Operational approaches to quantum resources in communication and security

A thesis submitted by

TUSHITA PRASAD

for the title of Doctor of Philosophy (PhD)
Supervisor: Dr. hab. Marcin Pawłowski, prof. UG

Faculty of Mathematics, Physics and Informatics
University of Gdańsk

2026

Acknowledgements

This thesis is the culmination of a four-year journey marked by the joys of discovery, moments of frustration, and the many long coffee breaks that sparked some of the most enlightening discussions. Along the way, I have been fortunate to meet and learn from many wonderful people who have shaped not only this work but also the person I have become.

First and foremost, I would like to express my gratitude to my supervisor, Marcin Pawłowski. I am grateful for the freedom he provided throughout my PhD, which challenged me to find my own path and shaped me into an independent researcher. I am equally grateful to Markus Grassl, for his invaluable guidance and patience. His meticulous attention to detail and rigorous feedback significantly improved the quality of my scientific work.

I am deeply thankful to the postdoctoral researchers from whom I have learned so much. In particular, I would like to thank Anubhav, Shubhayan, Some, Lucas, Pedro, Ankit, and Tanmoy for the many insightful discussions and intellectual exchanges. I am especially grateful to Lucas and Shubhayan for their careful reading of this thesis and for their detailed and constructive feedback.

My heartfelt thanks go to my close friends in Gdańsk – Chithra, Lucas and Ankit who have been a constant source of support and joy beyond work. I am certain these friendships will last a lifetime.

I would also like to thank my friends and colleagues from ICTQT and UG – Anuradha, Ekta, Sumit, Divyansh, Baldi, Chirag, Paweł, Marco, Shahana, Rishav, Vinicius, Amra, Mathias, Naveen, Aravind, Abhyoudai and Beata for the many moments shared both inside and outside the institute. A special thanks to Paweł for his help with the Polish abstract.

I am grateful to Andreas, John, Bel, and Karol for their guidance and support over the years. I would also like to sincerely thank Ewa, Gosia, and Marta for their administrative support, navigating bureaucracy without their help would have been impossible.

To my best friends – BC, Smruthi, Ashwin, and Mamu. Thank you for the constancy, for all the love and laughter, and for being the support system that kept me going. Finally, I would like to thank my family, my strongest pillars of support. My sister, Puttu, for her presence and strength. To my husband, Abhi, thank you for your constant encouragement, and for teaching me how to face setbacks with grace. To my parents, Radha and Prasad, thank you for always believing in me, and for giving me every opportunity to pursue my dreams. My father, for always motivating me to aim higher, and my mother, for nurturing in me a love for physics and mathematics from a very young age, this would not have been possible without you.

Lastly, the research presented in this thesis was supported at different stages by several funding sources: National Science Centre, Poland (OPUS 25, grant no. UMO-2023/49/B/ST2/02468); Foundation for Polish Science (IRAP project, ICTQT, contract no. MAB/2018/5, co-financed by the European Union under the Smart Growth Operational Programme); and the IRA Pro-

gramme (project no. FENG.02.01-IP.05-0006/23), financed by the FENG programme 2021–2027 (Priority FENG.02, Measure FENG.02.01) with support from the Foundation for Polish Science.

Dedication

॥ माता पिता गुरु दैवम् ॥

To Jaggi, Gundu and Prasadu

Abstract

Quantum information theory shows that fundamental features of quantum mechanics, such as entanglement and complementarity, can be used as resources for information processing. Understanding their operational significance requires going beyond their theoretical frameworks and analyzing how they can be used in concrete tasks, as well as identifying the conditions under which they provide an advantage or face limitations. This dissertation adopts such an operational perspective, focusing on realistic communication and cryptographic scenarios, and is based on three scientific articles.

In the first article, we study entanglement-assisted classical communication in finite regimes. We introduce an explicit coding scheme capable of correcting a fixed number of errors or erasures while accommodating a variable amount of shared entanglement. By reducing the problem to a classical framework, we identify optimal parameter regimes and demonstrate that adaptable entanglement usage provides a tangible communication advantage using experimentally accessible techniques.

In the second article, we explore the role of complementarity in quantum cryptography within the semi-device-independent framework. We establish a direct connection between wave-particle duality and security by expressing a semi-device-independent security witness in terms of interferometric quantities. This approach enables the certification of non-classicality and secure key generation using experimentally measurable parameters, and extends naturally to higher-dimensional systems.

Finally, we examine the limitations of entanglement as a resource for quantum key distribution. We show that entanglement alone is not sufficient to guarantee secure key extraction in realistic settings where even minimal classical side-channel leakage is present. By identifying classes of entangled states that are unusable for key generation under such conditions, we demonstrate a fundamental separation between entanglement and cryptographic usefulness, with implications for the scalability of quantum networks.

Together, these results provide a unified operational view on quantum resources, highlighting both their capabilities and their limitations in practical information-processing tasks.

Abstrakt

Teoria informacji kwantowej pokazuje, że fundamentalne własności mechaniki kwantowej, takie jak splątanie i komplementarność, mogą być wykorzystywane jako zasoby w przetwarzaniu informacji. Zrozumienie ich znaczenia operacyjnego wymaga wyjścia poza abstrakcyjne ramy teoretyczne w celu analizy sposobów ich wykorzystania w konkretnych zadaniach, a także określenia warunków, w których zapewniają one przewagę lub napotykają ograniczenia. Niniejsza rozprawa przyjmuje takie operacyjne podejście, koncentrując się na realistycznych scenariuszach komunikacyjnych i kryptograficznych, i opiera się na trzech artykułach naukowych.

W pierwszym artykule badamy klasyczną komunikację wspomaganą splątaniem w reżimie skończonym. Wprowadzamy jawny schemat kodowania zdolny do korekcji ustalonej liczby błędów lub wymazań, przy jednoczesnym uwzględnieniu zmiennej ilości współdzielonego splątania. Sprowadzając problem do ram klasycznych, identyfikujemy optymalne zakresy parametrów oraz pokazujemy, że adaptacyjne wykorzystanie splątania prowadzi do wymiernej przewagi komunikacyjnej przy użyciu technik dostępnych eksperymentalnie.

W drugim artykule analizujemy rolę komplementarności w kryptografii kwantowej w ramach podejścia pół-niezależnego od urządzeń. Ustalamy bezpośredni związek między dualizmem korpuskularno-falowym a bezpieczeństwem, wyrażając świadka bezpieczeństwa w tym schemacie w kategoriach wielkości interferometrycznych. Podejście to umożliwia certyfikację nieklasyczności oraz generowanie bezpiecznego klucza na podstawie wielkości mierzalnych eksperymentalnie, a także naturalnie uogólnia się na układy o wyższych wymiarach.

Wreszcie badamy ograniczenia splątania jako zasobu w dystrybucji klucza kwantowego. Pokazujemy, że samo splątanie nie jest wystarczające do zagwarantowania bezpiecznej ekstrakcji klucza w realistycznych warunkach, w których występuje nawet minimalny wyciek klasycznej informacji bocznej. Identyfikując klasy stanów splątanych, które w takich warunkach nie pozwalają na generowanie klucza, wykazujemy fundamentalne rozdzielenie między splątaniem a jego użytecznością kryptograficzną, co ma istotne konsekwencje dla skalowalności sieci kwantowych.

Łącznie wyniki te dostarczają spójnej operacyjnej perspektywy na zasoby kwantowe, podkreślając zarówno ich możliwości, jak i ograniczenia w praktycznych zadaniach przetwarzania informacji.

Manuscripts included in the dissertation

[1] Prasad, T. and Grassl, M., *Codes for entanglement-assisted classical communication*, npj Quantum Information **11** (2025).

[2] Raj, C., Prasad, T.[1], Chaturvedi, A., Pollyceno, L., Spegel-Lexne, D., Gómez, S., Argillander, J., Alarcón, A., Xavier, G. B., Pawłowski, M., and Dieguez, P. R., *Certifying semi-device-independent security via wave-particle duality experiments*, npj Quantum Information **12** (2025).

[3] Sarkar, S., Prasad, T., and Horodecki, K., *Entanglement is not sufficient for most practical entanglement-based QKD protocols*, arXiv:2603.06400 (2026).

[1] Co-first author.

Other manuscripts

[1] Yao, Y., Prasad, T., Grassl, M., Jafar, S., and Sun, H., *Space-sharing and Singleton bounds for entanglement-assisted classical coding*, arXiv:2603.08563 (2026).

[2] Viola, G., Panwar, E., Prasad, T., Saha, D., and Chaturvedi, A., *Operational nonclassicality and Semi Device-Independent Quantum Key Distribution from Bounded Success in Communication Tasks*, to appear on arXiv.

List of abbreviations

EA	Entanglement-assisted
EACC	Entanglement-assisted classical communication
WPD	Wave-particle duality
EURs	Entropic uncertainty relations
QKD	Quantum key distribution
SDI	Semi-device-independent
DI	Device-independent
DD	Device-dependent
MZI	Mach-Zehnder interferometer
OAM	Orbital angular momentum
WPDRs	Wave-particle duality relations
PM	Prepare-and-measure
EB	Entanglement-based
QRAC	Quantum random access code
TBS	Tunable beam splitter
MDI	Measurement device-independent
EAQECCs	Entanglement-assisted quantum error correcting codes
C.C.	Convex-combination

Table of Contents

List of Figures

Figure **Page**

Chapter 1

Introduction

The ability to communicate information reliably and securely is one of the defining challenges of modern science and technology. From global communication networks to secure financial systems, much of our infrastructure depends on understanding not only how information can be transmitted, but also what guarantees can be made about its integrity and privacy. Classical information theory, founded by Claude Shannon, provided a precise framework [77] for addressing these questions. It showed that noise in communication channels does not necessarily prevent reliable transmission, and that there exist fundamental limits in the form of channel capacities that determine what is achievable.

At the same time, cryptography developed along a different path. It built security on assumptions about computational difficulty. Protocols such as RSA [71] or Diffie-Hellman [31] are considered secure because they rely on specific mathematical problems such as factoring large integers or computing discrete logarithms that are believed to be hard to solve with any efficient algorithm. This approach has proven extremely successful in practice, yet it carries a certain vulnerability. The security of such protocols depends on these hardness assumptions remaining valid. If more efficient algorithms are discovered, or if new computational models, such as large-scale quantum computers become available, these problems may become easily solvable, and the security of the protocols would be compromised. In this sense, classical cryptography offers security that is conditional.

Quantum mechanics substantially reshapes this landscape. It introduces new constraints on how information can be encoded, transmitted, and measured, constraints that arise not from technological limitations, but from the very structure of physical laws. The impossibility of cloning an unknown quantum state [91] and the disturbance of a quantum system caused by measurement [87] are two prominent examples. At a first glance, these features might appear to limit our ability to process information. Yet, interestingly, they can also be turned into

advantages.

This shift, from viewing quantum phenomena as obstacles to treating them as resources lies at the core of quantum information science. Entanglement, once at the center of foundational debates [6, 34, 75], is now understood as an important ingredient in communication tasks that achieve advantages impossible in classical settings [10, 12, 13, 17]. Complementarity [15], which captures the incompatibility of certain measurements, provides a way of limiting the information accessible to an observer. These and other features of quantum theory are no longer seen as just conceptual oddities but as practical tools that can be used to perform real-world information-processing tasks.

However, identifying a quantum feature as a resource is only the starting point. To understand its actual significance, one must ask more detailed questions: How can the resource be used in practice? Under what conditions does it provide an advantage? And perhaps most importantly, what are its limitations? These questions naturally lead to an operational perspective, where the value of a resource is assessed through the tasks it makes possible, such as transmitting information over noisy channels or generating secret keys in the presence of an adversary.

Adopting this perspective also highlights a gap between theory and practice. Much of our current understanding of quantum resources is based on idealized, asymptotic scenarios, where one assumes access to infinitely many uses of a channel or perfectly controlled devices [21]. Realistic implementations, on the contrary, operate under finite resources, noise, and imperfect control. In these cases, the role of quantum resources can change significantly. Advantages predicted in the asymptotic limit may shrink, new trade-offs may arise, and even if imperfections existing previously were negligible, now they may amplify.

These considerations motivate the main theme of this thesis: to study quantum resources, specifically entanglement and complementarity from an operational perspective in realistic communication and cryptographic settings. The aim is to understand not only how these resources can be exploited, but also where their power reaches its limits.

A natural starting point is the role of entanglement in communication. Since the introduction of super-dense coding [13], it has been known that pre-shared entanglement can improve the transmission of classical information over quantum channels. More generally, entanglement-assisted (EA) communication has been extensively studied within information theory [7, 12, 27, 29, 30, 47, 76], leading to a detailed understanding of EA capacities and optimal rates in the asymptotic limit. Despite this progress, an important gap remains. Capacity theorems characterize ultimate limits but do not directly translate into explicit protocols suitable for realistic scenarios. In particular, while entanglement-assisted quantum error-correcting codes (EAQECCs) have been widely developed [17, 28, 37, 46, 63], there is a notable lack of explicit constructions tailored specifically for classical communication assisted by entanglement, especially in finite regimes where both the number of channel uses and the available entanglement are limited. Moreover, the interplay between these resources, how much entanglement is needed,

how it should be used, and how it affects error correction is not sufficiently understood in a constructive setting.

The first article in this thesis [68] attempts to address this gap. We develop an explicit coding scheme for entanglement-assisted classical communication (EACC) that operates in a finite regime and can correct a prescribed number of errors or erasures. Importantly, the scheme accommodates varying amounts of shared entanglement, revealing how entanglement can be treated as a tunable resource.

While entanglement enhances communication capabilities, quantum cryptography addresses a different operational role of quantum mechanics. It restricts the information that can be gained by an adversary. This restriction is deeply connected to the principle of complementarity [9, 24, 52, 90]. In interferometric settings, this is expressed through wave-particle duality (WPD) [36, 50], where the ability to obtain which-path information comes at the cost of reduced interference visibility. In recent years, this qualitative principle has been given a precise quantitative form through entropic uncertainty relations (EURs) [24], which directly bound an adversary's knowledge in cryptographic tasks. These developments have established complementarity as an important ingredient in security proofs [3, 52, 94], particularly in device-dependent (DD) and device-independent (DI) frameworks.

However, an important regime between these two extremes remains unexplored. Fully DI protocols provide strong security guarantees [1], but are challenging to implement in practice, whereas DD approaches rely on detailed assumptions about the inner workings of the devices. The semi-device-independent (SDI) framework [64] offers a more practical alternative, requiring only limited assumptions, such as an upper bound on the system dimension. Despite its relevance, the role of complementarity as an operational resource within the SDI framework is still not well understood.

The second article [70] of this thesis takes a step in this direction by connecting WPD experiments with security in the SDI setting. It shows that the relevant SDI security witness can be linked to simple interferometric quantities, making the connection between abstract security ideas and experimentally relevant quantities. This also clarifies the role of complementarity in this framework and extends the range of parameters for which secure communication is possible. These results in fact suggest that complementarity is not only a fundamental limitation but can also be used as a tool for certifying security in realistic scenarios.

The perspectives above suggest a unifying picture. Quantum resources such as entanglement and complementarity pave the way for new applications in communication and cryptography. This naturally leads to the fundamental question—are these resources always sufficient to guarantee reliable communication or secure key generation?

In the context of quantum key distribution (QKD), entanglement is widely considered as the essential resource underlying security [26, 35, 69, 93]. Many security proofs rely on the presence of entanglement in the shared quantum state, and it is known that entanglement is necessary

for key generation [11, 26, 42]. This has led to the common intuition that entanglement should also be sufficient.

The third article [73] of this thesis shows that this intuition does not hold in general. When moving beyond idealized models to include realistic imperfections, specifically, even arbitrarily small amounts of classical side-channel leakage, entanglement alone is no longer sufficient to guarantee secure key distribution in standard EB-QKD protocols. This result establishes a fundamental separation between entanglement and key extractability. It shows that the usefulness of a quantum resource depends not only on its presence, but also on the operational context in which it is used, including the flow of classical information.

Taken together, the results presented in this thesis provide an operational perspective on quantum resources in information processing. They show how entanglement can be used to enhance communication in finite regimes, how complementarity can be used to certify security in experimentally accessible ways, and how resources are subject to limitations in realistic settings.

The remainder of the thesis is organized as follows. Chapter 2 introduces the necessary preliminaries that form the basis for understanding the works presented in this thesis, including entanglement, complementarity, and their roles in the communication and cryptographic frameworks relevant to the problems studied in these articles. Chapter 3 provides a summary of the main results of the three articles comprising this dissertation. Lastly, Chapter 4 discusses future directions.

Chapter 2

Preliminaries

This chapter introduces the theoretical and operational tools relevant to our discussion. We focus on quantum resources and how they are used in information-processing tasks, particularly in communication and cryptography.

We begin by presenting the quantum resources pertinent to this thesis. We then examine how these resources can be used in communication scenarios, and finally study their role in secure communication protocols, with an emphasis on QKD and the limitations imposed by physical principles.

2.1 Quantum Resources for Information Processing

Quantum information processing exploits features of quantum mechanics that have no classical counterpart. These features, often referred to as quantum resources, enable tasks that are impossible or inefficient within classical information theory. Among the most important of these resources are quantum entanglement and complementarity, both of which play central roles in modern quantum communication and computation protocols.

In this section, we first examine entanglement, exploring its utility as a communication resource and its role in securing cryptographic protocols, focusing on entangled states relevant to the protocols studied in this work. We then turn to complementarity and WPD, developing an operational understanding in interferometric settings like the Mach-Zehnder interferometer (MZI). This includes defining and experimentally estimating path distinguishability and fringe visibility, analyzing their trade-offs through wave-particle duality relations (WPDRs), and ultimately framing complementarity as a quantifiable resource that constrains accessible information, providing fundamental security guarantees in cryptographic tasks.

2.1.1 Entanglement

Entanglement describes correlations between two or more quantum systems that cannot be explained classically or reproduced using shared randomness. When local measurements are performed on entangled systems, they can reveal correlations that persist even when the systems are spatially separated. This non-local nature of entanglement makes it a valuable resource that can be shared between distant parties and used in the context of communication and cryptography. We now express entanglement in mathematical terms. Consider a bipartite quantum system composed of two subsystems A and B associated with Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$. A pure state $|\psi\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$ is called entangled if it cannot be written as a product of local states of the form $|\alpha\rangle_A \otimes |\beta\rangle_B$. For mixed states described by a density operator ρ_{AB}, entanglement is defined through the concept of separability. A bipartite state is called separable if it can be written as a probabilistic mixture of product states,

$$\rho_{AB} = \sum_k q_k \, \rho_A^{(k)} \otimes \rho_B^{(k)}, \tag{2.1}$$

where the coefficients q_k satisfy $q_k \geq 0$ and $\sum_k q_k = 1$, and $\rho_A^{(k)}$ and $\rho_B^{(k)}$ are density operators that act on the subsystems A and B, respectively. If such a decomposition does not exist, the state ρ_{AB} is said to be entangled [45].

For pure bipartite states, entanglement can be characterized using the Schmidt decomposition [63]. In this representation, a state is entangled whenever its Schmidt rank is larger than one. For mixed states, the situation is more involved. A commonly used necessary condition for separability is the positivity of the partial transpose (PPT) criterion [44, 66], which provides a practical tool for detecting entanglement in many relevant cases.

Entanglement as a communication resource. Entanglement can be shared between different parties prior to the actual communication of information. This pre-shared entanglement can sometimes enhance communication over quantum channels, improving the transmission of both classical and quantum information in a way that has no classical analogue. In the absence of entanglement, sending a single qubit through a noiseless quantum channel allows the transmission of at most one classical bit of information. However, this limitation can be overcome using entanglement, as demonstrated by the protocol of super-dense coding [13]. In this scheme, a sender can transmit two classical bits of information by sending only a single qubit through a noiseless quantum channel, provided that the sender and receiver share a maximally entangled state beforehand. This result shows how entanglement can effectively increase the communication capacity of a quantum channel. Furthermore, for certain noisy quantum channels, it has been shown that the classical capacity can be significantly increased when the communicating parties have access to an unlimited supply of shared entanglement [12].

In the quantum domain, entanglement also enhances transmission of quantum information by enabling protocols such as teleportation [10]. In quantum teleportation, an unknown quantum state can be faithfully transferred from a sender to a receiver using pre-shared entanglement and the exchange of classical bits, without physically transmitting the system itself. This motivates the study of EA communication protocols, where entanglement is treated as a consumable resource that can be used to achieve improved rates or reliability in both classical and quantum settings. However, for the purposes of this thesis, we will focus on the role of entanglement in enhancing the transmission of classical information.

