeplitz Strong Extractor for Quantum Random Number Generators. In *2024 IEEE 5th India Council International Subsections Conference (INDISCON)*, page 1–5. IEEE, August 2024. doi: 10.1109/indiscon62179.2024.10744392.
- [35] Mario A. Ciampini, Giorgia Pinna, Paolo Mataloni, and Mauro Paternostro. Experimental signature of quantum Darwinism in photonic cluster states. *Physical Review A*, 98:020101, August 2018. doi: 10.1103/PhysRevA.98.020101.
- [36] John F. Clauser, Michael A. Horne, Abner Shimony, and Richard A. Holt. Proposed Experiment to Test Local Hidden-Variable Theories. *Physical Review Letters*, 23:880–884, October 1969. doi: 10.1103/PhysRevLett.23.880.
- [37] Timothy H. Click, Aibing Liu, and George A. Kaminski. Quality of random number generators significantly affects results of Monte Carlo simulations for organic and biological systems. *Journal of Computational Chemistry*, 32(3):513–524, 2011. doi: 10.1002/jcc.21638.
- [38] Roger Colbeck. Quantum and relativistic protocols for secure multi-party computation. 2011. arXiv: 0911.3814.
- [39] Roger Colbeck and Adrian Kent. Private randomness expansion with untrusted devices. *Journal of Physics A: Mathematical and Theoretical*, 44(9):095305, February 2011. doi: 10.1088/1751-8113/44/9/095305.
- [40] Matthew Coudron, Thomas Vidick, and Henry Yuen. Robust Randomness Amplifiers: Upper and Lower Bounds. In Prasad Raghavendra, Sofya Raskhodnikova, Klaus Jansen, and José D. P. Rolim, editors, *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*, pages 468–483, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg. ISBN 978-3-642-40328-6.
- [41] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory*. John Wiley & Sons, Hoboken, New Jersey, 2nd edition, 2012. ISBN 978-0-471-24195-9. doi: 10.1002/047174882X.
- [42] Creotech Instruments S.A. Creotech Instruments członkiem konsorcjum współtworzącym stację naziemną na potrzeby kwantowej dystrybucji klucza (QKD). creotech.pl, December 2025. Accessed: 2026-

04-04.

- [43] Imre Csiszar and János Körner. Broadcast channels with confidential messages. *IEEE Transactions on Information Theory*, 24(3):339–348, 1978. doi: 10.1109/TIT.1978.1055892.
- [44] FM Cucchietti, Juan Pablo Paz, and Wojciech H. Żurek. Decoherence from spin environments. *Physical Review A*, 72(5):052113, 2005. doi: 10.1103/PhysRevA.72.052113.
- [45] Borivoje Dakić, Yannick Ole Lipp, Xiaosong Ma, Martin Ringbauer, Sebastian Kropatschek, Stefanie Barz, Tomasz Paterek, Vlatko Vedral, Anton Zeilinger, Časlav Brukner, and Philip Walther. Quantum discord as resource for remote state preparation. *Nature Physics*, 8: 666–670, 2012.
- [46] Animesh Datta, Anil Shaji, and Carlton M. Caves. Quantum discord and the power of one qubit. *Physical Review Letters*, 100:050502, 2008. doi: 10.1103/PhysRevLett.100.050502.
- [47] Anna Dawid, Julian Arnold, Borja Requena, Alexander Gresch, Marcin Płodzień, Kaelan Donatella, Kim A. Nicoli, Paolo Stornati, Rouven Koch, Miriam Büttner, Robert Okuła, et al. *Machine Learning in Quantum Sciences*. Cambridge University Press, Cambridge, 2025. ISBN 978-1-009-50493-5. doi: 10.1017/9781009504942.
- [48] Anindya De, Christopher Portmann, Thomas Vidick, and Renato Renner. Trevisan’s extractor in the presence of quantum side information. *SIAM Journal on Computing*, 41(4):915–940, January 2012. ISSN 1095-7111. doi: 10.1137/100813683.
- [49] Elke De Mulder, Siddika Berna Örs, Bart Preneel, and Ingrid Verbauwhede. Differential power and electromagnetic attacks on a FPGA implementation of elliptic curve cryptosystems. *Computers & Electrical Engineering*, 33(5-6):367–382, 2007. doi: 10.1016/j.compeleceng.2007.05.009.
- [50] Sébastien Designolle, Gabriele Iommazzo, Mathieu Besançon, Sebastian Knebel, Patrick Gelß, and Sebastian Pokutta. Improved local models and new Bell inequalities via Frank-Wolfe algorithms. *Physical Review Research*, 5(4), October 2023. ISSN 2643-1564. doi: 10.1103/physrevresearch.5.043059.
- [51] David Deutsch. Quantum theory as a universal physical theory. *International Journal of Theoretical Physics*, 24:1–41, 1985. doi: 10.1007/BF00670071.
- [52] Péter Diviánszky, Erika Bene, and Tamás Vértesi. Qutrit witness from the Grothendieck constant of order four. *Physical Review A*, 96:

- 012113, July 2017. doi: 10.1103/PhysRevA.96.012113.
- [53] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal. Locking classical correlation in quantum states. *Physical Review Letters*, 92(6):067902, 2004.
 - [54] Thomas Durt, Berthold-Georg Englert, Ingemar Bengtsson, and Karol Życzkowski. On mutually unbiased bases. *International Journal of Quantum Information*, 8(04):535–640, 2010. doi: 10.1142/S0219749910006502.
 - [55] Philippe H. Eberhard. Background level and counter efficiencies required for a loophole-free einstein-podolsky-rosen experiment. *Physical Review A*, 47:R747–R750, February 1993. doi: 10.1103/PhysRevA.47.R747.
 - [56] Albert Einstein, Boris Podolsky, and Nathan Rosen. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Physical Review*, 47:777–780, May 1935. doi: 10.1103/PhysRev.47.777.
 - [57] Artur K. Ekert. Quantum cryptography based on Bell’s theorem. *Physical Review Letters*, 67:661–663, August 1991. doi: 10.1103/PhysRevLett.67.661.
 - [58] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE transactions on information theory*, 31(4):469–472, 1985.
 - [59] European Commission. The European Quantum Communication Infrastructure (EuroQCI). digital-strategy.ec.europa.eu, 2024. Accessed: 2026-04-04.
 - [60] European Space Agency. Eagle-1: Europe’s first space-based quantum key distribution system. esa.int, 2024. Accessed: 2026-04-04.
 - [61] Massimo Falcioni, Luigi Palatella, Simone Pigolotti, and Angelo Vulpiani. Properties making a chaotic system a good pseudo random number generator. *Physical Review E*, 72(1), July 2005. doi: 10.1103/physreve.72.016220.
 - [62] Niels Ferguson and Bruce Schneier. *Practical Cryptography*. Wiley, New York, NY, USA, 2003. ISBN 978-0-471-22357-3.
 - [63] A. Ferraro, L. Aolita, D. Cavalcanti, F. M. Cucchietti, and A. Acín. Almost all quantum states have nonclassical correlations. *Physical Review A*, 81(5):052318, 2010. doi: 10.1103/PhysRevA.81.052318.
 - [64] Aurelien Francillon and Claude Castelluccia. Tinyrng: A cryptographic random number generator for wireless sensors network nodes. In *2007 5th International Symposium on Modeling and Optimization*