Entanglement in cryptographic protocols. Entanglement proves to be equally powerful in cryptographic settings. It enables protocols in which secret keys are generated from correlations between distant parties [35], and more generally supports scenarios where security can be certified directly from observed correlations, even with limited trust in the devices [1]. At a fundamental level, entanglement gives rise to non-classical correlations that restrict the information accessible to an external observer. This makes it particularly well-suited for cryptographic tasks, where the objective is not only to establish shared data but to ensure that it remains partially inaccessible to an adversary. In this sense, entanglement serves as a fundamental resource for secure communication, a role that will be explored in detail in later sections.

Entangled states relevant for cryptography. We now study a particular family of entangled states —*isotropic states*. They are widely used in the study of entanglement and quantum cryptography. An isotropic state [83] is a bipartite quantum state that is invariant under transformations of the form

$$\rho_v = (U \otimes U^*)\, \rho_v\, (U^\dagger \otimes U^T) \quad \text{for all unitary } U.$$

For two qubits, isotropic states take the form

$$\rho_v = v\, |\Phi^+\rangle\langle\Phi^+| + (1-v)\, \frac{\mathbb{I}}{4}, \tag{2.2}$$

where $v \in [0,1]$ is a mixing parameter, $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is a maximally entangled Bell state, and $\mathbb{I}$ is the identity operator on the two-qubit Hilbert space. For two qubits, ρ_v is entangled for $v \geq 1/3$ and separable otherwise [88]. It is also important to note that in the qubit case, isotropic states are equivalent to Werner states [88] up to local unitary transformations. Werner states are another family of entangled states that are used to study entanglement versus classical correlations, test separability criteria, and explore limits of non-locality. We now consider a generalized form of isotropic states in a multipartite setting. Consider an N-qudit isotropic state of the form

$$\rho_v = v\, |\Phi_{d,N}\rangle\langle\Phi_{d,N}| + (1-v)\, \frac{\mathbb{I}}{d^N}, \tag{2.3}$$

where $|\Phi_{d,N}\rangle$ is the generalised GHZ state defined as

$$|\Phi_{d,N}\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle^{\otimes N}. \tag{2.4}$$

The state ρ_v is fully separable for $v \leq \frac{1}{1+d^{N-1}}$, and entangled across some bipartition otherwise [33].

This construction extends the idea of isotropic states from two parties to many parties and higher-dimensional systems. Instead of mixing a Bell state with white noise, we now mix a generalised GHZ state, representing maximal correlations shared among all N parties with completely random noise over the full d^N-dimensional space. The parameter v shows how much of the multipartite entanglement survives when noise is present. As v decreases, the noise gradually destroys correlations, and for $v \leq 1/(1 + d^{N-1})$, the state becomes fully separable. Above this threshold, some entanglement remains, although it may not involve all parties simultaneously. We introduced isotropic states and their generalisation as they play an important role in our work.

2.1.2 Complementarity and Wave-Particle Duality

At the heart of quantum mechanics lies Bohr's principle of complementarity [15]. WPD can be viewed as a direct manifestation of this principle: quantum entities such as photons and electrons may exhibit either wave-like or particle-like behavior, but not both within a single experimental setup. The principle has been confirmed in a wide range of experimental tests across different physical platforms [49, 51, 84, 85, 92].

The trade-off between wave and particle behaviour is quantified through wave-particle duality relations. A widely studied formulation [36, 50] expresses this trade-off in terms of two complementary quantities: the *fringe* visibility $\mathcal{V}$ which quantifies wave-like behaviour, and the *path* distinguishability $\mathcal{D}$ which captures particle-like behaviour [19]. These quantities satisfy the inequality:

$$\mathcal{D}^2 + \mathcal{V}^2 \leq 1. \tag{2.5}$$

The standard MZI (see Fig. 2.1) provides a concrete setting in which this trade-off can be observed.

2.1.2.1 Complementarity in a Mach-Zehnder Interferometer

In our work, we follow the operational framework of Ref. [25], which allows us to quantify wave- and particle-like behaviour in terms of information-theoretic measures applicable to interferometric setups such as the MZI.

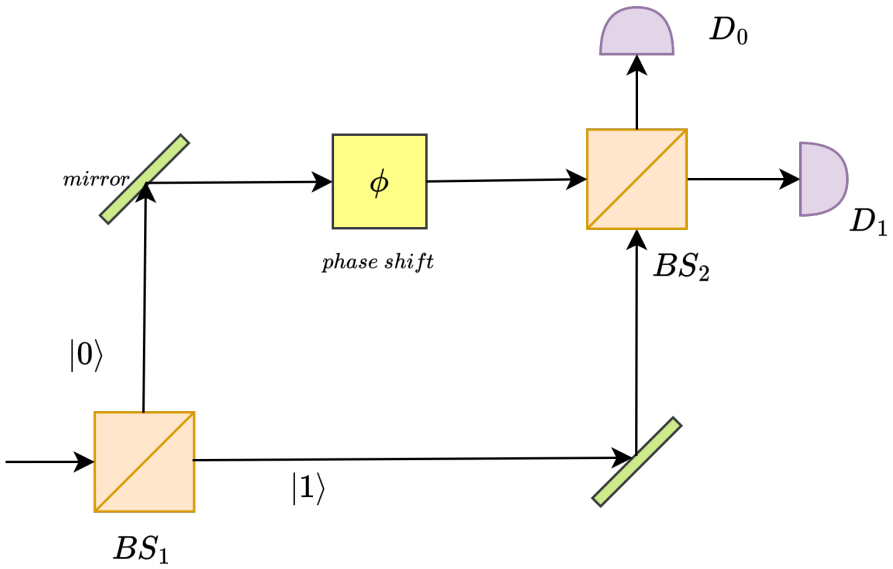

Figure 2.1: **Illustration of a Mach-Zehnder interferometer**. An incoming quantum system is directed onto a beam splitter, which creates a coherent superposition over two spatial paths associated with the states $|0\rangle$ and $|1\rangle$. A controllable phase ϕ is introduced along one of the paths, after which the two branches are brought together at a second beam splitter. The resulting interference is observed through measurements performed at the output detectors D_0 and D_1.

In a MZI, the relevant degrees of freedom can be restricted to a two-dimensional subspace spanned by the which-path states $\{|0\rangle, |1\rangle\}$, which may be treated as an effective qubit. The which-path observable is associated with the computational basis $Z = \{|0\rangle, |1\rangle\}$, while complementary observables W, each associated with a basis mutually unbiased with respect to Z, characterize the corresponding phase information. While the which-path observable is uniquely defined, phase information is associated with a family of complementary observables, reflecting different choices of relative phase between the paths.

The *path* distinguishability $\mathcal{D}$ is defined by the optimal success probability for correctly identifying the path taken by the particle,

$$\mathcal{D} := 2\, p_{\text{guess}}(Z) - 1. \tag{2.6}$$

Intuitively, $\mathcal{D}$ indicates the amount of which-path information accessible in the experiment, with $\mathcal{D} = 1$ corresponding to perfect path knowledge and $\mathcal{D} = 0$ corresponding to complete indistinguishability.

Wave-like behaviour is quantified by the interferometric visibility $\mathcal{V}$, which measures the extent to which the particle exhibits interference, corresponding to a coherent superposition of

the which-path states. Formally, it is defined as

$$\mathcal{V} := \max_{W} \left(2\, p_{\text{guess}}(W) - 1\right), \qquad W = \{|w_+\rangle, |w_-\rangle\}, \quad |w_\pm\rangle = \frac{1}{\sqrt{2}} \left(|0\rangle \pm e^{i\phi}|1\rangle\right), \tag{2.7}$$

where ϕ is the relative phase between the two paths in the interferometer.

The extreme cases of the trade-off (2.5) between $\mathcal{D}$ and $\mathcal{V}$ illustrate its physical meaning: perfect path distinguishability ($\mathcal{D} = 1$) implies the absence of interference ($\mathcal{V} = 0$), while maximal visibility ($\mathcal{V} = 1$) corresponds to completely indistinguishable paths. Intermediate values describe partial path information coexisting with reduced interference.

Experimental estimation of $\mathcal{D}$ and $\mathcal{V}$. $\mathcal{D}$ and $\mathcal{V}$ can be directly estimated in experiments. The *path* distinguishability $\mathcal{D}$ is obtained by blocking each path (upper U or lower L) in turn and measuring the resulting detection probabilities p_0 and p_1 at the interferometer outputs. The distinguishability associated with each blocked path is computed as

$$D_{U(L)} := \frac{|p_0 - p_1|}{p_0 + p_1}\Big|_{\text{path } U(L) \text{ blocked}}, \tag{2.8}$$

and the overall path distinguishability is then given by the average

$$\mathcal{D} := \frac{1}{2}(D_U + D_L). \tag{2.9}$$

The interferometric visibility $\mathcal{V}$ is determined by varying the relative phase ϕ between the two paths and recording the resulting modulation in output probabilities. For each output port j, the visibility is defined as

$$\mathcal{V}_j := \frac{p_j^{\max} - p_j^{\min}}{p_j^{\max} + p_j^{\min}}, \tag{2.10}$$

where $p_j^{\max}$ and $p_j^{\min}$ are the maximum and minimum detection probabilities observed. The overall visibility is obtained by averaging over the output ports:

$$\mathcal{V} := \frac{1}{2}(\mathcal{V}_0 + \mathcal{V}_1). \tag{2.11}$$

Higher dimensional generalization. The framework above extends to higher-dimensional interferometric settings involving multiple paths [23]. In such scenarios, particle-like behaviour is associated with the computational basis, encoding path information, while wave-like behaviour is described using complementary observables. In particular, for an n-path interferometer with symmetric beam splitters, this complementary basis is given by the Fourier transform of the computational basis, capturing interference across multiple paths.

In this multipath setting, these behaviours can be quantified operationally through guessing probabilities. The generalized distinguishability and visibility are defined as

$$\mathcal{D} := \frac{n\, p_{\text{guess}}(Z) - 1}{n-1}, \tag{2.12}$$

$$\mathcal{V} := \frac{n\, p_{\text{guess}}^{\max_{\{\phi_k\}}}(W) - 1}{n-1}, \tag{2.13}$$

where the maximization is taken over all controllable phase settings $\{\phi_k\}$.

Complementarity as a resource in cryptography. In an interferometric setup, one can attempt to guess either the which-path observable Z or a complementary phase observable W, with the success of each task quantified by the corresponding probabilities of correctly inferring the outcome. EURs impose a fundamental constraint on these probabilities: any increase in the predictability of one observable necessarily reduces the predictability of the other. This trade-off reflects the notion of complementarity. Since EURs play a central role in security proofs and information-theoretic analyses [24] in quantum cryptography, this connection motivates viewing complementarity as an operational resource in quantum information processing, with relevance to both communication tasks [22] and cryptographic security [24], which will be explored in later sections.

2.2 Communication using Quantum Systems

This section introduces the operational task of transmitting information using quantum systems. Building on the perspective developed in the previous section, where quantum features such as entanglement and complementarity were identified as resources, we now examine how these resources can be harnessed in concrete communication scenarios.

In a typical communication task, a sender encodes information into quantum states, which are transmitted through a physical channel to a receiver who performs measurements to recover the encoded message. In realistic settings, this process is affected by noise, imperfections, and other physical constraints, which can degrade the transmitted information. A central objective is therefore to design protocols that achieve reliable communication despite these limitations.

In addition, practical implementations are often subject to finite resources, such as limited system dimension, a bounded number of channel uses, or restricted measurement capabilities. These constraints motivate an operational framework in which the performance of communication protocols can be quantified and compared. Within this framework, quantum resources are understood in terms of the advantages they provide, such as enhancing reliability, increasing information transmission, or reducing resource requirements.

In what follows, we focus on the role of entanglement in communication tasks.

2.2.1 Entanglement-assisted Classical Communication

EACC refers to protocols in which a sender and receiver share entanglement prior to communication, enabling the transmission of classical information over a quantum channel more efficiently than would be possible classically. This is the protocol we focus on because it is central to the results in this work.

A canonical example of EACC is super-dense coding where shared entanglement allows the transmission of two classical bits by sending a single qubit.

This protocol can be naturally extended to higher-dimensional systems. When the shared resource is a maximally entangled state of local dimension d, the encoding can be performed using a set of d^2 orthogonal unitary operations, allowing the transmission of $2\log_2 d$ classical bits via the communication of a single d-dimensional quantum system.

In the following, we describe the qubit protocol explicitly and then generalize it to the higher-dimensional setting.

Qubit superdense coding. Let the sender (Alice) and receiver (Bob) share a maximally entangled Bell state

$$\left|\Phi^+\right\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right). \tag{2.14}$$

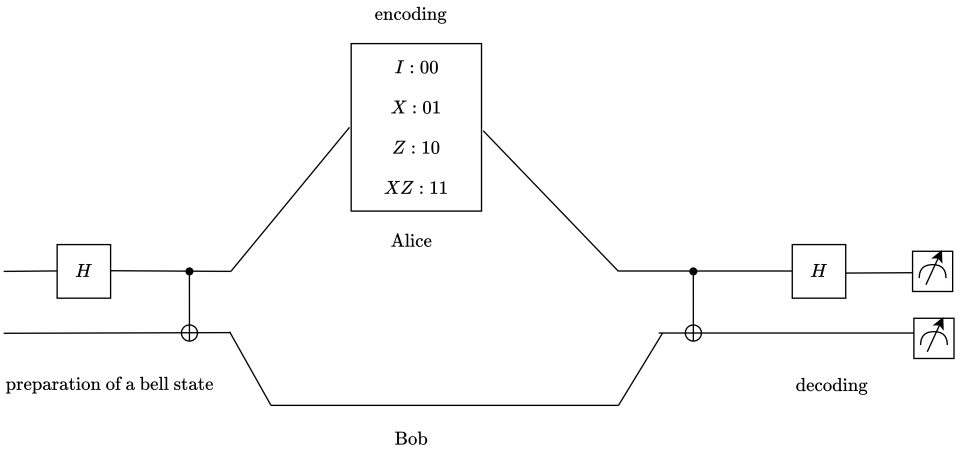

Figure 2.2: **Superdense coding protocol (qubit case).** Alice and Bob share a maximally entangled state. Alice encodes classical information by applying a local unitary operation to her subsystem and transmits it to Bob. Bob then performs a joint measurement on both subsystems to perfectly distinguish the encoded message.

Alice encodes two classical bits $x = (x_1, x_2) \in \{0,1\}^2$ by applying one of the Pauli operators

$$U_x \in \{\mathbb{I}, X, Z, XZ\}, \tag{2.15}$$

on her subsystem. The resulting states are

$$|\Psi_x\rangle_{AB} = (U_x \otimes \mathbb{I}) \left|\Phi^+\right\rangle_{AB}. \tag{2.16}$$

These four states form an orthonormal basis (the Bell basis),

$$\langle \Psi_x | \Psi_{x'} \rangle = \delta_{x,x'}. \tag{2.17}$$

Alice then sends her qubit to Bob, who performs a joint measurement in the Bell basis to perfectly distinguish the states $\{|\Psi_x\rangle\}$ and recover x.

Thus, two classical bits are transmitted through the communication of a single qubit:

$$C = 2 \text{ bits}. \tag{2.18}$$

Qudit super-dense coding. Each of the components of the qubit protocol can be extended to higher-dimensional systems [89]. The shared Bell state is replaced by a maximally entangled qudit state of local dimension d,

$$|\Phi_d\rangle_{AB} = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k\rangle_A \otimes |k\rangle_B, \tag{2.19}$$

while the set of Pauli operators generalizes to a collection of d^2 orthogonal unitary operators

$$U_{m,n} = X^m Z^n, \qquad m, n \in \{0, \ldots, d-1\}, \tag{2.20}$$

where the generalized shift and phase operators act as

$$X\,|k\rangle = |(k+1) \bmod d\rangle\,, \tag{2.21}$$

$$Z\,|k\rangle = \omega^k\,|k\rangle\,, \quad \omega = e^{2\pi i/d}. \tag{2.22}$$

These operations generate a set of d^2 mutually orthogonal qudit states,

$$|\Psi_{m,n}\rangle = (U_{m,n} \otimes \mathbb{I})\,|\Phi_d\rangle\,, \tag{2.23}$$

satisfying,

$$\langle \Psi_{m,n} | \Psi_{m',n'} \rangle = \delta_{m,m'}\,\delta_{n,n'}. \tag{2.24}$$

The receiver can therefore perfectly distinguish these states, allowing the transmission of

$$C = 2\log_2 d \tag{2.25}$$

classical bits through the communication of a single d-dimensional quantum system.

2.2.2 Finite Resource Communication

While super-dense coding illustrates the advantage of EA communication in an ideal, noiseless setting, practical communication scenarios are inherently subject to imperfections. Quantum channels are typically affected by noise, leading to errors or erasures during transmission, and implementations are restricted to a finite number of channel uses. As a result, asymptotic capacity-based descriptions [7, 30] are often insufficient to capture realistic performance. These considerations motivate the study of EACC protocols in finite-resource regimes, where the presence of noise and interference requires the use of error-correcting techniques, and where reliability must be ensured under physically relevant constraints.

To address these challenges, it is useful to introduce a minimal set of tools from coding theory, adapted to the present EACC setting. Rather than developing the full mathematical framework, we focus only on the essential concepts required to describe finite-length protocols and their performance in our context.

Coding theory for physicists

The basic problem in coding theory can be stated as follows. Suppose we have a message x of length k that we wish to transmit or store reliably. To protect against errors or losses, we encode x into a *codeword* m of length $n > k$, introducing redundancy. During transmission or storage, some components of m may be corrupted or lost, resulting in a distorted version of m, m^*. The goal of coding theory is to design the encoding so that, given m^* (or partial access to it), we can recover the original message x or at least some information about it. This idea applies to both storage and communication scenarios.

Linear codes. Formally, a *code* $\mathcal{C}$ of block length n over an alphabet $\mathcal{A}_q$ with q letters is a subset $\mathcal{C} \subseteq \mathcal{A}_q^n$ (where q denotes the dimension of the quantum system associated with the communication channel in our scenario). The elements $m \in \mathcal{C}$ are called *codewords*.

In the case of a *linear code*, the alphabet $\mathcal{A}_q$ is chosen to be a finite field $\mathbb{F}_q$, and the codewords form a linear structure over $\mathbb{F}_q$, meaning that linear combinations (over $\mathbb{F}_q$) of codewords are again codewords. A linear code of dimension k encodes q^k distinct messages, where k is the length of the original message, i.e., the number of information symbols encoded into each codeword. Such a code is typically denoted by $[n, k, d]_q$, where d is the *minimum distance* of the code, which quantifies its ability to detect and correct errors or erasures. The *rate* of a code,

$$R = \frac{k}{n}, \tag{2.26}$$

quantifies the fraction of transmitted symbols that carry actual information, providing a measure of communication efficiency. A higher rate means that less redundancy is used, allowing more information to be transmitted per channel use, but typically at the cost of reduced tolerance to errors and erasures.

In the context of EACC, we introduce a parameter c representing the number of channel uses assisted by shared entanglement. The generalized notation

$$[n, k, d; c]_q$$

extends the standard parameters by explicitly accounting for the available entanglement.

Finite fields. To construct and manipulate codes algebraically, it is convenient to endow the alphabet $\mathcal{A}_q$ with additional structure. In particular, we model it as a *finite field* $\mathbb{F}_q$ with q elements, where q is a power of a prime number. This allows two codewords to be added component-wise and multiplied by scalars from $\mathbb{F}_q$, ensuring that the set of codewords forms a linear structure and allowing structured constructions, for instance based on polynomials.

In the EA setting, it is also useful to consider an extension field $\mathbb{F}_{q^2}$, which can be viewed as an enlarged alphabet containing $\mathbb{F}_q$ as a subset. The field $\mathbb{F}_{q^2}$ has degree 2 over $\mathbb{F}_q$, meaning that every element $\alpha \in \mathbb{F}_{q^2}$ can be written in the form

$$\alpha = a + b\gamma, \tag{2.27}$$

where $a, b \in \mathbb{F}_q$ and $\gamma \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. The field $\mathbb{F}_{q^2}$ can be viewed as a two-dimensional extension of $\mathbb{F}_q$, meaning that it forms a two-dimensional vector space over $\mathbb{F}_q$ in which each element can be represented by a pair of elements from $\mathbb{F}_q$.