- in Mobile, Ad Hoc and Wireless Networks and Workshops*, pages 1–7, 2007. doi: 10.1109/WIOPT.2007.4480051.
- [65] Harald Fürst, Henning Weier, Sebastian Nauerth, Davide G. Marangon, Christian Kurtsiefer, and Harald Weinfurter. High speed optical quantum random number generation. *Optics Express*, 18(12): 13029–13037, June 2010. doi: 10.1364/OE.18.013029.
- [66] Christian Gabriel, Christoffer Wittmann, Denis Sych, Ruifang Dong, Wolfgang Maurer, Ulrik L. Andersen, Christoph Marquardt, and Gerd Leuchs. A generator for unique quantum random numbers based on vacuum states. *Nature Photonics*, 4(10):711–715, 2010. doi: 10.1038/nphoton.2010.197.
- [67] Rodrigo Gallego, Nicolas Brunner, Christopher Hadley, and Antonio Acín. Device-independent tests of classical and quantum dimensions. *Physical Review Letters*, 105(23), November 2010. ISSN 1079-7114. doi: 10.1103/physrevlett.105.230501.
- [68] Anupam Garg and N. D. Mermin. Detector inefficiencies in the einstein-podolsky-rosen experiment. *Physical Review D*, 35:3831–3835, June 1987. doi: 10.1103/PhysRevD.35.3831.
- [69] Nicolas Gisin and Helle Bechmann-Pasquinucci. Bell inequality, Bell states and maximally entangled states for n qubits. *Physics Letters A*, 246(1–2):1–6, September 1998. ISSN 0375-9601. doi: 10.1016/s0375-9601(98)00516-7.
- [70] Nicolas Gisin, Grégoire Ribordy, Wolfgang Tittel, and Hugo Zbinden. Quantum cryptography. *Reviews of Modern Physics*, 74:145–195, March 2002. doi: 10.1103/RevModPhys.74.145.
- [71] Michel X Goemans and David P Williamson. Improved approximation algorithms for maximum cut and satisfiability problems using semidefinite programming. *Journal of the ACM (JACM)*, 42(6):1115–1145, 1995.
- [72] Ian Goldberg and David Wagner. Randomness and the netscape browser. *Dr. Dobbs’s Journal*, pages 66–70, 1996.
- [73] Daniel Gottesman and Isaac Chuang. Quantum Digital Signatures. 2001.
- [74] Carl W. Helstrom. Quantum detection and estimation theory. *Journal of Statistical Physics*, 1(2):231–252, 1969. ISSN 1572-9613. doi: 10.1007/BF01007479.
- [75] L. Henderson and V. Vedral. Classical, quantum and total correlations. *Journal of Physics A: Mathematical and General*, 34(35):6899, 2001. doi: 10.1088/0305-4470/34/35/310.

- [76] B. Hensen, H. Bernien, A. E. Dréau, A. Reiserer, N. Kalb, M. S. Blok, J. Ruitenbergh, R. F. L. Vermeulen, R. N. Schouten, C. Abellán, W. Amaya, V. Pruneri, M. W. Mitchell, M. Markham, D. J. Twitchen, D. Elkouss, S. Wehner, T. H. Taminiau, and R. Hanson. Loophole-free bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575):682–686, October 2015. ISSN 1476-4687. doi: 10.1038/nature15759.
- [77] Fedor Herbut. A Review of Unitary Quantum Premeasurement Theory An Algebraic Study of Basic Kinds of Premeasurements. 2014. arXiv: 1412.7862.
- [78] Miguel Herrero-Collantes and Juan Carlos Garcia-Escartin. Quantum random number generators. *Reviews of Modern Physics*, 89:015004, February 2017. doi: 10.1103/RevModPhys.89.015004.
- [79] Thomas Van Himbeeck and Stefano Pironio. Correlations and randomness generation based on energy constraints. 2019. arXiv: 1905.09117.
- [80] Thomas Holenstein. Pseudorandom Generators from One-Way Functions: A Simple Construction for Any Hardness. In Shai Halevi and Tal Rabin, editors, *Theory of Cryptography*, pages 443–461, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg. ISBN 978-3-540-32732-5.
- [81] A.S Holevo. Statistical decision theory for quantum systems. *Journal of Multivariate Analysis*, 3(4):337–394, 1973. ISSN 0047-259X. doi: 10.1016/0047-259X(73)90028-6.
- [82] Yichen Huang. Computing quantum discord is np-complete. *New Journal of Physics*, 16(3):033027, March 2014. doi: 10.1088/1367-2630/16/3/033027.
- [83] David A. Huffman. A method for the construction of minimum-redundancy codes. *Proceedings of the IRE*, 40(9):1098–1101, 1952.
- [84] Marie Ioannou and Denis Rosset. Noncommutative polynomial optimization under symmetry, 2021.
- [85] Alban Jean-Marie Seguinard, Amélie Piveteau, Piotr Mironowicz, and Mohamed Bourennane. Experimental certification of more than one bit of quantum randomness in the two inputs and two outputs scenario. *New Journal of Physics*, 25(11):113022, November 2023. doi: 10.1088/1367-2630/ad05a6.
- [86] Chunlin Yu Jiajie Wu Tongge Zhao Xiangwei Zhu Jialiang Li, Zitao Huang and Shihai Sun. Quantum random number generation based on phase reconstruction. *Optics Express*, 32(4):5056, 2024. doi:

- 10.1364/OE.513374.
- [87] Lu Johnston et al. A 3.3-Gb/s SPAD-based quantum random number generator. *IEEE Journal of Solid-State Circuits*, 58(9):2632–2647, 2023. doi: 10.1109/JSSC.2023.3283733.
- [88] Jędrzej Kaniewski, Ivan Šupić, Jordi Tura, Flavio Baccari, Alexia Salavrakos, and Remigiusz Augusiak. Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems. *Quantum*, 3:198, October 2019. ISSN 2521-327X. doi: 10.22331/q-2019-10-24-198.
- [89] Prem Nigam Kar, David E. Roberson, Tim Seppelt, and Peter Zeman. NPA hierarchy for quantum isomorphism and homomorphism indistinguishability. In *52nd International Colloquium on Automata, Languages, and Programming (ICALP 2025)*, volume 334 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 105:1–105:19. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2025.
- [90] John Kelsey, Bruce Schneier, David Wagner, and Chris Hall. Cryptanalytic attacks on pseudorandom number generators. In *Fast Software Encryption (FSE ’98)*, volume 1372 of *Lecture Notes in Computer Science*, pages 168–188. Springer, 1998.
- [91] Neal Koblitz. Elliptic curve cryptosystems. *Mathematics of computation*, 48(177):203–209, 1987.
- [92] Aki Koivu, Joona-Pekko Kakko, Santeri Mäntyniemi, and Mikko Sairanen. Quality of randomness and node dropout regularization for fitting neural networks. *Expert Systems with Applications*, 207: 117938, 2022. doi: 10.1016/j.eswa.2022.117938.
- [93] Otto C. W. Kong and Hock King Ting. Mixed-state parameterization and two-qubit entanglement. *Quantum Information Processing*, 21(7): 241, July 2022. ISSN 1573-1332. doi: 10.1007/s11128-022-03589-4.
- [94] Gereon Koßmann and René Schwonnek. Bounding the conditional von-Neumann entropy for device independent cryptography and randomness extraction. 2024. arXiv: 2411.04858.
- [95] Markus G. Kuhn. Security limits for compromising emanations. In *Cryptographic Hardware and Embedded Systems–CHES 2005: 7th International Workshop, Edinburgh, UK, August 29–September 1, 2005. Proceedings 7*, pages 265–279. Springer, 2005. doi: 10.1007/11545262_20.
- [96] Osung Kwon, Young-Wook Cho, and Yoon-Ho Kim. Quantum random number generator using photon-number path entanglement. *Applied Optics*, 48(9):1774, March 2009. doi: 10.1364/ao.48.001774.

- [97] Corentin Lavaud, Robin Gerzaguët, Matthieu Gautier, Olivier Berder, Erwan Nogues, and Stephane Molton. Whispering devices: A survey on how side-channels lead to compromised information. *Journal of Hardware and Systems Security*, 5:143–168, 2021. doi: 10.1007/s41635-021-00112-6.
- [98] Euibum Lee, Dong-Hoon Choi, Taesik Nam, and Jong-Gwan Yook. A quantitative analysis of compromising emanation from TMDS interface and possibility of sensitive information leakage. *IEEE Access*, 10:73997–74011, 2022. doi: 10.1109/ACCESS.2022.3184294.
- [99] Anthony J. Leggett. The quantum measurement problem. *Science*, 307(5711):871–872, 2005. doi: 10.1126/science.1109541.
- [100] Arjen K. Lenstra, James P. Hughes, Maxime Augier, Joppe W. Bos, Thorsten Kleinjung, and Christophe Wachter. Ron was wrong, whit is right. Cryptology ePrint Archive, Paper 2012/064, 2012.
- [101] Mark Leuchter. Jeremiah’s 70-Year Prophecy and the Atbash Codes. *Biblica*, 85(4):503–522, 2004. ISSN 00060887. doi: 10.2143/BIB.85.4.3194438.
- [102] Hong-Wei Li, Piotr Mironowicz, Marcin Pawłowski, Zhen-Qiang Yin, Yu-Chun Wu, Shuang Wang, Wei Chen, Hong-Gang Hu, Guang-Can Guo, and Zheng-Fu Han. Relationship between semi- and fully-device-independent protocols. *Physical Review A*, 87:020302, February 2013. doi: 10.1103/PhysRevA.87.020302.
- [103] Ming-Han Li, Xingjian Zhang, Wen-Zhao Liu, Si-Ran Zhao, Bing Bai, Yang Liu, Qi Zhao, Yuxiang Peng, Jun Zhang, Yanbao Zhang, W.J. Munro, Xiongfeng Ma, Qiang Zhang, Jingyun Fan, and Jian-Wei Pan. Experimental Realization of Device-Independent Quantum Randomness Expansion. *Physical Review Letters*, 126(5), February 2021. ISSN 1079-7114. doi: 10.1103/physrevlett.126.050503.
- [104] Joe Loughry and David A Umphress. Information leakage from optical emanations. *ACM Transactions on Information and System Security (TISSEC)*, 5(3):262–289, 2002. doi: 10.1145/545186.545189.
- [105] Norbert Lütkenhaus. Security against individual attacks for realistic quantum key distribution. *Physical Review A*, 61(5), April 2000. ISSN 1094-1622. doi: 10.1103/physreva.61.052304.
- [106] Anindya Maiti and Murtuza Jadliwala. Light ears: Information leakage via smart lights. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 3(3):1–27, 2019. doi: 10.1145/3351256.
- [107] Vaisakh Mannalatha, Sandeep Mishra, and Anirban Pathak. A

- comprehensive review of quantum random number generators: concepts, classification and the origin of randomness. *Quantum Information Processing*, 22(12):439, December 2023. ISSN 1573-1332. doi: 10.1007/s11128-023-04175-y.
- [108] Lluís Masanes, Renato Renner, Matthias Christandl, Andreas Winter, and Jonathan Barrett. Full security of quantum key distribution from no-signaling constraints. *IEEE Transactions on Information Theory*, 60(8):4973–4986, 2014. doi: 10.1109/TIT.2014.2329417.
 - [109] Dominic Mayers and Andrew Yao. Quantum Cryptography with Imperfect Apparatus. In *Proceedings of the 39th Annual Symposium on Foundations of Computer Science*, FOCS '98, page 503, USA, 1998. IEEE Computer Society. ISBN 0818691727.
 - [110] Sonia Mazzucchi et al. Entropy certification of a realistic QRNG based on single-particle entanglement. *Physical Review A*, 104(2):022416, 2021. doi: 10.1103/PhysRevA.104.022416.
 - [111] Thomas S Messerges, Ezzy A Dabbish, and Robert H Sloan. Investigations of power analysis attacks on smartcards. *Smartcard*, 99:151–161, 1999. doi: 10.5555/1267115.1267132.
 - [112] Nadia Milazzo, Salvatore Lorenzo, Mauro Paternostro, and G. Massimo Palma. Role of information backflow in the emergence of quantum Darwinism. *Physical Review A*, 100(1):012101, 2019. doi: 10.1103/PhysRevA.100.012101.
 - [113] Carl A. Miller and Yaoyun Shi. Universal Security for Randomness Expansion from the Spot-Checking Protocol. *SIAM Journal on Computing*, 46(4):1304–1335, 2017. doi: 10.1137/15M1044333.
 - [114] Piotr Mironowicz. Applications of semi-definite optimization in quantum information protocols, 2018. Doctoral dissertation, arXiv: 1810.05145.
 - [115] Piotr Mironowicz. Quantum security and theory of decoherence. *New Journal of Physics*, 24(11):113054, December 2022. doi: 10.1088/1367-2630/aca558.
 - [116] Piotr Mironowicz and Marcin Pawłowski. Robustness of quantum-randomness expansion protocols in the presence of noise. *Physical Review A*, 88(3), September 2013. doi: 10.1103/physreva.88.032319.
 - [117] Piotr Mironowicz, Jarosław K. Korbicz, and Paweł Horodecki. Monitoring of the Process of System Information Broadcasting in Time. *Physical Review Letters*, 118:150501, April 2017. doi: 10.1103/PhysRevLett.118.150501.
 - [118] Piotr Mironowicz, Paweł Należyty, Paweł Horodecki, and Jarosław K.

- Korbicz. System information propagation for composite structures. *Physical Review A*, 98(2):022124, 2018. doi: 10.1103/PhysRevA.98.022124.
- [119] Piotr Mironowicz, Marcus Grünfeld, and Mohamed Bourennane. Generalized measurements on qubits in quantum randomness certification and expansion. *Physical Review Applied*, 22:044041, October 2024. doi: 10.1103/PhysRevApplied.22.044041.
- [120] Kavan Modi, Aharon Brodutch, Hugo Cable, Tomasz Paterek, and Vlatko Vedral. The classical-quantum boundary for correlations: Discord and related measures. *Reviews of Modern Physics*, 84:1655–1707, 2012. doi: 10.1103/RevModPhys.84.1655.
- [121] Vardaan Mongia, Abhishek Kumar, Shashi Prabhakar, Anindya Banerji, and R.P. Singh. Investigating device-independent quantum random number generation. *Physics Letters A*, 526:129954, 2024. doi: 10.1016/j.physleta.2024.129954.
- [122] Santiago Morales-Aguilar, Chaouki Kasmi, Milosch Meriac, Felix Vega, and Fahad Alyafei. Digital images preprocessing for optical character recognition in video frames reconstructed from compromising electromagnetic emanations from video cables. In *2020 XXXIIIrd General Assembly and Scientific Symposium of the International Union of Radio Science*, pages 1–4. IEEE, 2020. doi: 10.23919/URSIGASS49373.2020.9232388.
- [123] Tobias Moroder, Jean-Daniel Bancal, Yeong-Cherng Liang, Martin Hofmann, and Otfried Gühne. Device-independent entanglement quantification and related applications. *Physical Review Letters*, 111(3):030501, 2013.
- [124] Ben Nassi, Yaron Pirutin, Tomer Galor, Yuval Elovici, and Boris Zadov. Glowworm attack: Optical tempest sound recovery via a device’s power indicator LED. In *Proceedings of the 2021 ACM SIGSAC Conference on Computer and Communications Security*, pages 1900–1914, 2021. doi: 10.1145/3460120.3484775.
- [125] Miguel Navascués, Stefano Pironio, and Antonio Acín. Bounding the Set of Quantum Correlations. *Physical Review Letters*, 98:010401, January 2007. doi: 10.1103/PhysRevLett.98.010401.
- [126] Miguel Navascués, Stefano Pironio, and Antonio Acín. A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations. *New Journal of Physics*, 10(7):073013, July 2008. doi: 10.1088/1367-2630/10/7/073013.
- [127] Jorge Nocedal and Stephen J. Wright. *Numerical Optimization*.

- Springer, New York, NY, 2nd edition, 2006.
- [128] Ali Ibnun Nurhadi and Nana Rachmana Syambas. Quantum Key Distribution (QKD) Protocols: A Survey. In *2018 4th International Conference on Wireless and Telematics (ICWT)*, pages 1–5, 2018. doi: 10.1109/ICWT.2018.8527822.
 - [129] Robert Okuła and Piotr Mironowicz. How decoherence affects the security of BB84 quantum key distribution protocol. *Quantum Information Processing*, 24(2), February 2025. ISSN 1573-1332. doi: 10.1007/s11128-025-04650-8.
 - [130] Robert Okuła and Piotr Mironowicz. Device-independent Shannon entropy certification. *New Journal of Physics*, 27(11):114519, November 2025. ISSN 1367-2630. doi: 10.1088/1367-2630/ae20b2.
 - [131] Robert Okuła and Piotr Mironowicz. Extensive search of Shannon entropy-based randomness certification protocols, 2025. arXiv: 2511.22771.
 - [132] Harold Ollivier, David Poulin, and Wojciech H. Żurek. Objective properties from subjective quantum states: Environment as a witness. *Physical Review Letters*, 93(22):220401, 2004. doi: 10.1103/PhysRevLett.93.220401.
 - [133] Harold Ollivier and Wojciech H. Żurek. Quantum Discord: A Measure of the Quantumness of Correlations. *Physical Review Letters*, 88: 017901, 2001. doi: 10.1103/PhysRevLett.88.017901.
 - [134] Elsa Passaro, Daniel Cavalcanti, Paul Skrzypczyk, and Antonio Acín. Optimal randomness certification in the quantum steering and prepare-and-measure scenarios. *New Journal of Physics*, 17(11): 113010, October 2015. doi: 10.1088/1367-2630/17/11/113010.
 - [135] Marcin Pawłowski and Nicolas Brunner. Semi-device-independent security of one-way quantum key distribution. *Physical Review A*, 84 (1):010302, 2011. doi: 10.1103/PhysRevA.84.010302.
 - [136] Marcin Pawłowski, Tomasz Paterek, Dagomir Kaszlikowski, Valerio Scarani, Andreas Winter, and Marek Żukowski. Information causality as a physical principle. *Nature*, 461(7267):1101–1104, October 2009. ISSN 1476-4687. doi: 10.1038/nature08400.
 - [137] Juan Pablo Paz and Wojciech H. Żurek. Environment-induced decoherence and the transition from quantum to classical. In *Fundamentals of quantum information: quantum computation, communication, decoherence and all that*, pages 77–148. 2002. doi: 10.1007/3-540-45933-2.
 - [138] Stefano Pirandola. Quantum discord as a resource for quantum cryp-