An important structural feature of $\mathbb{F}_{q^2}$ is that elements outside $\mathbb{F}_q$ occur in conjugate pairs $\{\gamma, \gamma^q\}$. For polynomials $f \in \mathbb{F}_q[x]$ with coefficients in $\mathbb{F}_q$, this implies that evaluation at conjugate points satisfies

$$f(\gamma^q) = f(\gamma)^q. \tag{2.28}$$

These properties allow one to consistently relate symbols in $\mathbb{F}_{q^2}$ to pairs of symbols in $\mathbb{F}_q$, which is particularly useful in the construction of coding schemes where different channel uses may effectively carry different amounts of information.

Minimum distance and error/erasure correction. For a linear code, the minimum distance d of the code equals the minimum weight (number of non-zero components) of a non-zero codeword. Operationally, the minimum distance determines the error-correcting capability of the code: a code with minimum distance d can correct up to $d-1$ *erasures* (symbols lost at known positions) or up to $\lfloor (d-1)/2 \rfloor$ *errors* (symbols corrupted at unknown positions). Thus, the minimum distance provides a direct measure of the code's ability to ensure reliable communication in the presence of noise.

Erasures and errors. An *erasure* is an error at a known position [39], meaning that the receiver knows which symbol has been lost during transmission. This differs from a general *error*, where the symbol is corrupted but its position is not known. As a result, erasures are typically easier to correct than errors.

To build intuition, let us examine how erasures and errors appear in the EA setting we consider in our work. Erasures must always be interpreted in relation to the underlying communication protocol. Consider a quantum channel used n times, where c of these uses are assisted by shared entanglement via super-dense coding, and $n-c$ uses are unassisted. Each unassisted transmission corresponds to sending a single classical symbol from the alphabet $\mathbb{F}_q$, whereas each EA transmission effectively encodes two classical symbols, corresponding to an element of $\mathbb{F}_{q^2}$. Since $\mathbb{F}_{q^2}$ can be viewed as a two-dimensional extension of $\mathbb{F}_q$, each of its elements can be identified with a pair of symbols from $\mathbb{F}_q$. Thus, transmissions associated with $\mathbb{F}_{q^2}$ naturally correspond to blocks of two classical symbols.

As a result, an erasure affects the transmitted information differently depending on the type of channel use. An erasure occurring in an unassisted transmission corresponds to the loss of a single classical symbol. In contrast, an erasure in an EA (super-dense coded) transmission corresponds to the loss of an entire block of two classical symbols, since both are encoded into a single quantum system.

Singleton bound and Reed–Solomon codes. A fundamental limit on code parameters is provided by the *Singleton bound*:

$$k \leq n - d + 1. \tag{2.29}$$

This expresses a trade-off between the amount of information transmitted and the number of errors or erasures the code can correct. Codes that achieve equality in the Singleton bound are called *maximum distance separable (MDS)* codes, representing optimal redundancy for a given block length and minimum distance.

A prominent example of MDS codes are *Reed-Solomon codes*. These are constructed by evaluating polynomials $f \in \mathbb{F}_q[x]$ of degree at most $k-1$ at n distinct points $\beta_1, \ldots, \beta_n \in \mathbb{F}_q$. Each polynomial defines a codeword

$$(f(\beta_1), \ldots, f(\beta_n)),$$

so that encoding corresponds to a polynomial evaluation map.

A key property underlying this construction is that a polynomial of degree at most $k-1$ is uniquely determined by its values on any k distinct points. This is a consequence of polynomial interpolation over finite fields, and it ensures that the code achieves the Singleton bound. Reed–Solomon codes thus provide a good example of optimal codes and serve as a useful reference point for more general constructions.

For a detailed treatment of the essential concepts introduced in this section, see [57, 72].

2.3 Secure Communication

In the previous section, we discussed how to reliably send information using quantum systems, despite noise and other physical constraints. But in real-world situations, reliability alone is not enough, communication often needs to be secure, so that sensitive information cannot be accessed by unauthorized parties. This brings in a new layer of difficulty; beyond dealing with noise, we now also have to consider the possibility of an eavesdropper trying to intercept or learn something about the transmitted information.

Quantum mechanics addresses this challenge by providing resources like entanglement and complementarity, allowing us to design communication protocols whose security is guaranteed by physical principles rather than computational considerations.

This section develops these ideas in the context of quantum cryptography. We begin by introducing QKD and describe its two main realizations: entanglement-based (EB) and prepare-and-measure (PM) protocols. We then discuss different security models. Finally, we analyze relevant adversarial strategies, practical limitations and connect security to information-theoretic constraints, with particular emphasis on the role of complementarity and EURs.

2.3.1 Quantum Key Distribution

The central objective of QKD is to enable two distant parties to generate a shared secret key—namely, a string of correlated random bits that can be used for tasks such as encrypting messages with security guaranteed by the principles of quantum mechanics, even in the presence of an adversary. Broadly, QKD protocols can be realized in two complementary ways. In PM protocols, one party encodes information into quantum states and sends them to the other, who performs measurements on the received systems. In contrast, EB protocols rely on the distribution of entangled states, and both parties perform measurements on their respective subsystems to obtain correlated outcomes. These two approaches provide different operational descriptions of the same underlying task [69].

Entanglement-based QKD. In the standard EB-QKD setting [35, 74, 86], two distant parties, Alice and Bob, aim to establish a shared secret key by measuring quantum systems distributed by a common source. In each round, the source prepares an entangled state and sends one subsystem to Alice and the other to Bob. Upon receiving their systems, both parties independently choose measurement settings and record the corresponding outcomes, thereby generating correlated measurement results over many rounds.

The observed correlations are determined by the shared quantum state and the measurements performed by the parties. After the measurement stage, Alice and Bob publicly announce their measurement settings for all rounds and perform sifting to identify the subset of rounds with matching measurement bases, referred to as the sifted key. A subset of these sifted rounds is then selected for parameter estimation, for which the corresponding measurement outcomes are

publicly revealed. This allows the parties to estimate relevant quantities such as the quantum bit error rate (QBER) and to detect potential eavesdropping.

The remaining sifted rounds, after parameter estimation, are used for key generation. Their corresponding outcomes are kept private and form the raw key, which is subsequently processed using error correction and privacy amplification to obtain a final secure key.

While the above describes the two-party scenario, the framework naturally extends to multiple parties. Consider N parties labeled $A_1, A_2, \ldots, A_N$, each receiving a subsystem from a shared source. Each party A_i performs a measurement chosen from a set of inputs x_i, producing an outcome a_i. Each party's measurement device is described by a collection of operators $\{M_{a_i|x_i}\}$, corresponding to the outcome a_i obtained when the measurement setting x_i is chosen. Defining $\vec{x} = (x_1, \ldots, x_N)$ and $\vec{a} = (a_1, \ldots, a_N)$, the resulting correlations are captured by $\{p(\vec{a}|\vec{x})\}$, where,

$$p(\vec{a}|\vec{x}) = \mathrm{Tr}\left[\left(\bigotimes_{i=1}^{N} M_{a_i|x_i}\right)\rho_{A_1\ldots A_N}\right]. \tag{2.30}$$

Prepare-and-measure QKD. In the PM scenario [9, 64, 69], the task of key distribution is described in terms of state preparation and transmission. In each round, Alice selects an input $a \in \{0, \ldots, m_A - 1\}$ and encodes it into a d-dimensional physical system, which she sends to Bob through a potentially insecure channel. Upon receiving the system, Bob chooses a measurement setting $y \in \{0, \ldots, m_B - 1\}$ and obtains an outcome $b \in \{0, \ldots, k-1\}$. Repeating this process over many rounds gives rise to a conditional probability distribution $\{P(b|a,y)\}_{a,b,y}$ that characterizes the observed correlations.

The set of achievable correlations is constrained by the dimension d of the communicated system. In particular, if only classical systems of dimension d are used, the observed statistics must satisfy bounds of the form

$$\sum_{a,y,b} w_{a,y,b}\, P(b|a,y) \leq C_d, \tag{2.31}$$

where C_d denotes the maximal value attainable with classical resources. In the above equation, $w_{a,y,b} \in \mathbb{R}$ are fixed coefficients defining a linear dimension witness, i.e., a linear functional of the probability distribution $P(b|a,y)$. Inequalities such as 2.31 are known as *dimension witnesses*. Quantum systems of the same dimension, however, can surpass these classical limits. In this case, the probabilities are given by the Born rule $P(b|a,y) = \mathrm{Tr}(\rho_a M_b^y)$, where ρ_a are d-dimensional quantum states prepared by Alice, and $\{M_b^y\}$ are the measurement operators corresponding to Bob's measurement choice.

Security models. The security of QKD protocols depends crucially on the assumptions made about the devices used by the communicating parties. Importantly, the operational descriptions introduced above, both EB and PM protocols are independent of such assumptions. The same

protocol can therefore be analyzed under different security frameworks, depending on the level of trust assigned to the devices.

At one end of this spectrum lies the DD setting, where the measurement devices are assumed to be fully characterized and trusted. In this case, the security analysis relies on a detailed description of the underlying quantum states and measurement operators. Many standard implementations of EB-QKD are studied within this framework [11, 35, 53, 73].

At the other end of the spectrum, one can adopt an approach where no assumptions are made about the internal workings of the devices. In this case, security is inferred directly from the observed correlations, through the violation of Bell inequalities. Although this leads to very strong forms of security, it also comes with significant experimental challenges [1, 60, 93].

Intermediate between these regimes are SDI frameworks [64, 70], where only limited assumptions are imposed, such as a bound on the dimension of the communicated system. In such scenarios, one can still certify non-classical behavior and establish security without full trust in the internal functioning of the devices, thereby providing more relaxed and experimentally accessible conditions.

In this thesis, we focus primarily on EB-QKD protocols analyzed in the DD setting. We also examine SDI approaches closely. These frameworks are directly relevant to the results developed in our work, and provide a natural setting for studying the role of quantum resources in secure communication.

Entanglement as a security resource across QKD frameworks. In EB-QKD protocols, such as E91 [35] and BBM92 [11], a source distributes entangled states to distant parties, who perform local measurements to generate correlated outcomes. These correlations, when suitably processed, give rise to a shared secret key.

Although PM-QKD protocols differ operationally from EB schemes, they can always be reformulated as an equivalent EB protocol [69, 78]. This equivalence is not limited to PM-QKD; the security of standard QKD protocols, including the six-state protocol [18], B92 [8], decoy-state BB84 [82], and measurement-device-independent (MDI) QKD [54] can be analyzed using an entanglement-based picture. This allows one to characterize the correlations between the legitimate parties and an adversary in terms of a shared quantum state and associated measurement operators. Entanglement is also essential in more stringent security scenarios such as DI settings [93].

While entanglement is a necessary ingredient in QKD [26], its mere presence is not enough to guarantee security. Secure key generation requires key-distillability [42], which characterizes whether a given set of correlations can be processed into a secret key and the additional conditions needed to achieve this may depend on the specific protocol under consideration. We explore this aspect in our article [73] included in this thesis.

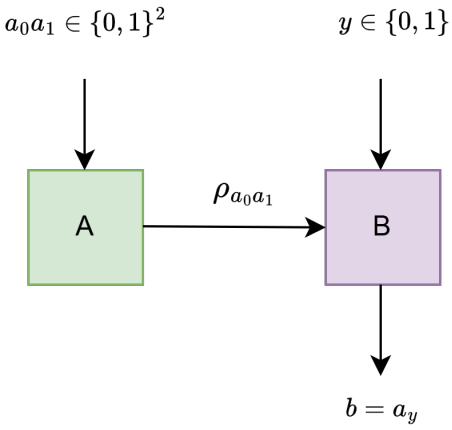

Figure 2.3: **$2 \to 1$ random access code.** PM scenario where Alice encodes two classical bits into a qubit and sends it to Bob, who then measures it to guess one of Alice's input bits based on y.

Semi-device-independent scenario. The discussion in this section is based primarily on the framework developed in [64]. The SDI framework is naturally realised in a PM setting. The dimension of states sent from Alice to Bob is restricted. This restriction, in turn, limits the correlations that can be observed in the protocol.

In this context, dimension witnesses, introduced in the PM scenario play a central role: they provide bounds on correlations achievable with systems of bounded dimension. Depending on the underlying assumptions, their violation can either certify that the observed correlations cannot be reproduced by classical systems of a given dimension, or establish a lower bound on the dimension of the underlying quantum systems.

A particularly useful way to understand SDI protocols is through their connection to quantum random access codes (QRACs). In the $(4, 2, 2)$ SDI scenario, Alice prepares two-dimensional quantum systems with four possible preparations, labeled by the two bits $a_0a_1 \in \{0,1\}^2$. For each of Alice's four possible input bit strings a_0a_1, she prepares and sends a quantum state $\rho_{a_0a_1}$ to Bob (see Fig. 2.3).

Explicitly, the four states are

$$\rho_{00} = |0\rangle\langle 0|, \quad \rho_{11} = |1\rangle\langle 1|, \quad \rho_{10} = |+\rangle\langle +|, \quad \rho_{01} = |-\rangle\langle -|, \tag{2.32}$$

where $|0\rangle$ and $|1\rangle$ are the eigenstates of σ_z, and $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ are the eigenstates of σ_x. These four preparations correspond exactly to those used in the BB84 protocol [9].

Bob's task is to guess the bit a_y. To do this, he performs one of two binary measurements, M_0 or M_1, depending on his input $y \in \{0,1\}$, and produces an outcome $b \in \{0,1\}$, which serves as his guess for the bit a_y. The observed data is described by the correlators $E_{a_0a_1,y} := P(b =$

$0 \mid a_0 a_1, y)$, from which one constructs the dimension witness

$$S = E_{00,0} + E_{00,1} + E_{01,0} - E_{01,1} - E_{10,0} + E_{10,1} - E_{11,0} - E_{11,1}. \tag{2.33}$$

From here on we refer to S as the "SDI witness". Classically, one has $S \leq 2$, while quantum strategies can reach up to $S = 2\sqrt{2}$.

For a given data table, Bob's average success probability in correctly identifying the target bit is,

$$P_B = \frac{1}{8} \sum_{a_0,a_1,y} P(b = a_y \mid a_0, a_1, y) = \frac{S+4}{8}, \tag{2.34}$$

Classical strategies satisfy $P_B \leq 3/4$, whereas higher values certify quantum behavior and, in particular, guarantee security within the SDI framework under the bounded-dimension assumption.

2.3.2 Security Analysis and Limitations

The security of QKD protocols is assessed by analyzing the information accessible to an adversary, commonly referred to as Eve, under well-defined attack models. These models specify the capabilities of the adversary and the strategies she may employ to gain information about the key while remaining undetected during the protocol.

In general, Eve interacts with the quantum systems exchanged between the legitimate parties and may also exploit classical information revealed during the protocol. The goal of the security analysis is to quantify how much information Eve can obtain and, consequently, to determine whether a secret key can still be extracted.

In what follows, we focus on three aspects that are particularly relevant to the results developed in this work: individual attacks, convex combination (C.C.) attacks, the effect of classical side-channel leakage, and the role of quantum repeaters in the scalability of QKD networks.

Individual attacks. We begin by considering *individual attacks* [64, 70], one of the simplest and most commonly studied adversarial models. In this setting, Eve interacts independently with each quantum system transmitted through the channel, applying the same strategy in every round and measuring her system immediately after the interaction.

Operationally, this means that Eve attempts to extract information about Alice's inputs directly from each intercepted system, without storing quantum information or performing joint measurements across multiple rounds. Her measurement strategy is unrestricted and can be optimized to maximize her average guessing probability.

In contrast, Bob's measurements are fixed by the protocol and are optimized to recover the encoded information and generate the key. Eve, on the other hand, is adversarial and aims to

extract as much information as possible about the key. The security of the protocol is thus determined by the trade-off between Bob's information gain and Eve's ability to guess the transmitted information.

Convex combination attacks. While a wide range of adversarial strategies beyond individual attacks can be considered, it is often sufficient to focus on simple yet representative attacks that capture the essential features of realistic eavesdropping.

One such class of attacks is given by C.C. strategies, originally introduced in the DI setting [2, 56]. These attacks are defined at the level of observed correlations and can be adapted to other security models, including the DD scenario relevant to our context.

In this model, the observed correlations $\{p(\vec{a}|\vec{x})\}$ in eq. 2.30 are expressed as a probabilistic mixture of two contributions,

$$p(\vec{a}|\vec{x}) = q_S\, p^{\mathcal{S}}(\vec{a}|\vec{x}) + (1 - q_S)\, p^{\mathcal{E}}(\vec{a}|\vec{x}), \tag{2.35}$$

where $p^{\mathcal{S}}$ denotes correlations achievable using separable resources, $p^{\mathcal{E}}$ denotes correlations arising from entangled resources, and $0 \leq q_S \leq 1$.

We introduce a classical variable $e \in \{\mathcal{S}, \mathcal{E}\}$ that labels which component of the mixture is distributed in a given round. This variable is assumed to be known to Eve, allowing her to condition her strategy on whether the correlations originate from the separable or entangled component.

This model captures an important operational feature. When the correlations arise from the separable component, they admit a classical explanation, and Eve can in principle obtain complete information about the outcomes, precluding the extraction of any secure key. In contrast, the entangled component can generate correlations that are partially inaccessible to Eve and may therefore be used for secure key generation. To quantify the amount of key that can be extracted we consider the intrinsic information $I(A_1, \ldots, A_N \downarrow e)$ [43, 61] , defined as

$$I(A_1 \ldots A_N \downarrow e)_\rho = \inf_{\rho' = (\mathbb{I}_{A_1 \ldots A_N} \otimes \Lambda_E)(\rho)} I(A_1 \ldots A_N|e)_{\rho'}, \tag{2.36}$$

where Λ_E denotes an arbitrary operation performed by Eve and $I(A_1 \ldots A_N|e)_{\rho'}$ is the mutual information of the parties conditioned on Eve's information. For separable correlations, one has $I(A_1 \ldots A_N \downarrow e)_{\rho^{\mathcal{S}}} = 0$, reflecting the fact that no secret key can be extracted.

In the present analysis, rather than minimizing over all possible operations Λ_E, we restrict attention to the specific convex-combination attack described above. Using the convexity of conditional mutual information, the key rate R is upper-bounded by

$$R \leq \frac{1}{N-1} \sum_e \sum_{\vec{x}} p_{\vec{x}}\, p(e|\vec{x})\, I_{\vec{x}}(A_1 \ldots A_N|e, C.C.), \tag{2.37}$$

where $I_{\vec{x}}(A_1 \ldots A_N|e, C.C.)$ denotes the conditional mutual information of the parties given inputs $\vec{x}$ and Eve's side information.

Classical side-channel leakage. In realistic implementations, information about the measurement outcomes can leak through unintended classical channels. This phenomenon, known as *classical side-channel leakage*, arises because quantum measurements are ultimately recorded using physical devices. For instance, detector outputs may be encoded in electrical signals such as voltage fluctuations, timing information, or electromagnetic emissions [5, 65, 81] . If these physical signatures depend on the measurement outcome, even slightly, an adversary may gain partial information about the key without directly interacting with the quantum systems.

This effect is particularly relevant in practice, as it introduces additional correlations between the legitimate parties and the adversary that are not captured by idealized protocol descriptions. As a result, even protocols that are secure in principle may become vulnerable in the presence of leakage.

To model this effect, one typically assumes that each measurement outcome is revealed to the adversary with some probability $\mathcal{L}$ [69]. In the worst-case scenario, this leakage may reveal the outcomes of both parties in the same round, thereby giving the adversary direct access to portions of the raw key.

Even small values of $\mathcal{L}$ can significantly degrade security [55, 58], as the leaked information accumulates over many rounds and can reduce or even eliminate the achievable key rate.

Quantum repeaters and QKD. While the above aspects focus on adversarial strategies and implementation imperfections at the protocol level, an additional important limitation arises when considering the extension of QKD to long distances. In practice, long-distance QKD is limited by loss and noise in optical channels, and by the impossibility of amplifying quantum states due to the no-cloning theorem. A quantum repeater [4, 16, 32] addresses this by replacing direct transmission with the distribution of entanglement over shorter segments, followed by entanglement swapping [48].

Consider a single repeater placed between Alice and Bob. Two sources generate bipartite entangled states ρ_{AR_1} and ρ_{R_1B}: the first source distributes one subsystem to Alice and the other to the repeater, while the second source distributes one subsystem to Bob and the other to the repeater. The repeater thus holds subsystems $R_1^{(1)}$ and $R_1^{(2)}$. In realistic scenarios, these states are noisy and can be modelled as isotropic states with visibility v. At this stage, Alice and Bob are not entangled with each other, but are each entangled only with the repeater.