- tography. *Scientific Reports*, 4:6956, 2014. doi: 10.1038/srep06956.
- [139] Stefano Pirandola, Ulrik L. Andersen, Leonardo Banchi, Mario Berta, Darius Bunandar, Roger Colbeck, Dirk Englund, Tobias Gehring, Cosmo Lupo, Carlo Ottaviani, et al. Advances in quantum cryptography. *Advances in Optics and Photonics*, 12(4):1012–1236, 2020. doi: 10.1364/AOP.361502.
 - [140] Stefano Pironio and Serge Massar. Security of practical private randomness generation. *Physical Review A*, 87(1), January 2013. ISSN 1094-1622. doi: 10.1103/physreva.87.012336.
 - [141] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, 11(4):045021, April 2009. doi: 10.1088/1367-2630/11/4/045021.
 - [142] Stefano Pironio, Antonio Acín, Serge Massar, A Boyer de La Giroday, Dzmitry N Matsukevich, Peter Maunz, Steven Olmschenk, David Hayes, Lefroy Luo, Andrew Manning, and Christopher Monroe. Random Numbers Certified by Bell’s Theorem. *Nature*, 464(7291):1021–1024, April 2010. doi: 10.1038/nature09008.
 - [143] Stefano Pironio, Miguel Navascués, and Antonio Acín. Convergent relaxations of polynomial optimization problems with noncommuting variables. *SIAM Journal on Optimization*, 20(5):2157–2180, 2010.
 - [144] Amelie Piveteau, Alban Seguinard, Piotr Mironowicz, and Mohamed Bourennane. Optimization of experimental quantum randomness expansion. *Physical Review Applied*, 24:044096, October 2025. doi: 10.1103/hc3f-3pbw.
 - [145] Poznańskie Centrum Superkomputerowo-Sieciowe. EuroQCI: quantum connections between Poland and Europe coming soon. psnc.pl, 2024. Accessed: 2026-04-04.
 - [146] L. N. Pradeep and Aniruddha Bhattacharjya. Random Key and Key Dependent S-box Generation for AES Cipher to Overcome Known Attacks. In *Security in Computing and Communications*, pages 63–69, Berlin, Heidelberg, 2013. Springer Berlin Heidelberg. ISBN 978-3-642-40576-1. doi: 10.1007/978-3-642-40576-1_7.
 - [147] Tom M. Ragonneau. *Model-Based Derivative-Free Optimization Methods and Software*. PhD thesis, Department of Applied Mathematics, The Hong Kong Polytechnic University, Hong Kong, China, 2022. URL <https://theses.lib.polyu.edu.hk/handle/200/12294>.
 - [148] Tom M. Ragonneau and Zhang Zaikun. COBYQA Version 1.1.2, 2024. URL <https://www.cobyqa.com>.

- [149] Ravishankar Ramanathan, Fernando G. S. L. Brandão, Karol Horodecki, Michał Horodecki, Paweł Horodecki, and Hanna Wojewódka. Randomness Amplification under Minimal Fundamental Assumptions on the Devices. *Physical Review Letters*, 117(23):230501, Dec 2016. doi: 10.1103/PhysRevLett.117.230501.
- [150] Min Ren, E Wu, Yan Liang, Yi Jian, Guang Wu, and Heping Zeng. Quantum random-number generator based on a photon-number-resolving detector. *Physical Review A*, 83:023820, February 2011. doi: 10.1103/PhysRevA.83.023820.
- [151] Alfréd Rényi. On Measures of Entropy and Information. In *Proceedings of the Fourth Berkeley Symposium on Mathematical Statistics and Probability, Volume 1: Contributions to the Theory of Statistics*, pages 547–561, Berkeley, 1961. University of California Press.
- [152] Ronald L Rivest, Adi Shamir, and Leonard Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21(2):120–126, 1978.
- [153] Miklos Santha and Umesh V. Vazirani. Generating quasi-random sequences from semi-random sources. *Journal of Computer and System Sciences*, 33(1):75–87, 1986. ISSN 0022-0000. doi: 10.1016/0022-0000(86)90044-9.
- [154] Valerio Scarani, Helle Bechmann-Pasquinucci, Nicolas J. Cerf, Miloslav Dušek, Norbert Lütkenhaus, and Momtchil Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3):1301–1350, September 2009. ISSN 1539-0756. doi: 10.1103/revmodphys.81.1301.
- [155] Maximilian Schlosshauer. Decoherence, the measurement problem, and interpretations of quantum mechanics. *Reviews of Modern Physics*, 76(4):1267–1305, February 2005. doi: 10.1103/revmodphys.76.1267.
- [156] Maximilian Schlosshauer. *Decoherence: and the Quantum-To-Classical Transition*. The Frontiers Collection. 2007. ISBN 978-3-540-35773-5. doi: 10.1007/978-3-540-35775-9.
- [157] Seth D. Schoen. Understanding Common Factor Attacks: An RSA-Cracking Puzzle, 30 April 2012. URL <http://www.loyalty.org/~schoen/rsa/>.
- [158] Michael Seevinck and George Svetlichny. Bell-Type Inequalities for Partial Separability in N-Particle Systems and Quantum Mechanical Violations. *Physical Review Letters*, 89(6), July 2002. ISSN 1079-7114. doi: 10.1103/physrevlett.89.060401.

- [159] Lynden K. Shalm, Yanbao Zhang, Joshua C. Bienfang, Collin Schlager, Martin J. Stevens, Michael D. Mařurek, Carlos Abellán, Waldimar Amaya, Morgan W. Mitchell, Mohammad A. Alhejji, Honghao Fu, Joel Ornstein, Richard P. Mirin, Sae Woo Nam, and Emanuel Knill. Device-independent randomness expansion with entangled photons. *Nature Physics*, 17(4):452–456, April 2021. doi: 10.1038/s41567-020-01153-4.
- [160] Claude E. Shannon. A Mathematical Theory of Communication. *The Bell System Technical Journal*, 27:379–423, 1948. doi: 10.1002/j.1538-7305.1948.tb01338.x.
- [161] Claude E. Shannon. Communication Theory of Secrecy Systems. *The Bell System Technical Journal*, 28(4):656–715, 1949. doi: 10.1002/j.1538-7305.1949.tb00928.x.
- [162] Shinya Murai Akira Murakami Hiroki Yamamuro Yuta Wakayama Shohei Beppu, Daniel J. Elson. Coexistence Transmission of 33.4-Tb/s O-band Coherent Classical Channels and a C-band QKD Channel over 80 km. In *Proceedings of 2025 Optical Fiber Communications Conference and Exhibition*, Tu3D. Optica Publishing Group, April 2025.
- [163] Peter W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer. *SIAM Journal on Computing*, 26(5):1484–1509, October 1997. ISSN 1095-7111. doi: 10.1137/s0097539795293172.
- [164] Peter W. Shor and John Preskill. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Physical Review Letters*, 85(2): 441–444, July 2000. ISSN 1079-7114. doi: 10.1103/physrevlett.85.441.
- [165] Maciej Skorski. How Much Randomness Can Be Extracted from Memoryless Shannon Entropy Sources? In *Information Security Applications*, pages 75–86. Springer International Publishing, 2016. ISBN 978-3-319-31875-2. doi: 10.1007/978-3-319-31875-2_7.
- [166] François-Xavier Standaert. Introduction to side-channel attacks. *Secure integrated circuits and systems*, pages 27–42, 2010. doi: 10.1007/978-0-387-71829-3_2.
- [167] Andrew Steane. Quantum computing. *Reports on Progress in Physics*, 61(2):117–173, February 1998. ISSN 1361-6633. doi: 10.1088/0034-4885/61/2/002.
- [168] Stockholm University. Nordic QCI: cybersecurity in the quantum era. su.se, January 2026. Department of Physics News. Accessed: 2026-04-04.

- [169] Alexander Streltsov. Quantum Correlations Beyond Entanglement: and Their Role in Quantum Information Theory, 2015.
- [170] Alexander Streltsov, Hermann Kampermann, and Dagmar Bruß. Quantum Cost for Sending Entanglement. *Physical Review Letters*, 108:250501, 2012.
- [171] Alexander Streltsov and Wojciech H. Żurek. Quantum Discord Cannot Be Shared. *Physical Review Letters*, 111:040401, 2013.
- [172] Weixiao Sun, Fuchuan Wei, Yuguo Shao, and Zhaohui Wei. Sudden death of quantum advantage in correlation generations. *Science Advances*, 10(47):eadr5002, 2024. doi: 10.1126/sciadv.adr5002.
- [173] Berk Sunar. True Random Number Generators for Cryptography. In *Cryptographic Engineering*, chapter 4, pages 55–73. Springer US, Boston, MA, 2009. ISBN 978-0-387-71817-0. doi: 10.1007/978-0-387-71817-0_4.
- [174] Ivan Šupić and Joseph Bowles. Self-testing of quantum systems: a review. *Quantum*, 4:337, September 2020. ISSN 2521-327X. doi: 10.22331/q-2020-09-30-337.
- [175] Hidema Tanaka. Information leakage via electromagnetic emanations and evaluation of tempest countermeasures. In *Information Systems Security: Third International Conference, ICISS 2007, Delhi, India, December 16-20, 2007. Proceedings 3*, pages 167–179. Springer, 2007. doi: 10.1007/978-3-540-77086-2_13.
- [176] The Quantum Insider. LuxQuanta launches second-generation NOVA LQ quantum key distribution system. thequantuminsider.com, 2025. Accessed: 2026-04-04.
- [177] Toshiba Digital Solutions Corporation. World’s first successful demonstration of quantum key distribution technology for multiplexing over 30 Tbps of high-capacity data and secret keys. global.toshiba, 2025. Accessed: 2026-04-04.
- [178] Akram Touil, Bin Yan, Davide Girolami, Sebastian Deffner, and Wojciech H. Żurek. Eavesdropping on the decohering environment: Quantum Darwinism, amplification, and the origin of objective classical reality. *Physical Review Letters*, 128(1):010401, 2022. doi: 10.1103/PhysRevLett.128.010401.
- [179] Jos Uffink. Quadratic Bell Inequalities as Tests for Multipartite Entanglement. *Physical Review Letters*, 88:230406, May 2002. doi: 10.1103/PhysRevLett.88.230406.
- [180] Ikram Ullah, Naveed Ahmed Azam, and Umar Hayat. Efficient and secure substitution box and random number generators over Mordell

- elliptic curves. *Journal of Information Security and Applications*, 56: 102619, 2021. ISSN 2214-2126. doi: 10.1016/j.jisa.2020.102619.
- [181] Mark Um, Xiang Zhang, Junhua Zhang, Ye Wang, Shen Yangchao, D.-L. Deng, Lu-Ming Duan, and Kihwan Kim. Experimental Certification of Random Numbers via Quantum Contextuality. *Scientific Reports*, 3(1):1627, April 2013. doi: 10.1038/srep01627.
- [182] Giuseppe Vallone, Davide G. Marangon, Marco Tomasin, and Paolo Villoresi. Quantum randomness certified by the uncertainty principle. *Physical Review A*, 90:052327, November 2014. doi: 10.1103/PhysRevA.90.052327.
- [183] Wim van Eck. Electromagnetic radiation from video display units: An eavesdropping risk? *Computers & Security*, 4(4):269–286, 1985. ISSN 0167-4048. doi: 10.1016/0167-4048(85)90046-X.
- [184] Lieven Vandenbergh and Stephen Boyd. Semidefinite programming. *SIAM review*, 38(1):49–95, 1996.
- [185] Ilpo Vattulainen, Kari Kankaala, Jukka Saarinen, and Tapio Alaniissilä. A comparative study of some pseudorandom number generators. *Computer Physics Communications*, 86(3):209–226, May 1995. doi: 10.1016/0010-4655(95)00015-8.
- [186] T. Vértesi. More efficient Bell inequalities for Werner states. *Physical Review A*, 78:032112, September 2008. doi: 10.1103/PhysRevA.78.032112.
- [187] David J. Wales and Jonathan P. K. Doye. Global Optimization by Basin-Hopping and the Lowest Energy Structures of Lennard-Jones Clusters Containing up to 110 Atoms. *The Journal of Physical Chemistry A*, 101(28):5111–5116, July 1997. ISSN 1520-5215. doi: 10.1021/jp970984n.
- [188] Chao Wang, Ignatius William Primaatmaja, Hong Jie Ng, Jing Yan Haw, Raymond Ho, Jianran Zhang, Gong Zhang, and Charles Lim. Provably-secure quantum randomness expansion with uncharacterised homodyne detection. *Nature Communications*, 14(1), January 2023. ISSN 2041-1723. doi: 10.1038/s41467-022-35556-z.
- [189] H. Wang. Quantum discord and classical correlation in two coupled double quantum dots system. *Applied Physics A*, 131(8), 2025. doi: 10.1007/s00339-025-08787-2. [7].
- [190] Wei Wei and Hong Guo. Bias-free true random-number generator. *Optics Letters*, 34(12):1876–1878, June 2009. doi: 10.1364/OL.34.001876.
- [191] Eugene P Wigner. The problem of measurement. *American Journal*

- of Physics*, 31(1):6–15, 1963. doi: 10.1119/1.1969254.
- [192] Peter Wittek. Algorithm 950: Ncpol2sdpa—sparse semidefinite programming relaxations for polynomial optimization problems of non-commuting variables. *ACM Transactions on Mathematical Software*, 41(3):1–12, June 2015. doi: 10.1145/2699464.
- [193] Erik Woodhead, Boris Bourdoncle, and Antonio Acín. Randomness versus nonlocality in the Mermin-Bell experiment with three parties. *Quantum*, 2:82, August 2018. ISSN 2521-327X. doi: 10.22331/q-2018-08-17-82.
- [194] Lewis Woollorton, Peter Brown, and Roger Colbeck. Tight Analytic Bound on the Trade-Off between Device-Independent Randomness and Nonlocality. *Physical Review Letters*, 129:150403, October 2022. doi: 10.1103/PhysRevLett.129.150403.
- [195] Guilherme B. Xavier, Thiago Ferreira da Silva, Giancarlo Vilela de Faria, Guilherme Penello Temporão, and Jean Pierre von der Weid. Practical random number generation protocol for entanglement-based quantum key distribution. *Quantum Information & Computation*, 9(7):683–692, July 2009. ISSN 1533-7146.
- [196] Feihu Xu, Jeffrey H. Shapiro, and Franco N. C. Wong. Experimental fast quantum random number generation using high-dimensional entanglement with entropy monitoring. *Optica*, 3(11):1266–1269, November 2016. doi: 10.1364/OPTICA.3.001266.
- [197] Wang Yiding, Huang Xiaofen, and Zhang Tinggui. Note on quantum discord, 2024. arXiv: 2408.05876.
- [198] Ting Yu and J. H. Eberly. Sudden Death of Entanglement. *Science*, 323(5914):598–601, 2009. doi: 10.1126/science.1167343.
- [199] Gong Zhang, Ignatius William Primaatmaja, Yue Chen, Si Qi Ng, Hong Jie Ng, Marco Pistoia, Xiao Gong, Koon Tong Goh, Chao Wang, and Charles Lim. Self-testing quantum randomness expansion on an integrated photonic chip, 2024.
- [200] Wojciech H. Żurek. Pointer basis of quantum apparatus: Into what mixture does the wave packet collapse? *Physical Review D*, 24:1516–1525, September 1981. doi: 10.1103/PhysRevD.24.1516.
- [201] Wojciech H. Żurek. Environment-induced superselection rules. *Physical Review D*, 26:1862–1880, October 1982. doi: 10.1103/PhysRevD.26.1862.
- [202] Wojciech H Żurek. Decoherence, einselection and the existential interpretation (the rough guide). *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering*