The repeater performs a Bell-state measurement on $R_1^{(1)}$ and $R_1^{(2)}$, resulting in entanglement swapping. Conditioned on the measurement outcome (and a corresponding local Pauli correction), Alice and Bob now share an entangled state ρ_{AB}. If the initial states have visibility v, the resulting state is again isotropic with visibility v^2.

Once entanglement is established, a standard EB-QKD protocol can be used to extract a secret key.

2.3.3 Complementarity, Entropic Uncertainty Relations and Security

The discussion of security so far has been framed in terms of the eavesdropper's capabilities together with the level of trust placed in devices. In each case, the main objective is to bound the information accessible to an adversary about the information shared between the honest parties. From an information-theoretic perspective, such knowledge is naturally quantified using entropic measures, which capture the adversary's uncertainty about classical random variables corresponding to the outcomes of measurements performed by the honest parties.

Security can therefore be understood as establishing lower bounds on this uncertainty, ensuring that a sufficiently large amount of randomness remains inaccessible to the adversary. At this stage, it is natural to ask how such limits on an adversary's knowledge can be expressed in a precise and quantitative manner.

In quantum settings, these limitations are captured by EURs, which quantify the trade-offs in predicting the outcomes of incompatible measurements. In particular, EURs formalize the fact that no physical system can simultaneously provide complete information about two non-commuting observables. Interestingly, in Ref. [25] it was shown that EURs can be understood as a quantitative expression of complementarity.

Equivalence between wave-particle duality relations and entropic uncertainty relations. The WPDR (2.5) introduced earlier can be mapped to an EUR based on min- and max-entropies [25]. This means that the WPDR can be expressed as,

$$H_{\min}(Z) + \min_{W} H_{\max}(W) \geq 1. \tag{2.38}$$

where $H_{\min}(Z)$ and $H_{\max}(W)$ quantify, respectively, the uncertainty about the which-path information and the complementary phase information. For a probability distribution $P = \{p_j\}$, these entropies are defined by

$$H_{\min}(P) := -\log_2 \max_j p_j, \tag{2.39}$$

$$H_{\max}(P) := 2\log_2 \sum_j \sqrt{p_j}. \tag{2.40}$$

This shows that the binary duality relation 2.5 can be viewed as an instance of an EUR, demonstrating that the trade-off between particle-like and wave-like properties is constrained by fundamental quantum uncertainty. Explicitly, the entropic quantities can be expressed in terms of $\mathcal{D}$ (2.6) and $\mathcal{V}$ (2.7) as follows,

$$H_{\min}(Z) = -\log_2 \left(\frac{1+\mathcal{D}}{2}\right), \tag{2.41}$$

$$H_{\max}(W) = \log_2 \left(1 + \sqrt{1-\mathcal{V}^2}\right). \tag{2.42}$$

The equivalence of entropic uncertainty with WPD was recently experimentally demonstrated [79].

In the higher-dimensional setting (2.5) is equivalent to

$$H_{\min}(Z) + \min_{W} H_{\max}(W) \geq \log_2 n, \tag{2.43}$$

highlighting the dimension-dependent limits on accessible information.

This framework admits a natural operational interpretation in terms of guessing games [25]. An adversary attempting to gain information about the system can be viewed as trying to predict the outcomes of measurements performed by the honest parties. EURs then impose quantitative limits on the success of such predictions, enforcing a trade-off between the predictability of incompatible observables. In this sense, complementarity itself acts as a resource: it enforces intrinsic information-theoretic constraints that can be harnessed to guarantee security [3, 14, 62, 74, 94].

This perspective is consistent with existing cryptographic paradigms. In standard DD protocols, security arises from the use of incompatible measurements, where gaining information about one observable necessarily disturbs its complementary counterpart, leading to detectable signatures of eavesdropping [52]. To address experimental challenges put forth by the DI paradigm, complementarity-based DI protocols have been proposed as more practical alternatives [94]. It is important to note that complementarity's significance in SDI scenarios remains largely underexplored.

CHAPTER 3

Summary of the dissertation

In this chapter, we summarize the main results of the articles included in this thesis [68, 70, 73]. Each article is first introduced through its central idea, followed by a discussion of the main insights and contributions.

3.1 Codes for entanglement assisted classical communication

At its core, this work develops a constructive coding framework for EACC over a q-dimensional quantum channel (qudit channel) used n times, supported by $c \leq n$ pre-shared maximally entangled qudit pairs. The scheme guarantees reliable transmission in the presence of up to $d-1$ erasures and achieves exact recovery, meaning that decoding succeeds with zero probability of error. This is accomplished in the following way.

The Essential Reduction. As is standard in coding theory, we reformulate the task of transmitting classical information over a quantum channel as an equivalent classical coding problem. Depending on the availability of entanglement, we decide how to utilize each channel use. In the absence of entanglement, we employ a single channel use to transmit one classical symbol from an alphabet of size q (the dimension of the quantum system). In contrast, when a maximally entangled pair is available, we choose to employ the channel together with super-dense coding to send q^2 distinct classical messages, which is equivalent to transmitting two classical symbols from an alphabet of size q. Suppose the channel is used n times, with entanglement consumed in c of these uses. The resulting communication scheme can then be described entirely classically as a length-n string in which $n-c$ symbols are drawn from an alphabet of size q, and c symbols are drawn from an alphabet of size q^2. An erasure on an unassisted channel use

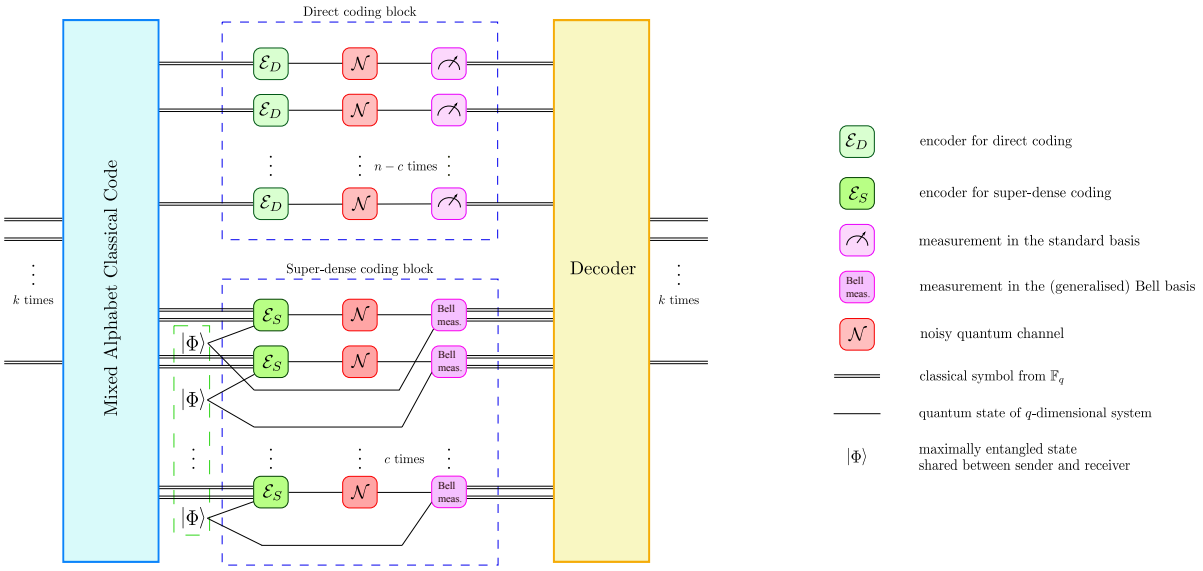

Figure 3.1: **The encoding and the decoding process.** The mixed-alphabet coding scheme where part of the information is transmitted directly and part via super-dense coding using shared entanglement. The receiver decodes the combined data to recover the original message.

removes one classical symbol, whereas an erasure on an EA use removes two classical symbols simultaneously. This setting is illustrated in Fig. 3.1.

The quantum communication task is therefore reduced to constructing classical codes over a mixed alphabet with a weighted erasure structure.

Code construction and the minimum distance. To construct such codes, we use a modified Reed–Solomon-type approach. Specifically, we consider all polynomials $f \in \mathbb{F}_q[x]$ of degree at most $k-1$ and evaluate them at n distinct points. These points are chosen such that $n_1 = n - c$ points lie in $\mathbb{F}_q$ and $n_2 = c$ points lie in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$. The resulting codewords consist of these evaluations, forming a mixed-alphabet code $[n, k, d; c]_q$ over $\mathbb{F}_q^{n-c} \times \mathbb{F}_{q^2}^c$, where d denotes the minimum distance of the code.

The minimum distance is determined by asking for the maximum number of evaluation points that are roots of a polynomial $f \in \mathbb{F}_q[x]$ of degree at most $k-1$. When $n_1 \geq k-1$, the minimum distance meets the classical Singleton bound 2.29. When $n_1 < k-1$, it exceeds it. In certain cases, entanglement enables our code to attain a substantially larger minimum distance than an equivalent code without entanglement assistance, thereby allowing it to correct more errors.

Why exceeding the classical Singleton bound is possible. Two structural features of the code construction allow for this. Firstly, from each conjugate pair $\{\gamma, \gamma^q\}$ in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$, only one element is chosen as an evaluation point. This prevents conjugate dependencies that would

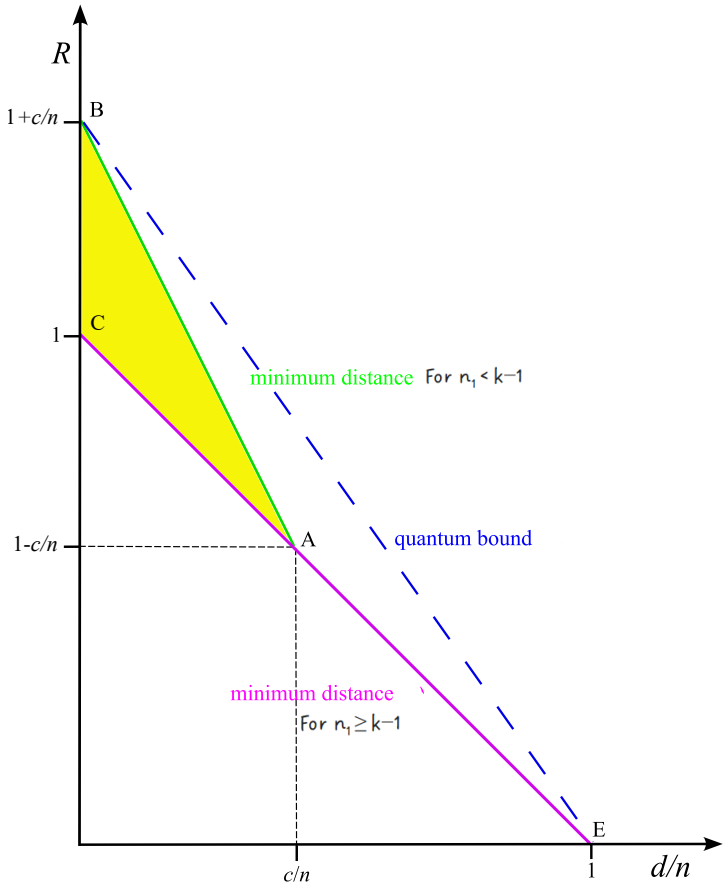

Figure 3.2: **Rate *vs* Distance**. In the asymptotic limit, the code rate $R = k/n$ of the mixed-alphabet Reed–Solomon code is analyzed as a function of the normalized minimum distance d/n. The line CE corresponds to the minimum distance for the case $n_1 \geq k - 1$, the line AB corresponds to the minimum distance for the case $n_1 < k - 1$.

otherwise reduce the minimum distance. Secondly, the number of evaluation points in $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ is maximized, subject to specific constraints. These choices together allow the mixed-alphabet structure brought about by entanglement assistance to strengthen the code beyond what is possible, classically. This behavior is reflected in Fig. 3.2 : all parameter points in the region ABC lie above the classical Singleton limit, while the line AE corresponds to the regime in which the minimum distance meets the Singleton bound with equality. It is worth noting that directly employing EAQECCs for classical transmission would be suboptimal in this setting, as their parameters remain constrained by the classical Singleton bound. Also, surpassing this bound in our construction is not simply a consequence of entanglement, but results from the way it is structurally incorporated into the mixed-alphabet coding framework.

Rates larger than one. In a purely classical setting, the rate satisfies $R = k/n \leq 1$. In contrast, whenever $c > 0$, our construction allows for $k > n$ while maintaining injectivity of

the encoding map. This follows from the fact that for $\gamma \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, $f(\gamma^q) = f(\gamma)^q$. Thus, for the receiver, knowledge of the codeword component at γ implies knowledge of the evaluation at its conjugate γ^q as well. The region ABC in Fig. 3.2 includes all achievable parameter points, covering both rates above one and rates below one. Specifically, the achievable rate is represented by the line segment AE when $n_1 \geq k - 1$, and by the line segment BA when $n_1 < k - 1$. The availability of entanglement is precisely what enables these elevated rates, which lie beyond the classical limit in this parameter regime.

Bounds. The next step is to evaluate our code against bounds derived in this work, which is essential in coding theory to understand how close a code comes to fundamental performance limits. We establish Singleton-like bounds specific to our EACC setting. In particular, we consider two bounds: the *block error bound*, which is obtained by treating each codeword symbol as a block and asking "how many erasures per block can be handled?", and the *quantum bound*, obtained by adapting an existing hybrid classical-quantum coding bound [59] to our scenario, which constrains the improvements in dimension and minimum distance achievable with entanglement assistance. These bounds are illustrated in Fig. 3.2. The line segments BA and AE align with the block error bound, while rates along the line segment BE, corresponding to the quantum bound, are achievable only for specific parameter choices. This identifies the ranges of n, k, and c where the code is optimal.

Finally, in contrast to prior work assuming either zero or unlimited entanglement, this framework accommodates flexible use of entanglement. Since the construction is based on super-dense coding, it relies on a standard and experimentally accessible primitive. More broadly, it illustrates how entanglement can enhance finite-length communication protocols.

3.2 Certifying semi-device independent security via wave particle duality relations

Essentially, this work establishes a direct operational link between WPD and SDI security. It shows that the SDI security witness can be expressed entirely in terms of two complementary interferometric quantities: visibility and distinguishability. This gives the witness a direct interpretation in terms of interferometric complementarity and allows for certifying security from experimentally accessible wave-particle quantities. The theoretical framework is supported by a proof-of-principle experiment and extended beyond the two-path case.

The main insights from the paper are as follows.

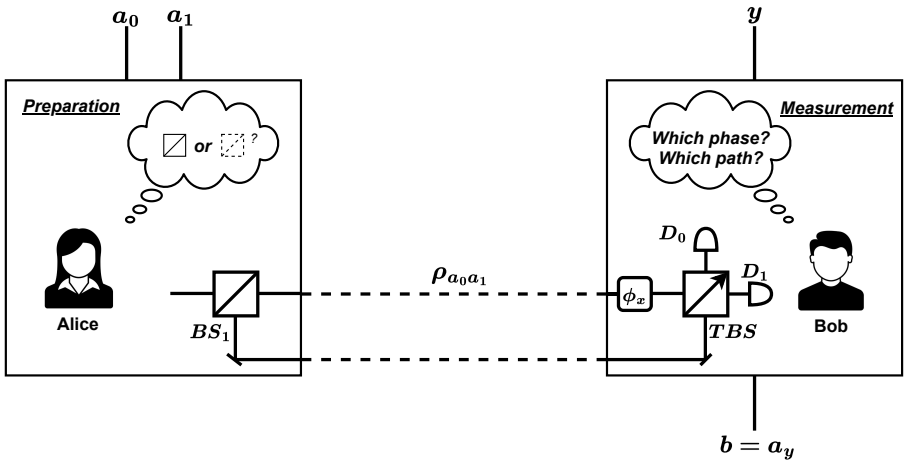

Figure 3.3: **SDI witness and wave-particle game.** In the preparation stage, Alice is given two classical bits (a_0, a_1), which she encodes into a two-dimensional quantum state $\rho_{a_0a_1}$ using an interferometric scheme. This encoding depends on whether an unbiased beam splitter BS_1 is inserted or not in the preparation of the computational basis states. The encoded state then undergoes a phase shift ϕ_x before reaching Bob. In the measurement stage, Bob performs a measurement determined by his input, using a tunable beam splitter (TBS) in his setup. By adjusting this element, he can access configurations that reveal either path information or interference. However, due to wave-particle duality and complementarity, these two types of information cannot be obtained simultaneously with arbitrary precision. This trade-off is quantified by the path distinguishability $\mathcal{D}$ and the visibility $\mathcal{V}$, which together form the basis for evaluating the SDI witness.

Theory

Turning SDI into a wave-particle game. We view the prepare and measure SDI protocol as a WPD game realised within a MZI. The core idea is to map Alice's inputs (a_0, a_1) according to parity; even parity $a_0 = a_1$ corresponds to particle-like experiments in which the path information is accessible when the first beam splitter is removed or the paths are blocked, while odd parity $a_0 \neq a_1$ corresponds to wave-like experiments, in which interference appears when the beam splitter is present. Using the four-state encoding 2.32 familiar from BB84 , which arises from the interferometric structure (path states and their superpositions), this parity mapping provides a clear separation between experiments testing distinguishability and those testing visibility. Distinguishability $\mathcal{D}$ (quantifying path knowledge) and Visibility $\mathcal{V}$ (quantifying interference strength) are then defined directly in terms of the conditional probabilities in the PM scenario, allowing for the SDI witness S (2.33) discussed earlier, to be rewritten accordingly. Optimizing over the interferometric phase, which controls interference, the witness decomposes into a sum of distinguishabilities for particle-like configurations and visibilities for wave-like ones. This gives the SDI witness a direct physical interpretation as the total accessible wave and particle behavior in the experiment. Therefore, certifying security is

equivalent to quantifying the optimal trade-off between these complementary quantities. This is illustrated in Fig. 3.3.

Higher dimensional generalisation. Extending the connection between SDI and the WPD game beyond two paths to a d-path interferometer introduces three key elements. First, we restrict to symmetric beam splitters, which ensures a clean operational definition of the experiments, since visibility is not uniquely defined in higher dimensions. In this setting, particle-like experiments are described using the computational basis, which encodes path information, while wave-like experiments are described using the Fourier basis, which generates interference. Second, the encoding is generalized: the four BB84 states are replaced by $2d$ well-defined interferometric preparations, forming a natural $(2 \to 1, d)$ RAC scenario, with a modulo-d parity rule separating them into particle-like and wave-like experiments. Third, a dimension-dependent complementarity bound emerges:

$$\mathcal{D} + \mathcal{V} \leq \frac{d - 2 + \sqrt{d}}{d - 1}. \tag{3.1}$$

Classical systems satisfy $\mathcal{D} + \mathcal{V} \leq 1$, while quantum systems can exceed this up to a tight limit determined by the optimal $(2 \to 1, d)$ RAC, establishing a nontrivial trade-off between distinguishability and visibility.

SDI Witness illustrated with a tunable interferometer. The next goal is to illustrate this general framework with a concrete example. We consider a photonic MZI equipped with a TBS, an input 50:50 beam splitter, and a controllable phase shift. We show how the SDI witness can be interpolated directly from the observed interferometric data, linking the measured visibility and distinguishability to the witness value. We use the symmetries in the experimental setup, combined with parity-oblivious encoding and selective path blocking to simplify the analysis and isolate particle-like and wave-like contributions. This gives us :

$$\max_{\phi_x} S_{\phi_x} = 2(\mathcal{D} + \mathcal{V}). \tag{3.2}$$

Experiment

The theoretical framework developed in this work was tested in a proof-of-principle experiment carried out by our collaborators.

Experimental validation. The implementation used a fiber-optical MZI in which orbital angular momentum (OAM) states of light were coupled into a few-mode fiber, with two guided modes defining the interferometric paths.

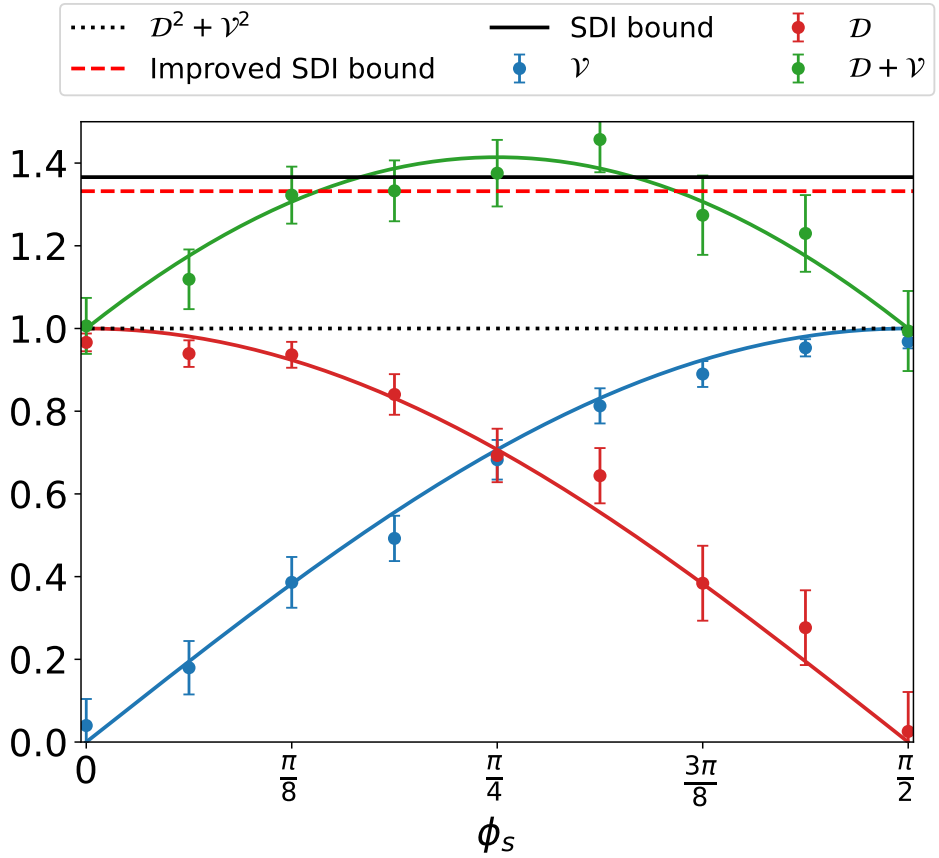

Figure 3.4: **SDI witness and security interplay** The curves show the behaviour of the visibility $\mathcal{V}$ and distinguishability $\mathcal{D}$, together with the corresponding SDI witness $S/2 = (\mathcal{D}+\mathcal{V})$. The classical limit is indicated (dotted black line), along with the security thresholds, including the improved SDI bound derived in this work. The figure illustrates that a violation of the classical limit, and hence certification of security requires a balanced contribution from both visibility and distinguishability.

Experimental probing of the SDI witness: wave-particle and entropic perspectives. Visibility $\mathcal{V}$ was obtained by scanning the interferometric phase, while path distinguishability $\mathcal{D}$ was measured by selective blocking of one arm of the interferometer. These measurements allow the reconstruction of the SDI witness S in terms of the relation between $\mathcal{D}$ and $\mathcal{V}$. The experimental data confirmed the theoretical prediction that a violation of the classical bound cannot be achieved through purely wave-like ($\mathcal{V} = 1$) or purely particle-like ($\mathcal{D} = 1$) behavior alone. Instead, a balanced contribution of both aspects is required, with the optimal violation occurring near $\mathcal{D} = \mathcal{V} = 1/\sqrt{2}$. In the wave-particle picture, the condition for secure communication proposed in Ref. [64], takes the form $\mathcal{D}+\mathcal{V} > 1.366$, corresponding to $S > 2.732$. In this work, we establish a refined bound, $\mathcal{D} + \mathcal{V} > 1.332$ (i.e., $S > 2.664$), which lowers the threshold and thereby increases the range of experimental parameters under which the SDI

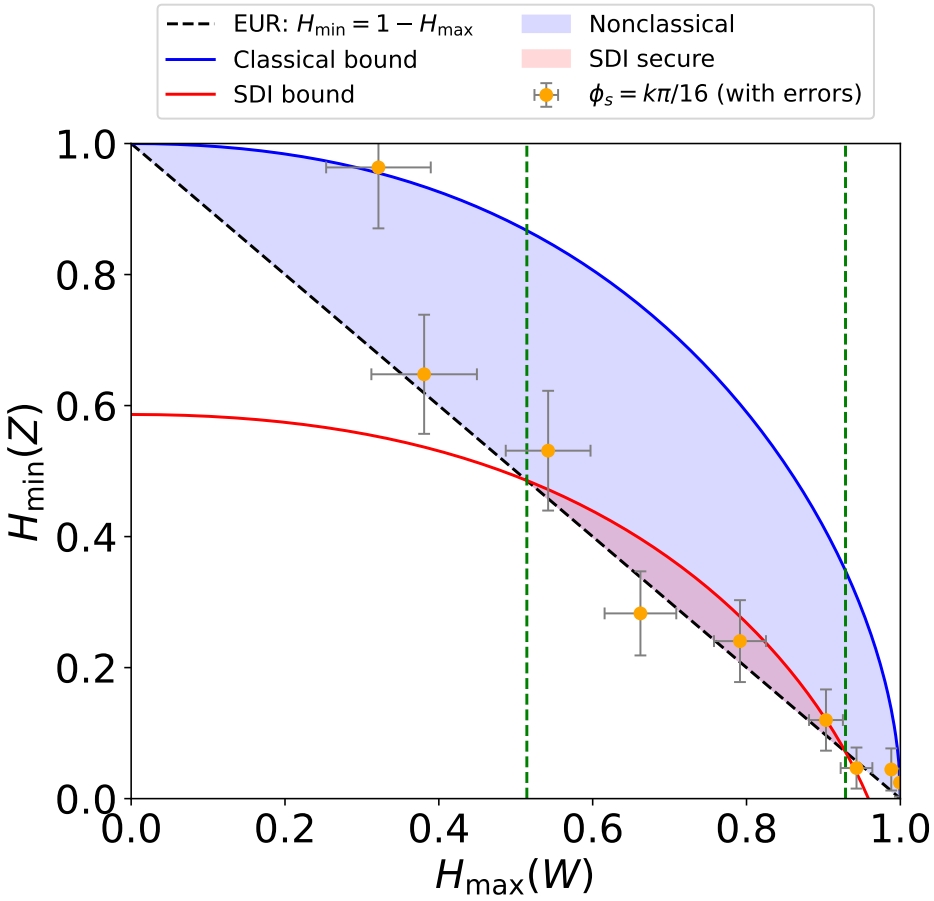

Figure 3.5: **Entropic representation of SDI security.** The figure shows the relevant regions in the $(H_{\max}(W), H_{\min}(Z))$ plane. The EUR defines the physically allowed region. Within this, the classical boundary separates correlations that can be reproduced with classical resources from those exhibiting quantum advantage. The SDI security bound further identifies the subset of correlations for which secure key generation is possible. The overlap between these constraints determines the regime where security can be certified.

witness can certify security. See Fig. 3.4.

Since WPDRs are operationally equivalent to EURs, the SDI witness can also be naturally reformulated within an entropic framework. This perspective is particularly important in the context of quantum cryptography, where security is fundamentally quantified in terms of entropic quantities. In this description, $\mathcal{D}$ and $\mathcal{V}$ map to the min- and max-entropies of complementary observables, which quantify an adversary's optimal guessing probability of the raw key. Using the theoretical relations derived in this work, the SDI witness and its classical bound ($S \leq 2$) can therefore be rewritten in the $(H_{\min}, H_{\max})$ plane, where the EUR $H_{\min}(Z) + H_{\max}(W) \geq 1$ defines the physically allowed region. The experimental data lie

within this region and intersect the domain corresponding to SDI security. In particular, the security condition derived in this work, $S \gtrsim 2.664$, is satisfied for values of the max-entropy in the interval $H_{\max}(W) \in [0.5144, 0.9287]$, showing that SDI key generation is possible for experimentally accessible parameters. Fig. 3.5 illustrates this.

This work thus shows that the SDI witness can be understood both through WPD and entropic uncertainty, with quantum advantage arising from a balanced interplay between these complementary aspects. This link offers a clear and intuitive way to understand SDI security, while also providing a framework that can be tested experimentally in real quantum communication setups.

3.3 Entanglement is not sufficient for most practical entanglement-based QKD protocols

In this work we introduce a general framework that handles classical side channel leakage in EB-QKD protocols. The framework allows one to derive upper bounds on the achievable key rate when such a leakage is present. We find that entanglement is not sufficient to guarantee secure key generation in the presence of even an arbitrarily small amount of leakage. As a result, there is a fundamental separation between entanglement and secret key distillation, with important implications for the scalability of practical QKD systems.

The main essence of the paper can be expressed in the following steps.

Framework. The framework considers classical side-channel leakage as additional information available to an adversary during the protocol and applies to standard EB-QKD schemes in which the devices are trusted (the DD setting), and the secret key is extracted directly from measurement outcomes together with public communication. These are often called quantum-memoryless protocols, since they do not require quantum storage or iterative quantum operations. More complex protocols [38] that rely on additional quantum processing fall outside the scope of this approach. By focusing on this class of protocols, the framework provides a general and protocol-independent treatment of leakage effects in practical QKD implementations.

The bipartite setting. We consider two parties sharing a two-qubit isotropic state ρ_v (see eq. 2.2) and attempting to extract a key in the presence of classical side-channel leakage, where $\mathcal{L}$ denotes the probability that a given round's measurement outcomes are leaked to the adversary. The state is written as a convex combination of a maximally entangled state and a separable ("junk") component, enabling Eve to implement a C.C. attack by distributing classical correlations in the separable part while exploiting leakage. By further reassigning a fraction of events to minimize the intrinsic information between the honest parties, Eve can completely destroy secrecy. The main result identifies explicit thresholds on the visibility v

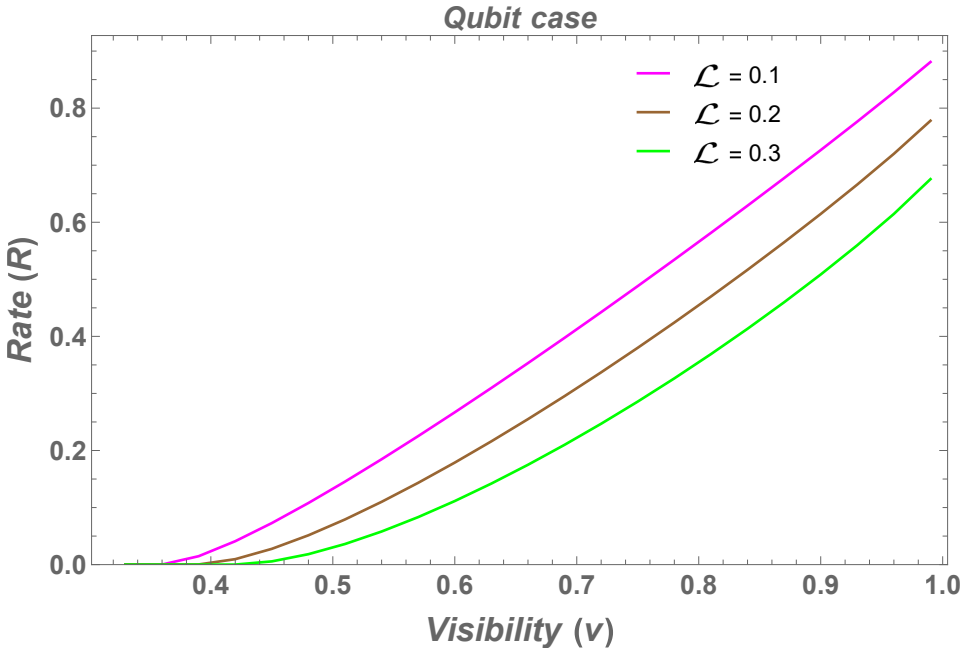

Figure 3.6: **Key rate *vs* Visibility.** Under the uniform leakage model, the curves show upper bounds on the secure key rate for protocols with publicly announced measurement inputs across different leakage scenarios.

below which no key can be extracted: for **uniform leakage**, where outcomes leak independently in every round with probability $\mathcal{L}$, security is impossible whenever

$$v \leq \frac{1}{3} + \frac{2\mathcal{L}}{3 - 2\mathcal{L}}, \tag{3.3}$$

while for **leakage only from the "junk" (separable) part**, where leakage occurs only in rounds that do not contribute to key generation, the threshold becomes

$$v \leq \frac{1}{3} + \frac{2\mathcal{L}}{3(\mathcal{L} + 3)}. \tag{3.4}$$

In both cases, these bounds lie strictly above the entanglement threshold $v = 1/3$, showing that even an arbitrarily small leakage ($\mathcal{L} > 0$) creates a gap between entanglement and key distillability. Figure 3.6 illustrates these upper bounds on the key rate versus visibility v for different leakage values in the bipartite qubit case.

Generalisation to arbitrary dimension and number of parties. The above reasoning extends directly to the general multipartite setting with arbitrary local dimension. In place of the two-qubit isotropic states, one considers their natural generalisation (see eq. 2.3) to N-partite d-dimensional isotropic states.

We identify the following visibility thresholds for which no secret key can be extracted. For **uniform leakage**, this occurs whenever

$$v \leq \frac{1}{1+d^{N-1}} + \frac{d^{N-1}\mathcal{L}}{(1+d^{N-1})(1-\mathcal{L})+\mathcal{L}}, \tag{3.5}$$

while for **leakage only from the "junk" part**, the corresponding threshold is

$$v \leq \frac{1}{1+d^{N-1}} + \frac{d^{N-1}\mathcal{L}}{(1+d^{N-1})(\mathcal{L}+1+d^{N-1})}. \tag{3.6}$$

As in the bipartite case, these thresholds lie strictly above the separability threshold, showing that the gap between entanglement and key distillability persists for arbitrary dimension and number of parties.

Examples. As concrete examples of our general framework, we compute upper bounds on the secret-key rate for isotropic states in the cases $d = 3, N = 2$ and $d = 2, N = 3$. These bounds are derived by identifying the optimal C.C. attack that an eavesdropper could implement, under the assumption that the parties perform arbitrary projective measurements on their subsystems.

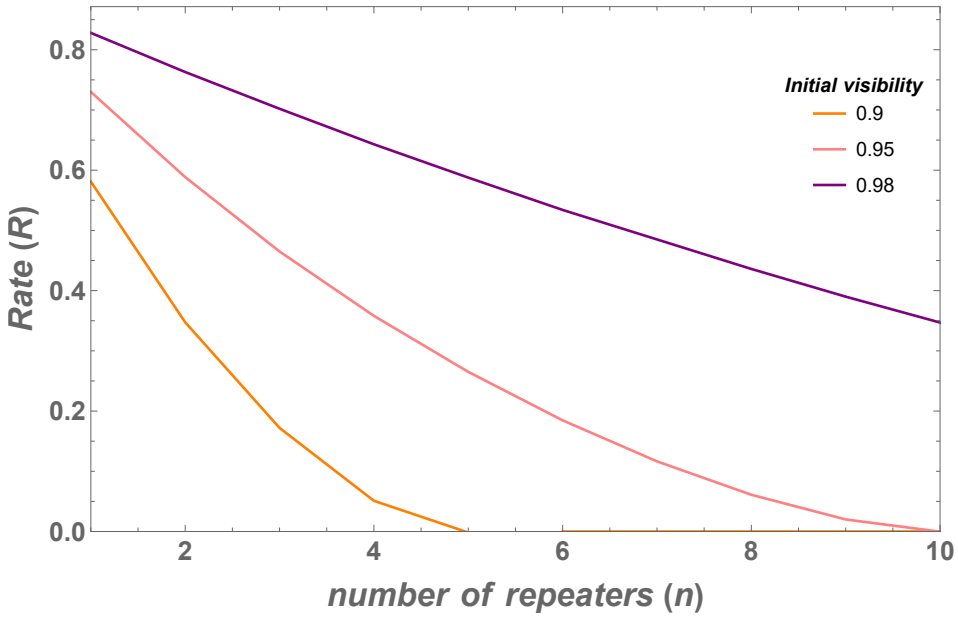

Figure 3.7: **Key rate *vs* Number of repeaters.** Dependence of the secure key rate R on the number of repeaters n for uniform leakage, illustrating its rapid degradation across different leakage scenarios.

Applications. We now apply the bound in eq. (3.3) to repeater-based QKD. In a chain of n quantum repeaters, each entanglement swapping step reduces the visibility of the shared

isotropic state. Specifically, if each elementary link has visibility v, the effective visibility between the end parties after n repeaters becomes v^{2n}. Using (3.3), this directly limits the number of repeater nodes compatible with secure key generation:

$$n_{\max} \leq \frac{\log_2\left(\frac{1}{3} + \frac{2\mathcal{L}}{3-2\mathcal{L}}\right)}{2\log_2 v}. \tag{3.7}$$

While in an idealised, error-free scenario any standard protocol would allow arbitrarily many repeaters, even modest imperfections significantly restrict scalability. For instance, with $v = 0.95$ and $\mathcal{L} = 0.1$, secure key generation is limited to at most ten repeaters. This demonstrates the extreme sensitivity of long-distance repeater-based QKD to small preparation errors. Key rates computed under the optimal C.C. attack show a rapid decrease with increasing n, as illustrated in Fig. 3.7.

Our results thus show a fundamental limitation of entanglement as a cryptographic resource, showing that it does not by itself guarantee secure key generation in practical QKD.

Chapter 4

Outlook

The results presented in this thesis contribute to a growing understanding of quantum resources from an operational perspective. By studying entanglement and complementarity in concrete communication and cryptographic tasks, we have seen both their power and limitations in realistic settings.

At the same time, a recurring theme has been that their usefulness depends on the context. A resource-based strong advantage at the level of abstract theory does not always translate directly into an advantage in realistic scenarios. Bridging this gap between theoretical insight and practical implementation is one of the central challenges in quantum information science, and it is precisely where many interesting open problems lie.

This is particularly evident in the context of EA communication. While it is well understood that entanglement can enhance communication capabilities, sometimes dramatically, much of this understanding is still rooted in general bounds and existence results. In contrast, explicit constructions that can be implemented, analyzed, and optimized for realistic settings are far fewer. The work presented in this thesis takes a step in this direction by providing constructive coding schemes for EACC, showing concretely how entanglement can improve both error correction and transmission rates.

Looking forward, an important direction is to better understand how far such advantages can be pushed and under what constraints. In particular, while our construction already surpasses classical limits, there remain regions of the rate-distance trade-off (specifically the region BAE, see Fig. 3.2) that are not yet accessible through current constructions. Finding new coding schemes that can reach these areas or proving fundamental limitations that prevent this would deepen our understanding of the role of entanglement in communication. More broadly, extending these constructions beyond the current framework by considering different types of classical codes or alternative error models could lead to more adaptable and practically relevant

protocols.

Closely related to this is ongoing work that revisits the fundamental limits themselves from a constructive viewpoint. Recent results have shown that the entropic quantum Singleton bounds [40] are tight via a space-sharing argument, including in the setting of EACC [80]. Building on this, we aim to better understand how these tight bounds manifest in explicit protocols, and how they are affected by more realistic constraints, such as distributing entanglement across multiple encoders with only local operations available. Developing such refined bounds, together with explicit constructions that approach them, is an important step towards a more complete treatment of EA communication.

Another promising direction is the development of hybrid communication schemes [41] that simultaneously transmit classical and quantum information. Combining our present approach with existing EA quantum codes may lead to improved protocols.

From a different angle, the results on complementarity highlight how ideas that were once seen as purely foundational can acquire a clear operational meaning. In this thesis, we showed that WPD can be directly connected to SDI security, by expressing the SDI security witness in terms of experimentally accessible quantities such as visibility and distinguishability, or equivalently through entropic measures. This creates a bridge between abstract principles and practical protocols, making complementarity a principle that can be used rather than just interpreted.

Looking ahead, several natural questions arise. One important direction is to understand whether this interferometric viewpoint can offer concrete advantages in realistic implementations. In practice, experiments are affected by losses, detector inefficiencies, and no-click events [20], and it remains to be seen how this approach performs under such imperfections. Addressing these issues is essential if these ideas are to move beyond proof-of-principle demonstrations.

Another challenge is to extend these results to higher-dimensional systems. A fully general formulation of SDI-QKD in arbitrary dimensions remains technically challenging [70], especially when one seeks closed-form key-rate expressions or operational definitions of visibility and distinguishability for arbitrary interferometers. These difficulties stem from the fact that, in multipath setups [23], the definitions of these quantities depend on the specific beam-splitter configurations employed, and addressing them effectively involves solving multiple open problems in SDI-QKD and EUR frameworks.