- Sciences*, 356(1743):1793–1821, 1998. doi: 10.1098/rsta.1998.0250.
- [203] Wojciech H. Żurek. Einselection and decoherence from an information theory perspective. *Annalen der Physik*, 512(11-12):855–864, 2000. doi: 10.1002/andp.200051211-1204.
 - [204] Wojciech H. Żurek. Decoherence, einselection, and the quantum origins of the classical. *Reviews of Modern Physics*, 75(3):715, 2003. doi: 10.1103/RevModPhys.75.715.
 - [205] Wojciech H. Żurek. Quantum Darwinism and envariance. In John D. Barrow, Paul C. W. Davies, and Charles L. Harper, Jr, editors, *Science and Ultimate Reality: Science and Ultimate Reality: Quantum Theory, Cosmology, and Complexity*, pages 121–137. Cambridge University Press, 2004. doi: 10.1017/CBO9780511814990.010.
 - [206] Wojciech H. Żurek. Quantum darwinism. *Nature Physics*, 5(3):181–188, March 2009. doi: 10.1038/nphys1202.
 - [207] Michael Zwolak, Haitao Quan, and Wojciech H. Żurek. Quantum Darwinism in a mixed environment. *Physical Review Letters*, 103(11):110402, 2009. doi: 10.1103/PhysRevLett.103.110402.
 - [208] Michael Zwolak, Haitao Quan, and Wojciech H. Żurek. Redundant imprinting of information in nonideal environments: Objective reality via a noisy channel. *Physical Review A*, 81(6):062110, 2010. doi: 10.1103/PhysRevA.81.062110.
 - [209] W. H. Żurek. Quantum discord and maxwell’s demons. *Physical Review A*, 67(1):012320, 2003. [4].
 - [210] Wojciech H. Żurek. Reduction of the wavepacket: How long does it take? In *Frontiers of nonequilibrium statistical physics*, pages 145–149. Springer, Boston, MA, 1986. ISBN 978-1-4613-2182-8. doi: 10.1007/978-1-4613-2181-1_10.

List of Figures

- 1.1 The nested hierarchy of bipartite correlation sets. The inner polytope represents the set of local correlations ($\mathcal{L}$), bounded by linear Bell inequalities. The intermediate convex set with curved boundaries denotes the set of quantum correlations ($\mathcal{Q}$), which exceeds the local bound up to the Tsirelson's bound. Both are contained within the no-signaling polytope ($\mathcal{N}$). 24

- 3.1 The Information Plateau in Quantum Darwinism. For pointer states, mutual information $I(\mathcal{S} : \mathcal{E}_f)$ quickly reaches the system's entropy $H_{\mathcal{S}}$, creating a plateau where additional environment fragments provide no new information. The superposition curve lacks a redundancy plateau, as information about non-selected states is not proliferated throughout the environment and can only be recovered by measuring nearly the entire global state. 56

- 4.1 The dependence of the average decoherence factor Γ for the interaction $U^{(\mathcal{A}\mathcal{E}_1)}$ given the size of the first environmental layer $\mathcal{E}_1$. The average is calculated over the cases rejected in BB84, for different interaction degree values (ε). Only the first decoherence interaction, between the apparatus and the first layer of the environment, is taken into consideration, as this is where the collapse of the state of the apparatus occurs. 67

- 4.2 Guessing probability of a key bit for different values of ε degree of interaction (4.10) between apparatus and the environment for a single-layer environment (4.6). The eavesdropper fully controls the last (and only) layer of the environment. . 69

5.1	Brief description of proposed randomness certification method using Shannon entropy.	79
5.2	Shannon entropy-based min-entropy sequence lower bounds based on (5.15), per event in the sequence, compared to the min-entropy for a single event. Three statistical distance bounds ϵ have been analyzed: (a) $\epsilon = 10^{-8}$; (b) $\epsilon = 10^{-12}$; (c) $\epsilon = 10^{-16}$. In (a), for $k \approx 30k$ (and $k \approx 45k$ in (b), and $k \approx 62.5k$ for (c)), this lower bound (divided per event) exceeds the maximal single-event min-entropy value for CHSH.	80
5.3	Lower bounds on Shannon entropy for randomness certification provided by CHSH inequality, as well as (5.17), as a function of the level of noise.	83
5.4	Lower bounds on Shannon entropy for randomness certification provided by the family of Braunstein-Caves inequalities, as a function of the level of noise.	84
5.5	Lower bounds of Shannon entropy for randomness certification provided by the I_1 and I_2 inequalities, as a function of the level of noise.	85
5.6	Lower bounds of Shannon entropy for randomness certification provided by the I_δ (with decreasing values of δ) inequalities, as a function of the level of noise.	86
5.7	Lower bounds on Shannon entropy for different Bell inequalities used for randomness certification, as a function of noise.	87
5.8	Shannon and min-entropy lower bounds for CHSH for different levels of noise, based on (5.25) and (5.26).	90
5.9	Shannon and min-entropy lower bounds for CHSH for different Mermin values $2 \leq \mathfrak{B}_M \leq 4$, based on (5.27).	91
5.10	BC_3 function calculated based on Observation 5.2.1 compared with its first and second derivative (as described in Appendix B).	92
5.11	Lower bounds on Shannon entropy for modified CHSH Bell inequality with and without additional constraints.	94
5.12	Shannon certification of randomness using the Bell inequality proposed in [88], for $d = 3$ Werner state, quantum bound $ \mathfrak{B} _Q = 1.718233$, settings $(x = 4, y = 2)$ and $(x = 3, y = 2)$ for comparison.	95

5.13	A distribution of the Bell certificates, as defined by (5.8). The certificates are classified based on the value of the measure of randomness (Shannon entropy) that the certificate yields. The histograms are presented for the white noise value $p = 1e-6$, for both Shannon and min-entropy.	98
5.14	Difference between the Shannon entropy values obtained from (5.27) and those derived from nonlinear optimization, illustrating the overestimation of entropy by (5.27) at higher noise levels.	100
5.15	Certification of randomness using the Bell inequalities defined in Table 5.2, for two measures of randomness. The measure is Shannon entropy based on (5.27).	100
5.16	Certification of randomness using the Bell inequalities defined in Table 5.2, for two measures of randomness. The measure is Shannon entropy. The values are obtained using the standard certification approach, which relies on the nonlinear optimization, constrained by the NPA-obtained bounds, as opposed to (5.27).	101
5.17	Certification of randomness using the Bell inequalities defined in Table 5.2, for two measures of randomness. The measure is min-entropy. The values are obtained using the standard certification approach, which relies on the nonlinear optimization, constrained by the NPA-obtained bounds, as opposed to (5.27).	102
6.1	Lower bounds on quantum discord for CHSH inequality, as well as (5.17), as a function of the fraction $\bar{p}$ of the quantum bounds $ \mathfrak{B}_{CHSH} _{\mathcal{Q}}$ or $ \mathfrak{B}_{Mod} _{\mathcal{Q}}$, respectively.	110
6.2	Lower bounds on quantum discord for the family of Braunstein-Caves inequalities, as a function of the fraction $\bar{p}$ of the quantum bounds $ \mathfrak{B}_{BC_n} _{\mathcal{Q}}$	111
6.3	Lower bounds on quantum discord for the I_1 and I_2 inequalities, a function of the fraction $\bar{p}$ of the quantum bounds $ \mathfrak{B}_{I_1} _{\mathcal{Q}}$ or $ \mathfrak{B}_{I_2} _{\mathcal{Q}}$, respectively.	111
6.4	The summary of discord optimization results for all analyzed Bell expressions, as a function of the fraction $\hat{p}$ of the quantum bound $ \mathfrak{B} _{\mathcal{Q}}$	112
6.5	Combination of the results of numerical experiments undertaken to minimize the discord function for the CHSH expression, as a function of the value of the expression (Bell value).	113