Finally, our results on the role of entanglement in QKD emphasize that understanding the limitations of quantum resources is just as important as understanding their advantages. We showed that entanglement alone is not sufficient for secure key generation in the presence of even minimal classical leakage, revealing a clear gap between entanglement and key extractability. This challenges a widely held intuition and calls for a more refined understanding of what actually enables security in practice.

An important open problem in this direction is to identify general criteria that distinguish

entangled states that can be used for key generation from those that cannot under realistic conditions. Such a characterization would go beyond entanglement itself and point towards more operationally meaningful quantities.

Another natural direction is to consider stronger and more general adversarial strategies [1, 67, 69]. While the present work focuses on relatively simple leakage models, more sophisticated attacks may reveal even stronger limitations. Understanding the full extent of these effects is essential for assessing how robust practical QKD protocols really are. These questions become especially relevant when considering large-scale quantum networks.

Taken together, these directions point toward a broader goal: to better understand quantum resources in realistic settings, where their advantages, trade-offs, and limitations all come into play. The results of this thesis offer a few steps in this direction.

Bridging the gap between foundational principles and practical implementations remains a challenge in quantum information science. By continuing to study quantum resources through concrete tasks in scommunication and cryptography we can hope not only to gain a deeper understanding of quantum theory, but also to inform the development of future quantum technologies.

Bibliography

[1] A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani, *Device-independent security of quantum cryptography against collective attacks*, Phys. Rev. Lett., 98 (2007), p. 230501.

[2] A. Acín, N. Gisin, and L. Masanes, *From bell's theorem to secure quantum key distribution*, Phys. Rev. Lett., 97 (2006), p. 120405.

[3] M. Ardehali, *Quantum cryptography based on wheeler's delayed choice experiment*, Physics Letters A, 217 (1996), pp. 301–304.

[4] K. Azuma, S. E. Economou, D. Elkouss, P. Hilaire, L. Jiang, H.-K. Lo, and I. Tzitrin, *Quantum repeaters: From quantum networks to the quantum internet*, Rev. Mod. Phys., 95 (2023), p. 045006.

[5] A. Baliuka, M. Stöcker, M. Auer, P. Freiwang, H. Weinfurter, and L. Knips, *Deep-learning-based radio-frequency side-channel attack on quantum key distribution*, Phys. Rev. Appl., 20 (2023), p. 054040.

[6] J. S. Bell, *On the einstein podolsky rosen paradox*, Physics Physique Fizika, 1 (1964), pp. 195–200.

[7] C. Bennett, P. Shor, J. Smolin, and A. Thapliyal, *Entanglement-assisted capacity of a quantum channel and the reverse shannon theorem*, IEEE Transactions on Information Theory, 48 (2002), pp. 2637–2655.

[8] C. H. Bennett, *Quantum cryptography using any two nonorthogonal states*, Phys. Rev. Lett., 68 (1992), pp. 3121–3124.

[9] C. H. Bennett and G. Brassard, *Quantum cryptography: Public key distribution and coin tossing*, Theoretical Computer Science, 560 (2014), pp. 7–11.
Theoretical Aspects of Quantum Cryptography – celebrating 30 years of BB84.

[10] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels*, Phys. Rev. Lett., 70 (1993), pp. 1895–1899.

[11] C. H. Bennett, G. Brassard, and N. D. Mermin, *Quantum cryptography without bell's theorem*, Phys. Rev. Lett., 68 (1992), pp. 557–559.

[12] C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, *Entanglement-assisted classical capacity of noisy quantum channels*, Phys. Rev. Lett., 83 (1999), pp. 3081–3084.

[13] C. H. Bennett and S. J. Wiesner, *Communication via one- and two-particle operators on einstein-podolsky-rosen states*, Phys. Rev. Lett., 69 (1992), pp. 2881–2884.

[14] M. Berta, M. Christandl, R. Colbeck, J. M. Renes, and R. Renner, *The uncertainty principle in the presence of quantum memory*, Nature Physics, 6 (2010), pp. 659–662.

[15] N. Bohr, *The quantum postulate and the recent development of atomic theory1*, Nature, 121 (1928), pp. 580–590.

[16] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, *Quantum repeaters: The role of imperfect local operations in quantum communication*, Phys. Rev. Lett., 81 (1998), pp. 5932–5935.

[17] T. Brun, I. Devetak, and M.-H. Hsieh, *Correcting quantum errors with entanglement*, Science, 314 (2006), pp. 436–439.

[18] D. Bruss, *Optimal eavesdropping in quantum cryptography with six states*, Phys. Rev. Lett., 81 (1998), pp. 3018–3021.

[19] P. Busch and C. Shilladay, *Complementarity and uncertainty in mach–zehnder interferometry and beyond*, Physics Reports, 435 (2006), pp. 1–31.

[20] A. Chaturvedi, M. Ray, R. Veynar, and M. Pawłowski, *On the security of semi-device-independent QKD protocols*, Quantum Inf. Process., 17 (2018), p. 131.

[21] E. Chitambar and G. Gour, *Quantum resource theories*, Rev. Mod. Phys., 91 (2019), p. 025001.

[22] P. J. Coles, *Role of complementarity in superdense coding*, Phys. Rev. A, 88 (2013), p. 062317.

[23] P. J. Coles, *Entropic framework for wave-particle duality in multipath interferometers*, Phys. Rev. A, 93 (2016), p. 062111.

[24] P. J. Coles, M. Berta, M. Tomamichel, and S. Wehner, *Entropic uncertainty relations and their applications*, Rev. Mod. Phys., 89 (2017), p. 015002.

[25] P. J. Coles, J. Kaniewski, and S. Wehner, *Equivalence of wave-particle duality to entropic uncertainty*, Nat. Commun., 5 (2014), p. 5814.

[26] M. Curty, M. Lewenstein, and N. Lütkenhaus, *Entanglement as a precondition for secure quantum key distribution*, Phys. Rev. Lett., 92 (2004), p. 217903.

[27] N. Datta and M.-H. Hsieh, *One-shot entanglement-assisted quantum and classical communication*, IEEE Transactions on Information Theory, 59 (2013), pp. 1929–1939.

[28] J. DeFranco and A. Nemec, *Entanglement-assisted codes outside the stabilizer framework*, 2026.

[29] I. Devetak, A. W. Harrow, and A. Winter, *A family of quantum protocols*, Phys. Rev. Lett., 93 (2004), p. 230504.

[30] I. Devetak and P. W. Shor, *The capacity of a quantum channel for simultaneous transmission of classical and quantum information*, Commun. Math. Phys., 256 (2005), pp. 287–303.

[31] W. Diffie and M. E. Hellman, *New directions in cryptography*, IEEE Transactions on Information Theory, IT-22 (1976), pp. 644–654.

[32] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, *Long-distance quantum communication with atomic ensembles and linear optics*, Nature, 414 (2001), pp. 413–418.

[33] W. Dür and J. I. Cirac, *Classification of multiqubit mixed states: Separability and distillability properties*, Physical Review A, 61 (2000), p. 042314.

[34] A. Einstein, B. Podolsky, and N. Rosen, *Can quantum-mechanical description of physical reality be considered complete?*, Phys. Rev., 47 (1935), pp. 777–780.

[35] A. K. Ekert, *Quantum cryptography based on bell's theorem*, Phys. Rev. Lett., 67 (1991), pp. 661–663.

[36] B.-G. Englert, *Fringe visibility and which-way information: An inequality*, Phys. Rev. Lett., 77 (1996), pp. 2154–2157.

[37] Y. Fujiwara, D. Clark, P. Vandendriessche, M. De Boeck, and V. D. Tonchev, *Entanglement-assisted quantum low-density parity-check codes*, Phys. Rev. A, 82 (2010), p. 042338.

[38] D. Gottesman and H.-K. Lo, *Proof of security of quantum key distribution with two-way classical communications*, IEEE Transactions on Information Theory, 49 (2003), pp. 457–475.

[39] M. Grassl, T. Beth, and T. Pellizzari, *Codes for the quantum erasure channel*, Phys. Rev. A, 56 (1997), pp. 33–38.

[40] M. Grassl, F. Huber, and A. Winter, *Entropic proofs of singleton bounds for quantum error-correcting codes*, IEEE Transactions on Information Theory, 68 (2022), pp. 3942–3950.

[41] M. Grassl, S. Lu, and B. Zeng, *Codes for simultaneous transmission of quantum and classical information*, in 2017 IEEE International Symposium on Information Theory (ISIT), 2017, pp. 1718–1722.

[42] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, *Secure key from bound entanglement*, Phys. Rev. Lett., 94 (2005), p. 160502.

[43] K. Horodecki, M. Winczewski, and S. Das, *Fundamental limitations on the device-independent quantum conference key agreement*, Phys. Rev. A, 105 (2022), p. 022604.

[44] M. Horodecki, P. Horodecki, and R. Horodecki, *Separability of mixed states: necessary and sufficient conditions*, Physics Letters A, 223 (1996), pp. 1–8.

[45] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, *Quantum entanglement*, Rev. Mod. Phys., 81 (2009), pp. 865–942.

[46] M.-H. Hsieh, I. Devetak, and T. Brun, *General entanglement-assisted quantum error-correcting codes*, Phys. Rev. A, 76 (2007), p. 062313.

[47] M.-H. Hsieh and M. M. Wilde, *Trading classical communication, quantum communication, and entanglement in quantum Shannon theory*, IEEE Transactions on Information Theory, 56 (2010), pp. 4705–4730.

[48] M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, *"event-ready-detectors" bell experiment via entanglement swapping*, Phys. Rev. Lett., 71 (1993), pp. 4287–4290.

[49] V. Jacques, E. Wu, F. Grosshans, F. Treussart, P. Grangier, A. Aspect, and J.-F. Roch, *Experimental realization of Wheeler's delayed-choice gedanken experiment*, Science, 315 (2007), pp. 966–968.

[50] G. Jaeger, A. Shimony, and L. Vaidman, *Two interferometric complementarities*, Phys. Rev. A, 51 (1995), pp. 54–67.

[51] B. King, A. Di Piazza, and C. H. Keitel, *A matterless double slit*, Nature Photonics, 4 (2010), pp. 92–94.

[52] M. Koashi, *Simple security proof of quantum key distribution based on complementarity*, New Journal of Physics, 11 (2009), p. 045018.

[53] H. K. Lo and H. F. Chau, *Unconditional security of quantum key distribution over arbitrarily long distances*, Science, 283 (1999), pp. 2050–2056.

[54] H.-K. Lo, M. Curty, and B. Qi, *Measurement-device-independent quantum key distribution*, Phys. Rev. Lett., 108 (2012).

[55] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, *Practical security bounds against the trojan-horse attack in quantum key distribution*, Phys. Rev. X, 5 (2015), p. 031030.

[56] K. Łukanowski, M. Balanzó-Juandó, M. Farkas, A. Acín, and J. Kołodyński, *Upper bounds on key rates in device-independent quantum key distribution based on convex-combination attacks*, Quantum, 7 (2023), p. 1199.

[57] F. MacWilliams and N. Sloane, *The Theory of Error-Correcting Codes*, Elsevier Science, 1978.

[58] V. Makarov, A. Anisimov, and J. Skaar, *Effects of detector efficiency mismatch on security of quantum cryptosystems*, Phys. Rev. A, 74 (2006), p. 022313.

[59] M. Mamindlapally and A. Winter, *Singleton bounds for entanglement-assisted classical and quantum error correcting codes*, IEEE Transactions on Information Theory, 69 (2023), pp. 5857–5868.

[60] L. Masanes, S. Pironio, and A. Acín, *Secure device-independent quantum key distribution with causally independent measurement devices*, Nat. Commun., 2 (2011), p. 238.

[61] U. Maurer and S. Wolf, *The intrinsic conditional mutual information and perfect secrecy*, in Proceedings of IEEE International Symposium on Information Theory, 1997, pp. 88–.

[62] A. Mizutani, T. Sasaki, G. Kato, Y. Takeuchi, and K. Tamaki, *Information-theoretic security proof of differential-phase-shift quantum key distribution protocol based on complementarity*, Quantum Science and Technology, 3 (2017), p. 014003.

[63] M. A. Nielsen, I. L. Chuang, and I. L. Chuang, *Quantum computation and quantum information, 10th anniversary ed.*, Cambridge University Press,, 10th ann. ed. ed., 2010.

[64] M. Pawłowski and N. Brunner, *Semi-device-independent security of one-way quantum key distribution*, Phys. Rev. A, 84 (2011), p. 010302.

[65] M. Pereira, M. Curty, and K. Tamaki, *Quantum key distribution with flawed and leaky sources*, NPJ Quantum Inf., 5 (2019).

[66] A. Peres, *Separability criterion for density matrices*, Phys. Rev. Lett., 77 (1996), pp. 1413–1415.

[67] C. Portmann and R. Renner, *Security in quantum cryptography*, Rev. Mod. Phys., 94 (2022), p. 025008.

[68] T. Prasad and M. Grassl, *Codes for entanglement-assisted classical communication*, NPJ Quantum Inf., 11 (2025).

[69] I. W. Primaatmaja, K. T. Goh, E. Y.-Z. Tan, J. T.-F. Khoo, S. Ghorai, and C. C.-W. Lim, *Security of device-independent quantum key distribution protocols: a review*, Quantum, 7 (2023), p. 932.

[70] C. Raj, T. Prasad, A. Chaturvedi, L. Pollyceno, D. Spegel-Lexne, S. Gómez, J. Argillander, A. Alarcón, G. B. Xavier, M. Pawłowski, and P. R. Dieguez, *Certifying semi-device-independent security via wave-particle duality experiments*, NPJ Quantum Inf., 12 (2025).

[71] R. L. Rivest, A. Shamir, and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, Commun. ACM, 21 (1978), pp. 120–126.

[72] S. Roman, *Coding and Information Theory*, Graduate texts in mathematics, Springer-Verlag, 1992.

[73] S. Sarkar, T. Prasad, and K. Horodecki, *Entanglement is not sufficient for most practical entanglement-based qkd protocols*, 2026.

[74] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, *The security of practical quantum key distribution*, Rev. Mod. Phys., 81 (2009), p. 1301.

[75] E. Schrödinger, *The present situation in quantum mechanics: A translation of Schrödinger's "cat paradox" paper*, Proceedings of the American Philosophical Society, 124 (1980), pp. 323–338.
Originally published in German in Naturwissenschaften, 1935.

[76] Z. Shadman, H. Kampermann, C. Macchiavello, and D. Bruss, *Optimal super dense coding over noisy quantum channels*, New Journal of Physics, 12 (2010), p. 073042.

[77] C. E. Shannon, *A mathematical theory of communication*, The Bell System Technical Journal, 27 (1948), pp. 379–423.

[78] P. W. Shor and J. Preskill, *Simple proof of security of the bb84 quantum key distribution protocol*, Phys. Rev. Lett., 85 (2000), pp. 441–444.

[79] D. Spegel-Lexne, S. Gómez, J. Argillander, M. Pawłowski, P. R. Dieguez, A. Alarcón, and G. B. Xavier, *Experimental demonstration of the equivalence of entropic uncertainty with wave-particle duality*, Science Advances, 10 (2024), p. eadr2007.

[80] H. Sun and S. A. Jafar, *On the capacity of erasure-prone quantum storage with erasure-prone entanglement assistance*, (2025).

[81] K. Tamaki, M. Curty, and M. Lucamarini, *Decoy-state quantum key distribution with a leaky source*, New J. Phys., 18 (2016), p. 065008.

[82] K. Tamaki, H.-K. Lo, and C.-H. F. Fung, *Decoy-state quantum key distribution with a biased basis choice and its application to the b92 protocol*, Physical Review A, 77 (2008), p. 032341.

[83] B. M. Terhal and K. G. H. Vollbrecht, *Entanglement of formation for isotropic states*, Phys. Rev. Lett., 85 (2000), pp. 2625–2628.

[84] G. THOMSON and A. REID, *Diffraction of cathode rays by a thin film*, Nature, 119 (1927), p. 890.

[85] R. Tirole, S. Vezzoli, E. Galiffi, I. Robertson, D. Maurice, B. Tilmann, S. A. Maier, J. B. Pendry, and R. Sapienza, *Double-slit time diffraction at optical frequencies*, Nature Physics, 19 (2023), pp. 999–1002.

[86] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, *Tight finite-key analysis for quantum cryptography*, Nat. Commun., 3 (2012), p. 634.

[87] J. von Neumann, *Mathematical Foundations of Quantum Mechanics*, Princeton University Press, Princeton, NJ, 1955.
Translated from the 1932 German edition: Mathematische Grundlagen der Quantenmechanik.

[88] R. F. Werner, *Quantum states with einstein-podolsky-rosen correlations admitting a hidden-variable model*, Journal of Mathematical Physics, 28 (1987), pp. 1529–1535.

[89] R. F. Werner, *All teleportation and dense coding schemes*, Journal of Physics A: Mathematical and General, 34 (2001), p. 7081.

[90] S. Wiesner, *Conjugate coding*, SIGACT News, 15 (1983), p. 78–88.

[91] W. K. Wootters and W. H. Zurek, *A single quantum cannot be cloned*, Nature, 299 (1982), pp. 802–803.

[92] T. Young, *The bakerian lecture. experiments and calculations relative to physical optics*, Phil. Trans. R. Soc., 94 (1804), p. 1–16.

[93] V. Zapatero, T. van Leent, R. Arnon-Friedman, W.-Z. Liu, Q. Zhang, H. Weinfurter, and M. Curty, *Advances in device-independent quantum key distribution*, NPJ Quantum Inf., 9 (2023).

[94] X. Zhang, P. Zeng, T. Ye, H.-K. Lo, and X. Ma, *Quantum complementarity approach to device-independent security*, Phys. Rev. Lett., 131 (2023), p. 140801.

npj | quantum information

Article

Published in partnership with The University of New South Wales

https://doi.org/10.1038/s41534-024-00954-2

Codes for entanglement-assisted classical communication

Tushita Prasad ✉ & Markus Grassl

Entanglement-assisted classical communication (EACC) aims to enhance communication systems using entanglement as an additional resource. However, there is a scarcity of explicit protocols designed for finite transmission scenarios, which presents a challenge for real-world implementation. In response, we introduce a new EACC scheme capable of correcting a fixed number of erasures/errors. It can be adjusted to the available amount of entanglement and sends classical information over a quantum channel. We establish a general framework to accomplish such a task by reducing it to a classical problem. Comparing with specific bounds, we identify optimal parameter ranges. The scheme requires only the implementation of super-dense coding which has been demonstrated successfully in experiments. Furthermore, our results show that an adaptable entanglement use confers a communication advantage. Overall, our work sheds light on how entanglement can elevate various finite-length communication protocols, opening new avenues for exploration in the field.

Entanglement serves as a valuable resource in many quantum communication and quantum information processing tasks. Pre-existing entanglement can sometimes enhance the information transmission capabilities of quantum channels. One of the earliest results demonstrating this power of entanglement-assisted communication came in 1992. Wiesner introduced the technique of super-dense coding[1] in which a sender can communicate two classical bits while sending a single qubit across a noiseless quantum channel, provided they have pre-shared entanglement. Subsequently, Bennett et al.[2] showed that the classical capacity of some noisy quantum channels can be significantly increased with the assistance of unbounded pre-shared entanglement between the sender and the receiver. In 2002, Bowen[3] presented a class of entanglement-assisted (EA) quantum codes that achieve the quantum EA channel capacity when a certain amount of shared entanglement per channel use is provided. A few years later, Brun et al.[4] proved that assisting a quantum channel with entanglement allows quantum codes to have better parameters than codes not aided by entanglement.

So far, entanglement-assisted communication has been largely explored through an information-theoretic lens. This means, prominently questions on entanglement-aided capacities have been addressed[2,5–11]. For instance, Hsieh and Wilde[12] proved a capacity theorem establishing the maximum rate at which one can transmit classical and quantum information simultaneously across a noisy quantum channel supported by entanglement. Shadman and Bruß[10], on the other hand, consider a similar problem setting but focus on transmitting only classical information. They determine the super-dense coding capacity for specific resource states in the presence of noise. The interest in capacity questions is completely natural considering how the concept of capacity forms a central theme in information theory. Its significance can be seen in Shannon's noisy-channel coding theorem[13], a foundational result lying at the heart of information theory. Shannon showed that for a noisy channel, given an information transmission rate below capacity, the transmission error probability asymptotically tends to zero when the coding length increases.