- 6.6 Combination of the results of numerical experiments undertaken to minimize the discord function for the I_1 expression, as a function of the value of the expression (Bell value). . . 114
- 6.7 Combination of the results of numerical experiments undertaken to minimize the discord function for the BC_5 expression, as a function of the value of the expression (Bell value). 114

List of Tables

4.1	Guessing probability of a key bit for an eavesdropper that uses Helstrom measurement on a controlled part of the environment's sole ($N_l = 1$) layer for $\varepsilon = 0$. It can be observed that the guessing probability is linearly proportional to the controlled part of the environment, counted as the percentage of dimension, and thus the control of the $N_{\mathcal{E}} - 1$ qubits leads to the guessing probability of around 75%.	68
4.2	Key bit guessing probability for $N_{\mathcal{E}} = 2$ and different values of ε degree of interaction between apparatus and the environment and different number of layers ($N_l = 1, 2, 3$).	69
5.1	Comparison between the Shannon entropy and min-entropy lower bounds for certain values of noise, for I_{δ} and J_{γ} protocols. The parameters are chosen to maximize the amount of key certified by these protocols ($\delta = \frac{\pi}{6}$ and $\gamma = 0.0$).	86
5.2	Protocols chosen for the further analysis, in the form of (5.8). All spot-settings equal $(x_0, y_0) = (0, 0)$	99
5.3	Comparison between different certificates presented in Table 5.2. Only two of the presented protocols show flex that equals exactly 1, i.e., when the box attaining Tsirelson's bound is unique.	103

Index

- asymmetric-key cryptography, 40
- basin-hopping, 77, 94, 109, 112
- BB84, 14, 15, 42–45, 59–61, 63, 66, 67, 70, 115, 116
- Bell expression, 21, 71, 74, 75, 81, 83, 101
- Bell inequality, 21, 44, 49, 72, 89, 101
- Bell operator, 20, 21, 74, 95, 96
- Boxes self-testing, 96, 101, 102
- Braunstein-Caves inequalities, 82, 109, 110
- CHSH, 21, 24, 25, 45, 49, 71, 72, 82, 87, 89, 94, 99, 108–110, 112, 113
- classical bound, 21, 22, 98, 110
- COBYQA, 33, 77, 109
- computational basis, 19, 42, 60, 62
- decoherence, 18, 43, 52–54, 57–60, 62, 66
- decoherence factor, 57, 66, 68, 69
- device-independence, 37, 39, 44, 48, 49, 72, 89, 96, 98, 115
- E91, 44
- einselection, 53, 54
- Hadamard basis, 19, 42, 60, 62
- information plateau, 69
- linear programming, 34
- local correlations, 23, 24
- min-entropy, 27–29, 38, 48, 49, 71, 76, 78, 80, 81, 84, 89, 90, 97–99, 117
- mutual information, 25–27, 30, 56, 63, 65
- mutually unbiased basis, 19, 43, 61, 66
- Naimark’s dilation theorem, 36
- non-linear programming, 31–33, 77, 82, 87, 93, 94, 107, 109, 110
- non-locality correlations, 24
- NPA hierarchy, 35–37, 75–77, 93, 97
- pointer state, 53–56, 58, 62, 68
- post-quantum cryptography, 41
- predictability sieve, 53–55
- QKD protocol, 14, 39, 42–45
- quantum correlations, 23, 24
- quantum Darwinism, 14, 51–55, 58, 59, 62, 115, 116, 118

- quantum discord, 29–31, 104,
105, 108–110, 112, 113,
115
- quantum key distribution, 13, 39,
42–44, 47, 59, 116, 118
- quantum RNG, 15, 47, 48, 71–73,
77, 81, 117

- random number generator, 15,
28, 46, 47, 71
- randomness amplification, 39, 48
- randomness certification, 49, 50,
71, 72, 74, 81, 94, 96–98
- randomness expansion, 39, 72
- randomness extraction, 39, 47,
48, 68, 73, 78, 81, 105,
117
- Rényi entropy, 29

- semi-device-independence, 45
- semidefinite programming, 31, 34,
35
- Shannon entropy, 25, 26, 28, 29,
71–73, 76–78, 80–85,
87–91, 93, 94, 96–99
- symmetric-key cryptography, 40

- Tsirelson’s bound, 21, 24, 25, 74,
75, 82–85, 92, 95, 97,
101, 102, 112

- Wooltorton-Brown-Colbeck
inequalities, 85

Appendices

A QR decomposition

The incorporation of the noise parameter between the subspaces in the form of $Q(\varepsilon, \alpha) = \varepsilon \cdot \mathbb{1}_2 + (1 - \varepsilon) \cdot C_X(\alpha)$ leads to a non-unitary matrix, which cannot be used as a quantum operator, therefore we need to decompose it into an orthonormal matrix, with the factor that was causing non-unitarity removed. One approach would be to use the singular value decomposition $M = U\Sigma V^\dagger$, where Σ represents the rectangular diagonal matrix with singular values on the diagonal, V and U form two sets of orthonormal bases. This decomposition for this matrix leads to an eigendecomposition that removes the noise factor ε , which makes the transformation useless.

The QR decomposition $Q = Q'R$ transforms the initial matrix into an orthonormal Q and an upper triangular matrix R . It can be calculated using the Gram–Schmidt process. We divide our matrix into columns $Q = [q_1|q_2]$:

$$q_1 = \begin{bmatrix} \varepsilon + (1 - \varepsilon) \sin(\alpha) \\ (1 - \varepsilon) \cos(\alpha) \end{bmatrix}, q_2 = \begin{bmatrix} (1 - \varepsilon) \cos(\alpha) \\ \varepsilon - (1 - \varepsilon) \sin(\alpha) \end{bmatrix}. \quad (10)$$

The norm from the vector $\|a_1\| = \sqrt{(\varepsilon + (1 - \varepsilon) \sin(\alpha))^2 + (1 - \varepsilon)^2 \cos(\alpha)^2}$. The first column of the matrix equals

$$u_1 = \frac{q_1}{\|q_1\|} = \begin{bmatrix} \frac{\varepsilon + (1 - \varepsilon) \sin(\alpha)}{\sqrt{(\varepsilon + (1 - \varepsilon) \sin(\alpha))^2 + (1 - \varepsilon)^2 \cos(\alpha)^2}} \\ \frac{(1 - \varepsilon) \cos(\alpha)}{\sqrt{(\varepsilon + (1 - \varepsilon) \sin(\alpha))^2 + (1 - \varepsilon)^2 \cos(\alpha)^2}} \end{bmatrix}. \quad (11)$$

The second vector is calculated similarly. First, we need need a projection of q_2 on u_1 : $\text{proj}_{u_1} q_2 = \frac{\langle u_1 | q_2 \rangle}{\langle u_1 | u_1 \rangle} u_1 = \begin{bmatrix} 2(1 - \varepsilon) \cos(\alpha) \\ -2(1 - \varepsilon) \sin(\alpha) \end{bmatrix}$. This value is used to calculate the intermediate vector $q'_2 = q_2 - \text{proj}_{u_1} q_2 = \begin{bmatrix} -(1 - \varepsilon) \cos(\alpha) \\ \varepsilon + (1 - \varepsilon) \sin(\alpha) \end{bmatrix}$.