The problem of reliable transmission of either classical or quantum information, or a combination of both, across n uses of a quantum channel with the help of entanglement has been explored from a coding theory perspective as well, although this approach has been much less prevalent. This perspective involves addressing the problem in a practical setting, defined by specific parameters like a fixed code length and a set of errors that can be perfectly corrected. Kremsky et al.[14] proposed a generalization of the stabilizer framework to capture entanglement-assisted hybrid codes. Here "hybrid" refers to the fact that these codes can transmit both classical and quantum information at the same time. The authors give examples of hybrid codes, but none that transmit only classical information. Their work primarily focuses on establishing a framework and conditions for error correction without addressing how to find codes that meet these conditions. Also, they do not connect the parameters of the code described in their "extended stabilizer formalism" with the properties of the corresponding classical codes. In particular, there are no constructions in the literature for codes designed for entanglement-assisted classical communication.

While considerable attention has been devoted to exploring EA quantum codes, the exploration of EA classical codes has been notably scarce. A common assumption is that an unlimited amount of entanglement

International Centre for Theory of Quantum Technologies, University of Gdańsk, Jana Bażyńskiego 1A, 80-309 Gdańsk, Poland.
✉e-mail: tushita.prasad@phdstud.ug.edu.pl

can be used, but the question of less entanglement has, for example, been considered in ref. 3. Directly using EA quantum codes to transmit classical information is inferior to the solution we present here. This is related to the fact that the parameters $[[n, k, d; c]]_q$ of an EA quantum code obey the classical Singleton bound $d \leq n-k+1$ given in Eq. (3) below[15], while our codes can exceed that bound.

Addressing these aspects, in this paper, we present an explicit encoding scheme that can transmit classical information using a qudit channel n times assisted by $c \leq n$ maximally entangled qudit pairs when, at most, $d-1$ erasures occur. We demand perfect error correction, i.e., the probability of error after decoding should be zero. Our scheme is "explicit" in the sense that we provide a construction method that works for all parameters within a certain range and allows us to easily deduce the parameters of the resulting code.

The flow of the paper is as follows. First, the task of transmitting classical information over a quantum channel using maximally entangled pairs is simplified by reducing it to a classical one. We then present an explicit encoding scheme, offering practical methods for creating directly implementable codes. Following this, we derive Singleton-like bounds, compare our scheme to these bounds, and identify parameter ranges where the scheme is optimal. We then analyze how our proposed EACC scheme surpasses classical protocols in terms of error correction capability and information transfer rate. Finally, we conclude by discussing potential future directions and implications of our work.

Results

Reduction to a classical problem

Let q be the dimension of the quantum system associated with the quantum channel. We distinguish two cases. If we do not have entanglement available, for each use of the quantum channel we can send q mutually orthogonal states over the channel (one at a time), and the receiver measures in the corresponding basis. In case we have entanglement available, we can send q^2 different messages per use of the channel with the super-dense coding protocol[16] which requires one maximally entangled pair for each single transmission. This allows for our problem to be translated to a classical one. The amalgamation of direct coding and super-dense coding results in a combination of classical channels: $n-c$ classical channels transmitting one symbol each and c classical channels transmitting two symbols each. Each of the c symbols being communicated via the super dense-coding protocol can be interpreted as two symbols from an alphabet containing q letters. The problem now reduces to finding an encoding of messages into a string of n symbols, where $n-c$ of them come from an alphabet $\mathcal{A}_q$ with q letters and c symbols are from the alphabet $\mathcal{A}_{q^2} = \mathcal{A}_q \times \mathcal{A}_q$ with q^2 letters. An erasure during a single transmission in the context of a super-dense coding scheme implies that two classical symbols are erased, otherwise a single symbol is considered to be erased. The setting is illustrated in Fig. 1. In the extremal case of $c = 0$ we can use a classical error-correcting code over the alphabet $\mathcal{A}_q$. When $n = c$ we can use a code over $\mathcal{A}_{q^2}$. The case of $n = c$ has been considered earlier in ref. 17, Proposition 11. We denote the code by $\mathcal{C} = [n, k, d; c]_q$, where n is the number of channel uses, and c is the amount of entanglement required by the code. The parameter d is the minimum distance of the code. A code with minimum distance d can correct a maximum of $d-1$ erasures or $\lfloor (d-1)/2 \rfloor$ errors. An erasure is an error at a known position[18]. Further, k is the dimension of the code, that is, q^k different classical messages can be sent across the channel. From here on, we assume q to be a power of prime. Lastly, the alphabets $\mathcal{A}_q = \mathbb{F}_q$ and $\mathcal{A}_{q^2} = \mathbb{F}_{q^2}$ are chosen to be finite fields with q elements and q^2 elements, respectively. For an introduction to finite fields and the basics of coding theory see, for example, ref. 19 or ref. 20.

Code construction

We use the following modified version of the concept of Reed–Solomon codes[21] to construct the code. Let $\mathbb{F}_q[x]$ denote the set of polynomials in x with coefficients in $\mathbb{F}_q$ and let $\mathbb{F}_q^{n-c} \times \mathbb{F}_{q^2}^{c}$ be the direct product of vector spaces. We obtain our *mixed alphabet Reed–Solomon code* $[n, k, d; c]_q \subseteq \mathbb{F}_q^{n-c} \times \mathbb{F}_{q^2}^{c}$ by evaluating all polynomials $f \in \mathbb{F}_q[x]$ of degree at most $k-1$. More precisely,

$$\mathcal{C} = \left\{ \left(f(\alpha_1), \ldots, f(\alpha_{n-c}), f(\gamma_1), \ldots, f(\gamma_c)\right) : f \in \mathbb{F}_q[x];\ \deg \mathrm{f} \leq \mathrm{k}-1 \right\} \tag{1}$$

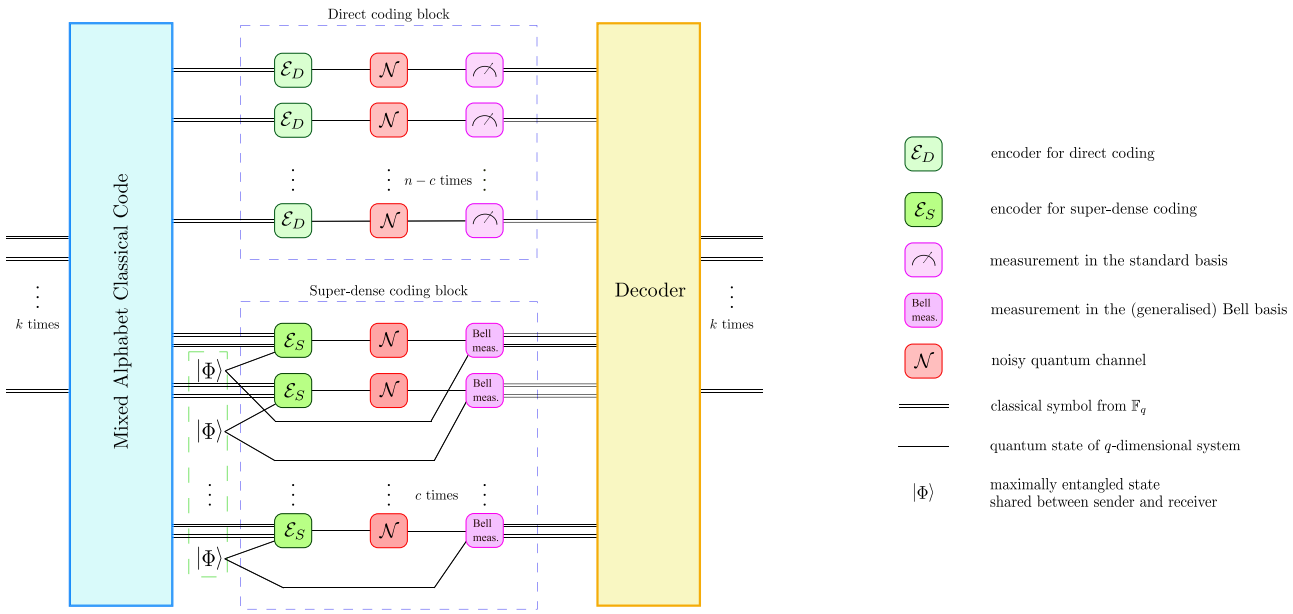

Fig. 1 | Schematic representation of the encoding and decoding process. The mixed alphabet classical code maps k input symbols to n outputs from different alphabets. Then, $n-c$ of the symbols are transmitted using direct coding and c symbols are transmitted using super-dense coding. The encoder $\mathcal{E}_D$ maps one classical symbol from $\mathbb{F}_q$ onto a qudit which is transmitted across a noisy quantum channel $\mathcal{N}$ and measured in the corresponding basis. This process is repeated $n-c$ times as illustrated by the *direct coding block*. The encoder $\mathcal{E}_S$ encodes a pair of classical symbols (identifying $\mathbb{F}_{q^2}$ and $(\mathbb{F}_q)^2$) onto one half of a maximally entangled state $|\Phi\rangle$. This encoded state is then transmitted across a noisy quantum channel $\mathcal{N}$. The other half of the maximally entangled state $|\Phi\rangle$ is shared with the receiver noiselessly. Upon reception, the receiver performs a measurement in the Bell basis on the received pair of states. This process is repeated c times as illustrated by the *super-dense coding block*. Finally, the decoder corrects errors and outputs a classical message.

where $n-c = n_1$ distinct evaluation points from $\mathbb{F}_q$ and $c = n_2$ distinct points from $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ are denoted by α_i and γ_j, respectively. The elements of $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ come in conjugate pairs $\{\gamma, \gamma^q\}$. We choose only a single element γ from each conjugate pair to be present among our evaluation points. This gives rise to the partitioning of the n evaluation points as $n = n_1 + n_2$, where n_1 is the number of elements from $\mathbb{F}_q$, and n_2 is the number of elements from $\mathbb{F}_{q^2}$.

In the standard classical setting, without entanglement assistance, one cannot achieve a rate $R = k/n$ higher than one, since the size of the code q^k cannot exceed the number q^n of different strings over an alphabet with q symbols. In contrast, our scheme allows k to be larger than n (whenever c is non-zero) while maintaining an injective encoding. To see this, consider the situation at the receiver's end. In order to retrieve the encoded information from a received codeword, the receiver uses the fact that a polynomial of degree at most $k-1$ is uniquely determined by its value at k evaluation points. For evaluation points $\gamma \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, we have $f(\gamma^q) = f(\gamma)^q$. Hence if the receiver knows the component of a codeword corresponding to an evaluation point γ_j, he can also compute the evaluation at the conjugate point γ_j^q. This means that in the error-free case the receiver actually has $n_1 + 2n_2 = n + n_2$ evaluation points at his disposal to identify the polynomial, i.e., interpolation is possible as long as the degree of the polynomial is strictly smaller than the number of evaluation points. Therefore we have $\deg(f) < n_1 + 2n_2$, or equivalently, $k-1 < n_1 + 2n_2 = n + n_2$.

The length of our code is limited by the maximum number of elements one can pick from $\mathbb{F}_q$ and the maximum number of single elements one can pick from $\mathbb{F}_{q^2}$. Therefore we have $1 \le n \le q + (q^2-q)/2 = (q^2+q)/2$. We note that we can extend the length by one and increase the minimum distance by one as well, using "the point at infinity". For simplicity, we do not consider that option in what follows.

For a linear code, the minimum distance d of the code equals the minimum weight (number of non-zero components) of a non-zero codeword. It can be deduced from the maximum number of evaluation points that are roots of a polynomial $f \in \mathbb{F}_q[x]$ of degree at most $k-1$.

For $n_1 \ge k-1$ we have

$$d = n - k + 1, \tag{2}$$

since there exists a polynomial f of degree at most $k-1$ with coefficients in $\mathbb{F}_q$ that has the maximal possible number of $k-1$ roots among the n evaluation points. The distance in Eq. (2) meets the so-called (classical) Singleton bound

$$d \le n - k + 1 \tag{3}$$

with equality. The bound is derived as follows. A code with distance d can correct $d-1$ erasures. Erasing $d-1$ of the n symbols results in strings of length $n-d+1$. Since all these strings have to be different, we get the bound $k \le n-d+1$, which is equivalent to Eq. (3).

For $n_1 < k-1$, we have

$$\begin{aligned} d &= n - \left(n_1 + \lfloor (k-1-n_1)/2 \rfloor\right) \\ &= \lceil (n-k+1+n_2)/2 \rceil \\ &> n-k+1. \end{aligned} \tag{4}$$

This is because of the following reasoning. We know that a polynomial of degree at most $k-1$ has at most $k-1$ roots. In the worst-case scenario, all of the n_1 evaluation points from the base field $\mathbb{F}_q$ are roots, and the remaining $k-1-n_1$ roots come from the extension field $\mathbb{F}_{q^2}$. If an element γ in $\mathbb{F}_{q^2}$ is a root, its conjugate partner γ^q is also a root. Since we have only single elements present among our evaluation points, not their conjugate partners, this implies that, in the worst case, at most half of the remaining $k-1-n_1$ roots are among the n_2 elements. The inequality follows from the fact that $n_1 < k-1$ implies that $n_2 = n-n_1 > n-k+1$. Hence, the minimum distance in Eq. (4) exceeds the classical Singleton bound in Eq. (3).

In the case of $n_1 < k-1$ we have the freedom to choose n_1, n_2 according to $n = n_1 + n_2$ and the constraints listed below such that the minimum distance (4) of a code $\mathcal{C} = [n, k, d; c]_q$ is maximized. This optimization involves picking as many evaluation points $c = n_2$ from $\mathbb{F}_{q^2} \setminus \mathbb{F}_q$ as possible, constrained by $c = n_2 \le (q^2-q)/2$. The number of evaluation points one can pick from $\mathbb{F}_q$ is restricted by the values of n, c and q, giving us $n-c \le n_1 \le q$. Also, we have $0 \le c \le n$.

Bounds

We now examine different ranges of n, c and k to determine when our code is optimal with respect to certain bounds.

The size of our code, i.e., the number of classical messages that our code can transmit, can be bounded, assuming that the code can correct a maximum of $d-1$ erasures.

Each of the n_1 symbols in a codeword can be visualized as a block of length one. Each of the n_2 symbols in a codeword can be seen as a block of length two. Overall, a codeword of length n contains n_1 blocks from $\mathbb{F}_q$ and n_2 blocks from $\mathbb{F}_{q^2}$. The blocks from $\mathbb{F}_{q^2}$ contain two symbols from $\mathbb{F}_q$ per block, allowing us to identify each element of $\mathbb{F}_{q^2}$ with an element in $(\mathbb{F}_q)^2$. This means erasing an element from the extension field corresponds to erasing a block of two symbols. First, assume that $n_2 \ge d-1$. Then, in the worst case, all the $d-1$ erasures occur within the n_2 blocks from $\mathbb{F}_{q^2}$. After the erasures have occurred, we are left with strings of $n_2-(d-1)$ symbols from $\mathbb{F}_{q^2}$ and n_1 symbols from $\mathbb{F}_q$. All these strings have to be different. This results in the bound

$$\begin{aligned} |\mathcal{C}| = q^k &\le q^{2(n_2-(d-1))} q^{n_1} \\ k &\le 2(n_2-(d-1)) + n_1. \end{aligned} \tag{5}$$

This is the block error bound. Essentially, in the analysis above we have customized the bound in ref. 22 to our situation. The block error bound (5) is met when $n \le q + \frac{q^2-q}{2}$, $n-q \le c$. In this case, the minimum distance is $d = \lceil (n-k+1+c)/2 \rceil$ as given in Eq. (4). In the scenario when $n_2 < d-1$, the block error bound reduces to the Singleton bound $k \le n-d+1$. This bound is met as long as $n_1 \ge k-1$ (see Eq. (2)).

We continue examining general bounds on the parameters of our setting. In this context, ref. 23 establishes a bound on hybrid codes that can transmit classical and quantum information simultaneously with the assistance of entanglement. We apply the bound in ref. 23 to our scenario. Since we are not transmitting quantum information, their parameter $Q = 0$ in our case. From Theorem 8 in ref. 23 and the corresponding equations (54)–(56) therein, we obtain the inequalities:

$$k \le (n-d+1)(1+t) \tag{6}$$

$$-c \le (n-2d+2)t \tag{7}$$

$$k - c \le (n-d+1) - t(d-1) \tag{8}$$

Here t is a parameter such that $t \in [0, 1]$. Note that in ref. 23, all logarithms use base 2, while our parameters k and c are related to base q. Hence the range $[0, \log_2 q]$ for the parameter t in ref. 23 yields the range $[0, 1]$ in our setting. Also, the amount of classical information k we are sending is C in their case, and the amount of available entanglement c for us is E in their scenario.

Consider the inequalities (6) and (8). Fixing all but k and t, we see that the maximum value of k is achieved when the corresponding bounds on k are equal. We compute the intersection point as $(n-d+1)(1+t) = c + (n-d+1) - t(d-1)$ giving us $t = c/n$. Particularly, we find that $t = c/n$ lies in the interval $[0, 1]$. When we substitute $t = c/n$ in Eq. (7) we find that it is fulfilled. This means $k_{\max} = (n-d+1)(1+c/n)$.

Using the above analysis, we obtain the following quantum-bound:

$$k \le (n-d+1)(1+c/n). \tag{9}$$

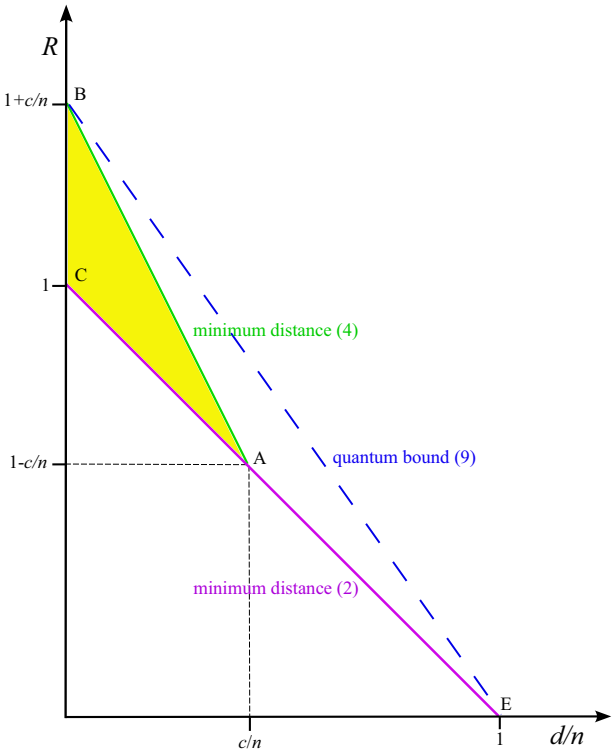

Fig. 2 | The code rate $R = k/n$ of our mixed-alphabet Reed–Solomon code is plotted as a function of the normalized minimum distance d/n in the asymptotic limit.

Equivalently, this gives the following bound on the distance

$$d \le n + 1 - \frac{kn}{n+c}. \tag{10}$$

The main question that we seek to answer in this section is for which range of n, k and c the code we have constructed is optimal. To reach the maximal integral value of k in Eq. (9), we get the condition

$$\Gamma = (n - d + 1)(1 + c/n) - k < 1. \tag{11}$$

In this case, we say that our code achieves dimension optimality.

To reach the maximal integral value of d in Eq. (10), we get the condition

$$\Delta = n + 1 - \frac{kn}{n+c} - d < 1. \tag{12}$$

In this scenario, we say that the code achieves distance optimality. Distance and dimension optimality are related as follows. When $\Delta < n/(n+c)$, we have dimension optimality. When $n/(n+c) \le \Delta < 1$, we have distance optimality but not dimension optimality since fixing all other parameters of the code we could increase the dimension by one without violating the bound (10). This means that dimension optimality is harder to achieve and implies distance optimality as well.

For the minimum distance in Eq. (4) we have $\Delta = n + 1 - \frac{kn}{n+c} - \lceil (n - k + 1 + c)/2 \rceil$. As a reminder, the minimum distance given in Eq. (4) is obtained after imposing the conditions $n \le q + (q^2 - q)/2$ and $n - q \le c$. We know that when $n = c$, we can use super-dense coding and obtain optimal solutions. Therefore we only consider the case $n > c$. The ranges of k for which our code is distance optimal are as follows

$$k > \begin{cases} n + c - 2\left(\frac{n+c}{n-c}\right), & \text{if } n - k + 1 + c \text{ is odd;} \\ \dfrac{(n+c)(n-c-1)}{n-c}, & \text{otherwise.} \end{cases}$$

When $n - k + 1 + c$ is even, we reach dimension optimality only for $k = n + c$ which implies $d = 1$. However, when $n - k + 1 + c$ is odd, we reach dimension optimality when $k > n + c - \frac{2n}{n-c}$.