Analogously:

$$u_2 = \frac{q_2}{\|q_2\|} = \left[\frac{\frac{-(1-\varepsilon) \cos(\alpha)}{\sqrt{(\varepsilon+(1-\varepsilon) \sin(\alpha))^2 + (1-\varepsilon)^2 \cos(\alpha)^2}}}{\frac{\varepsilon+(1-\varepsilon) \sin(\alpha)}{\sqrt{(\varepsilon+(1-\varepsilon) \sin(\alpha))^2 + (1-\varepsilon)^2 \cos(\alpha)^2}}} \right]. \quad (12)$$

This leads to the final forms of Q' :

$$Q'(\varepsilon, \alpha) = \begin{bmatrix} u_1 & u_2 \end{bmatrix} = \begin{bmatrix} \frac{\varepsilon+(1-\varepsilon) \sin(\alpha)}{\sqrt{(\varepsilon+(1-\varepsilon) \sin(\alpha))^2 + (1-\varepsilon)^2 \cos(\alpha)^2}} & \frac{-(1-\varepsilon) \cos(\alpha)}{\sqrt{(\varepsilon+(1-\varepsilon) \sin(\alpha))^2 + (1-\varepsilon)^2 \cos(\alpha)^2}} \\ \frac{(1-\varepsilon) \cos(\alpha)}{\sqrt{(\varepsilon+(1-\varepsilon) \sin(\alpha))^2 + (1-\varepsilon)^2 \cos(\alpha)^2}} & \frac{\varepsilon+(1-\varepsilon) \sin(\alpha)}{\sqrt{(\varepsilon+(1-\varepsilon) \sin(\alpha))^2 + (1-\varepsilon)^2 \cos(\alpha)^2}} \end{bmatrix}. \quad (13)$$

B Second-degree derivation for Shannon entropy

For the analysis of the convexity of the Shannon entropy, we had to verify the form of its second-order derivative, concerning functions for lower and upper bounds used by the Conjecture 5.2.1. As these functions are dependent on the variable p , we needed to calculate the derivative of a composite function:

$$H(l_{-1,-1}(p), l_{-1,1}(p), u_{1,-1}(p)) = H(p), \quad (14)$$

where H is the Shannon entropy function, $l_{-1,-1}$ is the lower bound for the probability of receiving a result ($a = -1, b = -1$), $l_{-1,1}$ is the lower bound for the probability of receiving a result ($a = -1, b = 1$) and $u_{1,-1}$ is the upper bound for the probability of receiving a result ($a = 1, b = -1$), as in the Conjecture 5.2.1.

Based on the chain rule for differentials:

$$\begin{aligned} \frac{\partial H}{\partial p} \Big|_{l_{-1,-1}, l_{-1,1}, u_{1,-1}} &= \frac{\partial H}{\partial l_{-1,-1}} \Big|_{l_{-1,1}, u_{1,-1}} \frac{dl_{-1,-1}}{dp} + \\ \frac{\partial H}{\partial l_{-1,1}} \Big|_{l_{-1,-1}, u_{1,-1}} \frac{dl_{-1,1}}{dp} &+ \frac{\partial H}{\partial u_{1,-1}} \Big|_{l_{-1,-1}, l_{-1,1}} \frac{du_{1,-1}}{dp}. \end{aligned} \quad (15)$$

The values of $\frac{dl_{-1,-1}}{dp}$, $\frac{dl_{-1,1}}{dp}$ and $\frac{du_{1,-1}}{dp}$ were obtained using central differences method, as these have to be based on the results of the NPA optimization. The Shannon entropy formula is based on Observation 5.2.1:

$$\begin{aligned} H &= -l_{-1,-1} \log_2(l_{-1,-1}) - l_{-1,1} \log_2(l_{-1,1}) - u_{1,-1} \log_2(u_{1,-1}) \\ &- (1 - l_{-1,-1} - l_{-1,1} - u_{1,-1}) \log_2(1 - l_{-1,-1} - l_{-1,1} - u_{1,-1}). \end{aligned} \quad (16)$$

Thus, partial derivatives with respect to lower and upper bounds equal:

$$\begin{aligned}
\left. \frac{\partial H}{\partial l_{-1,-1}} \right|_{l_{-1,1}, u_{1,-1}} &= \log_2 \left(\frac{1 - l_{-1,-1} - l_{-1,1} - u_{1,-1}}{l_{-1,-1}} \right), \\
\left. \frac{\partial H}{\partial l_{-1,1}} \right|_{l_{-1,-1}, u_{1,-1}} &= \log_2 \left(\frac{1 - l_{-1,-1} - l_{-1,1} - u_{1,-1}}{l_{-1,1}} \right), \\
\left. \frac{\partial H}{\partial u_{1,-1}} \right|_{l_{-1,-1}, l_{-1,1}} &= \log_2 \left(\frac{1 - l_{-1,-1} - l_{-1,1} - u_{1,-1}}{u_{1,-1}} \right).
\end{aligned} \tag{17}$$

The second derivative is now simply a sum of derivatives of the components of the first derivative. In other words:

$$\frac{\partial^2 H}{\partial p^2} = \frac{\partial}{\partial p} \left(\frac{\partial H}{\partial l_{-1,-1}} \frac{dl_{-1,-1}}{dp} \right) + \frac{\partial}{\partial p} \left(\frac{\partial H}{\partial l_{-1,1}} \frac{dl_{-1,1}}{dp} \right) + \frac{\partial}{\partial p} \left(\frac{\partial H}{\partial u_{1,-1}} \frac{du_{1,-1}}{dp} \right). \tag{18}$$

A single component equals:

$$\begin{aligned}
\frac{\partial}{\partial p} \left(\frac{\partial H}{\partial l_{-1,-1}} \frac{dl_{-1,-1}}{dp} \right) &= \frac{d^2 l_{-1,-1}}{dp^2} \frac{\partial H}{\partial l_{-1,-1}} + \left(\frac{dl_{-1,-1}}{dp} \right)^2 \frac{\partial^2 H}{\partial l_{-1,-1}^2} \\
&+ \frac{dl_{-1,-1}}{dp} \left(\frac{dl_{-1,1}}{dp} \frac{\partial^2 H}{\partial l_{-1,1} \partial l_{-1,-1}} + \frac{du_{1,-1}}{dp} \frac{\partial^2 H}{\partial u_{1,-1} \partial l_{-1,-1}} \right).
\end{aligned} \tag{19}$$

Once again, $\frac{dl_{-1,-1}}{dp}$, $\frac{dl_{-1,1}}{dp}$ and $\frac{du_{1,-1}}{dp}$ (as well as $\frac{d^2 l_{-1,-1}}{dp^2}$) were obtained using central differences. The other subcomponents equal:

$$\begin{aligned}
\frac{\partial^2 H}{\partial l_{-1,-1}^2} &= -\frac{1}{\ln 2} \left(\frac{1 - l_{-1,1} - u_{1,-1}}{1 - l_{-1,-1}^2 - l_{-1,1} - u_{1,-1}} \right), \\
\frac{\partial^2 H}{\partial l_{-1,1} \partial l_{-1,-1}} &= \frac{\partial^2 H}{\partial u_{1,-1} \partial l_{-1,-1}} = -\frac{1}{\ln 2} \left(\frac{1}{1 - l_{-1,-1} - l_{-1,1} - u_{1,-1}} \right).
\end{aligned} \tag{20}$$

Additionally, we denote:

$$\begin{aligned}
\alpha &= \frac{1}{1 - l_{-1,-1} - l_{-1,1} - u_{1,-1}}, \\
\beta_1 &= \frac{1 - l_{-1,1} - u_{1,-1}}{1 - l_{-1,-1}^2 - l_{-1,1} - u_{1,-1}}, \\
\beta_2 &= \frac{1 - l_{-1,-1} - u_{1,-1}}{1 - l_{-1,-1} - l_{-1,1}^2 - u_{1,-1}}, \\
\beta_3 &= \frac{1 - l_{-1,-1} - l_{-1,1}}{1 - l_{-1,-1} - l_{-1,1} - u_{1,-1}^2}.
\end{aligned} \tag{21}$$

The previous subcomponents are thus reduced to

$$\frac{\partial^2 H}{\partial l_{-1,-1}^2} = -\frac{\beta_1}{\ln 2}, \quad \frac{\partial^2 H}{\partial l_{-1,1} \partial l_{-1,-1}} = \frac{\partial^2 S}{\partial u_{1,-1} \partial l_{-1,-1}} = -\frac{\alpha}{\ln 2}. \quad (22)$$

The full component can therefore be reduced to

$$\begin{aligned} \frac{\partial}{\partial p} \left(\frac{\partial H}{\partial l_{-1,-1}} \frac{dl_{-1,-1}}{dp} \right) &= \frac{d^2 l_{-1,-1}}{dp^2} \log_2 \frac{1}{\alpha l_{-1,-1}} - \\ \frac{1}{\ln 2} \left(\beta_1 \left(\frac{dl_{-1,-1}}{dp} \right)^2 + \alpha \frac{dl_{-1,-1}}{dp} \left(\frac{dl_{-1,1}}{dp} + \frac{du_{1,-1}}{dp} \right) \right). \end{aligned} \quad (23)$$

We transform the remaining components of (18), which leads to (5.28).