Note that for linear codes, the dimension k is an integer, while the upper bound (9) on the dimension is, in general, non-integral. This means that when the bound is non-integral, it might be possible to find larger codes, but they cannot be linear. However, as we have shown, in specific instances where the upper bound is integral, linear codes attain the bound (9).

Discussion

Our proposed protocol achieves quantum advantage by surpassing the capabilities of classical codes through the use of entanglement. In our approach, entanglement strengthens error correction by increasing the minimum distance of the codes. We can see this using

$$d = \lceil (n - k + 1 + n_2)/2 \rceil$$

from Eq. (4) where the parameter n_2 equals the required amount of entanglement $c \ge n - k + 1$. If we fix k, with more entanglement, we can achieve a higher minimum distance. At the same time, fixing the distance d, with more entanglement, we get a higher dimension k and, in turn, a higher rate. Therefore, in our scenario entanglement helps us both to increase the distance or to increase the rate.

Moreover, entanglement allows us to achieve significantly higher minimum distances than what is possible classically without entanglement. Consider the following example. A code $[34, 20, 22; 28]_8$ using $c = n_2 = 28$ maximally entangled pairs achieves a minimum distance of 22. In contrast, without the use of entanglement, a linear code with parameters $[34, 20, d]_8$ can attain a maximum minimum distance of only 12. Furthermore, only a code $[38, 20, 10]_8$ is explicitly known[24]. To illustrate further, consider fixing the distance instead of the dimension. That is, we might ask what the largest possible code with distance 22 could be. Without the use of entanglement, a linear code with parameters $[34, k, 22]_8$ can achieve a maximum dimension of only 10[24]. In contrast, with entanglement assistance, we achieve twice the dimension, specifically $k = 20$.

In general, entanglement helps to achieve better code parameters in our scheme. Consider the code rate $R = k/n$. As discussed earlier in this section, there exists a trade-off between maximizing the rate for efficient information transmission and increasing the minimum distance for reliable error correction. Finding the best trade-off is an important question in coding theory.

In Fig. 2 we illustrate this trade-off for the code we constructed. We plot the code rate R as a function of the normalized minimum distance d/n in the asymptotic limit, ignoring additive terms that vanish when n goes to infinity. When $n_1 \ge k - 1$ our code with minimum distance (2) achieves rates represented by the line AE. Conversely, when $n_1 < k - 1$, our code with minimum distance (4) achieves rates represented by the line BA. Note that the line segments BA and AE agree with the block error bound. The region ABC encompasses points where the rate is greater than one and also includes points with rates less than one, all of which still exceed the Singleton bound, indicating that we are surpassing the performance of any classical code. Entanglement is the reason we can reach these higher rates unattainable by classical means within this range. The line AE indicates the range when our codes meet the Singleton bound. While the length of a classical MDS code with $1 < k < n - 1$ cannot exceed $2q - 2$ (see ref. 25, p. 94), our entanglement-assisted codes can have lengths up to $(q^2 + q)/2$.

We now examine certain additional aspects of our protocol. Our scheme allows to use the mixed alphabet Reed–Solomon codes introduced here. Using not only evaluation points from the field $\mathbb{F}_q$, but also from the field $\mathbb{F}_{q^2}$ we obtain longer codes, extending the length of optimal codes for fixed parameter q from $O(q)$ to $O(q^2)$. The scheme is not restricted to these codes. One can use other mixed alphabet codes or error-block correcting codes[26].

Also, our scheme is not restricted to the setting of perfect entanglement. Noisy entanglement (studied widely in the literature) results in errors in the super-dense coding protocol, which can equivalently be treated as errors during the transmission. In the error correction process, as long as the number of errors plus the number of "bad" entangled states is less than half of the minimum distance, our scheme will still work.

While our scheme provides an advantage over unassisted classical codes, we reach the quantum bound (9) only for specific parameters. We leave it to future research to determine whether there are entanglement-assisted codes for classical communication whose parameters lie in the region BAE of Fig. 2.

Finally, we would like to point out that our scheme does not require quantum memory or quantum computation. It only uses the primitive of super-dense coding that has been experimentally demonstrated[27,28].

We have thus designed an explicit protocol together with its parameters for EA classical communication. Our research provides an avenue to illustrate how entanglement can boost various finite-length communication protocols. In certain scenarios, using entanglement can enable a code to correct twice as many errors compared to a code with similar parameters without entanglement assistance. Additionally, in specific cases, entanglement allows a code to achieve a rate higher than one, a feat that is not possible classically without entanglement.

One of the open problems is to find coding schemes whose parameters are in the region BAE of Fig. 2. As the classical codes underlying our scheme meet the block error bound, codes reaching the quantum bound BE are unlikely to be derived from our reduction to a classical problem.

Our work paves the way for finding new explicit code constructions as well. Also, hybrid protocols for simultaneously sending both classical and quantum information with the assistance of entanglement can potentially be obtained by combining our scheme with existing schemes for EA quantum communication. Developing such hybrid codes, facilitated by our code construction, has far-reaching benefits. Explicit hybrid protocols have the potential to enhance error correction and secure communication and may play an important role in quantum computing tasks.

Received: 14 March 2024; Accepted: 24 December 2024;
Published online: 27 January 2025

References

1. Bennett, C. H. & Wiesner, S. J. Communication via one- and two-particle operators on Einstein–Podolsky–Rosen states. *Phys. Rev. Lett.* **69**, 2881–2884 (1992).
2. Bennett, C. H., Shor, P. W., Smolin, J. A. & Thapliyal, A. V. Entanglement-assisted classical capacity of noisy quantum channels. *Phys. Rev. Lett.* **83**, 3081–3084 (1999).
3. Bowen, G. Entanglement required in achieving entanglement-assisted channel capacities. *Phys. Rev. A* **66**, 052313 (2002).
4. Brun, T., Devetak, I. & Hsieh, M.-H. Correcting quantum errors with entanglement. *Science* **314**, 436–439 (2006).
5. Bennett, C. H., Shor, P. W., Smolin, J. A. & Thapliyal, A. V. Entanglement-assisted capacity of a quantum channel and the reverse Shannon theorem. *IEEE Trans. Inf. Theory* **48**, 2637–2655 (2002).
6. Devetak, I. & Shor, P. W. The capacity of a quantum channel for simultaneous transmission of classical and quantum information. *Commun. Math. Phys.* **256**, 287–303 (2005).
7. Datta, N. & Hsieh, M.-H. One-shot entanglement-assisted quantum and classical communication. *IEEE Trans. Inf. Theory* **59**, 1929–1939 (2013).
8. Hsieh, M.-H. & Wilde, M. M. Trading classical communication, quantum communication, and entanglement in quantum Shannon theory. *IEEE Trans. Inf. Theory* **56**, 4705–4730 (2010).
9. Devetak, I., Harrow, A. W. & Winter, A. A family of quantum protocols. *Phys. Rev. Lett.* **93**, 230504 (2004).
10. Shadman, Z., Kampermann, H., Macchiavello, C. & Bruß, D. Optimal super dense coding over noisy quantum channels. *N. J. Phys.* **12**, 073042 (2010).
11. Laurenza, R., Lupo, C., Lloyd, S. & Pirandola, S. Dense coding capacity of a quantum channel. *Phys. Rev. Res.* **2**, 023023 (2020).
12. Hsieh, M.-H. & Wilde, M. M. Entanglement-assisted communication of classical and quantum information. *IEEE Trans. Inf. Theory* **56**, 4682–4704 (2010).
13. Shannon, C. E. A mathematical theory of communication. *Bell Syst. Tech. J.* **27**, 379–423 (1948).
14. Kremsky, I., Hsieh, M.-H. & Brun, T. A. Classical enhancement of quantum-error-correcting codes. *Phys. Rev. A* **78**, 012341 (2008).
15. Grassl, M., Huber, F. & Winter, A. Entropic proofs of singleton bounds for quantum error-correcting codes. *IEEE Trans. Inf. Theory* **68**, 3942–3950 (2022).
16. Werner, R. F. All teleportation and dense coding schemes. *J. Phys. A: Math. Gen.* **34**, 7081–7094 (2001).
17. Brun, T. A., Devetak, I. & Hsieh, M.-H. Catalytic quantum error correction. *IEEE Trans. Inf. Theory* **60**, 3073–3089 (2014).
18. Grassl, M., Beth, T. & Pellizzari, T. Codes for the quantum erasure channel. *Phys. Rev. A* **56**, 33–38 (1997).
19. Roman, S. Coding and information theory. Graduate Texts in Mathematics, vol. 134 (Springer-Verlag, 1992)
20. MacWilliams, F. & Sloane, N. *The Theory of Error-Correcting Codes* (Elsevier Science, 1978).
21. Reed, I. S. & Solomon, G. Polynomial codes over certain finite fields. *J. Soc. Ind. Appl. Math.* **8**, 300–304 (1960).
22. Feng, K., Xu, L. & Hickernell, F. J. Linear error-block codes. *Finite Fields Their Appl.* **12**, 638–652 (2006).
23. Mamindlapally, M. & Winter, A. Singleton bounds for entanglement-assisted classical and quantum error correcting codes. *IEEE Trans. Inf. Theory* **69**, 5857–5868 (2023).
24. Grassl, M. *Bounds on the Minimum Distance of Linear Codes and Quantum Codes* http://www.codetables.de (2007).
25. Ball, S. *A Course in Algebraic Error-Correcting Codes* (Birkhäuser, Cham, 2020).
26. Ling, S. & Özbudak, F. Constructions and bounds on linear error-block code. *Des. Codes Cryptogr.* **45**, 297–316 (2007).
27. Mattle, K., Weinfurter, H., Kwiat, P. G. & Zeilinger, A. Dense coding in experimental quantum communication. *Phys. Rev. Lett.* **76**, 4656–4659 (1996).
28. Williams, B. P., Sadlier, R. J. & Humble, T. S. Superdense coding over optical fiber links with complete Bell-state measurements. *Phys. Rev. Lett.* **118**, 050501 (2017).

Acknowledgements

This research is supported by the 'International Centre for Theory of Quantum Technologies' project (contract no. MAB/2018/5) carried out within the International Research Agendas Program of the Foundation for Polish Science co-financed by the European Union from the funds of the Smart Growth Operational Program 2014-2020, axis IV: Increasing the research potential (Measure 4.3). M. Grassl's work is partially carried out under IRA Programme, project no. FENG.02.01-IP.05-0006/23, financed by the FENG program 2021-2027, Priority FENG.02, Measure FENG.02.01, with the support of the FNP. The funder played no role in the study design, data collection, analysis, and interpretation of data, or the writing of this manuscript.

Author contributions

All authors equally contributed to the conceptualization and preparation of the manuscript.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to Tushita Prasad.

Reprints and permissions information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

npj | quantum information

Article

Published in partnership with The University of New South Wales

https://doi.org/10.1038/s41534-025-01160-4

Certifying semi-device-independent security via wave-particle duality experiments

Chithra Raj[1,7], Tushita Prasad[1,7], Anubhav Chaturvedi[2,3], Lucas Pollyceno[1], Daniel Spegel-Lexne[4], Santiago Gómez[5], Joakim Argillander[4], Alvaro Alarcón[6], Guilherme B. Xavier[4] ✉, Marcin Pawłowski[1] & Pedro R. Dieguez[1] ✉

Wave-particle duality (WPD) is known to be equivalent to an entropic uncertainty relation (EUR) based on the min- and max-entropies, which have a clear operational meaning in quantum cryptography. Here, we derive a connection between wave-particle relations and the semi-device-independent (SDI) security framework. In particular, we express an SDI witness entirely in terms of two complementary interferometric quantities: visibility and input distinguishability. Applying a symmetry condition to the interferometric quantities, we identify a scenario in which the classical bound is violated and the security condition is met in wave-particle experiments with a tunable beam splitter (TBS). This enables the certification of non-classicality and the positivity of the key rate directly from complementary interferometric quantities, as well as from informational entropic quantities. Moreover, we perform a proof-of-principle experiment using orbital-angular-momentum (OAM) encoded quantum states of light in a tunable interferometer, validating our theoretical predictions. We analyze an improved bound on the SDI security condition for qubits, effectively enlarging the parameter region where secure communication can be certified. Finally, we extend the framework to multipath interferometers, establishing that the fundamental correspondence between information-access limitations and interferometric complementarity, demonstrated in the two-path scenario, persists across arbitrary dimensions.

Bohr's complementarity principle, a cornerstone of quantum theory, provides a unified framework in which matter and radiation can exhibit either wave-like or particle-like behavior, depending on the experimental context[1,2]. Its validity has been thoroughly tested in a wide range of systems —from double-slit experiments with light[3–5] and matter waves[6–8] to modern delayed-choice scenarios[1,9–12], demonstrating that interference arises when path information is unavailable, while the reveal of which-path information suppresses interference and yields particle-like detections. These results, consistent across diverse platforms, highlight the contextual nature of quantum phenomena[13,14] and challenge classical assumptions of simultaneously well-defined "elements of reality" for incompatible observables[1,15–17].

In a Mach-Zehnder interferometer (MZI), WPD can be expressed through conceptually distinct relations depending on the experimental configuration[18,19]. When the first beam splitter is biased, the setup defines a predictive scenario where the trade-off is between path predictability and fringe visibility. In contrast, a balanced first beam splitter defines a retrodictive scenario, where input distinguishability replaces predictability as the particle-like quantity. More generally, if an environment interacts with the system inside the interferometer, wave-particle duality is characterized by path distinguishability obtained from environmental measurements[20–22]. In all cases, the fundamental principle holds: increased knowledge of particle-like behavior reduces the visibility of interference fringes, and vice versa.

A substantial refinement of these ideas arises from the discovery that wave-particle duality relations (WPDRs) are equivalent to optimal EURs formulated with min- and max-entropies[20,21]. This equivalence lends an operational, information-theoretic meaning to the trade-off between the

[1]International Centre for Theory of Quantum Technologies, University of Gdańsk, Gdańsk, Poland. [2]Faculty of Applied Physics and Mathematics, Gdańsk University of Technology, Gdańsk, Poland. [3]Institute of Theoretical Physics and Astrophysics, Faculty of Mathematics, Physics and Informatics, University of Gdańsk, ul. Wita Stwosza 57, 80-308 Gdańsk, Poland. [4]Institutionen för Systemteknik, Linköpings Universitet, Linköping, Sweden. [5]Dipartimento di Fisica, Sapienza Università di Roma, Roma, Italy. [6]Departamento de Ingeniería Eléctrica y Electrónica, Facultad de Ingeniería, Universidad del Bío-Bío, Concepción, Chile. [7]These authors contributed equally: Chithra Raj, Tushita Prasad. ✉e-mail: guilherme.b.xavier@liu.se; pedro.dieguez@ug.edu.pl

interferometric quantities: the same entropic quantities that limit simultaneous wave and particle manifestations also bound an eavesdropper's optimal guessing probability and, therefore, the secrecy achievable in quantum key distribution (QKD)[23–26]. This equivalence was recently confirmed in a photonic experiment using OAM quantum states of light, where the equivalence between WPD and EURs was demonstrated on a versatile, reconfigurable platform based on few-mode optical fibers and photonic lanterns[27]. As a result, WPD emerges not merely as a conceptual pillar but as a practical resource for quantum information science.

Complementarity plays a key role in both device-dependent (DD) and device-independent (DI) quantum cryptography. In the DD regime, it underlies the security of protocols like BB84, where mutually unbiased bases ensure that eavesdropping induces detectable disturbances[28]. Delayed-choice-inspired cryptographic protocol[29] similarly uses flexible measurement settings to enforce security through wave-particle duality. In the DI paradigm, security relies solely on Bell inequality violations[30–32], offering strong guarantees but requiring stringent experimental conditions[32]. To mitigate these challenges, complementarity-based DI protocols have been proposed for more practical scenarios[26], and broader operational perspectives on complementarity have also been explored[33]. Given the experimental limitations of DI protocols, the semi-device-independent (SDI) framework, requiring only a bound on system dimension[34], offers a promising alternative. While complementarity has been linked to both DD and fully DI cryptographic frameworks, its role in the SDI scenario remains largely unexplored.

In this work, we aim to bridge this gap by establishing a connection between WPDRs and SDI security witnesses. We derive a method to express an SDI witness in terms of interferometric quantities—visibility and input distinguishability, capturing the operational features of complementarity across arbitrary experimental contexts. We present a particular mapping to assess a region in the visibility-distinguishability plane where both the classical bound and the security threshold can be violated via WPD experiments with a final TBS, thereby demonstrating non-classicality and key-rate positivity with purely interferometric data. Moreover, we analyze a better bound on the SDI security condition, which enlarges the accessible security region. Finally, using a fiber-optical interferometer designed to be dynamically reconfigurable to measure the visibility and path distinguishability of OAM quantum states of light[27], we perform a proof-of-principle experiment that validates our main result.

Results

Theoretical framework

We begin by outlining the theoretical framework underlying our analysis. In general *prepare-and-measure* (PM) scenarios, Alice prepares a message using a d-dimensional physical system from a set $a \in \{0, \ldots, N-1\}$ and sends it to Bob through a potentially insecure channel. Bob performs a measurement chosen by $y \in \{0, \ldots, m-1\}$ and obtains an outcome $b \in \{0, \ldots, k-1\}$. The PM scenario is defined by the dimension d and the tuple (N, m, k). After many rounds, the observed statistics are given by the conditional probability distribution $\{P(b|a,y)\}_{b,a,y}$. Such correlations are constrained by the available resources, especially the communication dimension d. When limited to classical resources of dimension d, the statistics must satisfy inequalities of the form

$$\sum_{a,y,b} w_{a,y,b} P(b|a,y) \leq C_d, \tag{1}$$

where C_d is the classical bound. These expressions are referred to as *dimension witnesses*. Quantum systems can violate these bounds while still using dimension d, as the probabilities are governed by the Born rule

$$P(b|a,y) = \mathrm{Tr}\left(\rho_a M_y^b\right), \tag{2}$$

where ρ_a are d-dimensional quantum states and M_y^b denotes Bob's measurement POVMs.

The SDI approach assumes a known dimension d, and a violation of the dimension witness certifies the system's quantum nature without full device characterization. As demonstrated in ref. 34, such violations also ensure security in one-way QKD, as quantum messages cannot be copied like classical ones. A particularly relevant scenario is (4, 2, 2), as depicted in Fig. 1, in which Alice selects one of four preparations, labeled by two bits a_0a_1, and Bob performs one of two binary measurements. The conditional probabilities are grouped into correlators $E_{a_0a_1,y} := P(b=0|a_0a_1,y)$, and the SDI witness takes the form:

$$S = E_{00,0} + E_{00,1} + E_{01,0} - E_{01,1} - E_{10,0} + E_{10,1} - E_{11,0} - E_{11,1}. \tag{3}$$

Classically, $S \leq 2$, but quantum strategies allow up to $S = 2\sqrt{2}$. This witness is related to a quantum random access code (QRAC) task[34], where Bob attempts to guess one of Alice's bits a_y:

$$P_B = \frac{1}{8}\sum_{a_0,a_1,y} p(b = a_y|a_0,a_1,y) = \frac{S+4}{8}. \tag{4}$$

In this setting, it is important to distinguish between Bob's and Eve's (the eavesdropper) roles. Eve attempts to guess Alice's inputs (a_0, a_1) by intercepting the quantum systems that Alice sends to Bob. Since the scenario assumes non-characterized devices, Eve's measurements are not restricted to any particular form—she could, in principle, perform any quantum measurement to maximize her average guessing probability P_E. This corresponds to the standard individual attack scenario, where Eve acts on each transmission separately and measures the intercepted state immediately. Bob, by contrast, measures the quantum system he directly receives from Alice, for the purpose of key generation. His average success probability P_B depends on his chosen measurement basis, which can be optimized for maximum performance. Whereas Bob's measurements are fixed by the protocol, Eve's are arbitrary within the laws of quantum mechanics.

Reference 34 shows that secure key distribution is guaranteed when $P_B > P_E$. Using results from guessing probability games, it is proved that security is ensured when $P_B > 0.8415$.

Our analysis also involves two operational quantities, input distinguishability $\mathcal{D}$ and interferometric visibility $\mathcal{V}$, which respectively characterize particle-like and wave-like behavior in binary

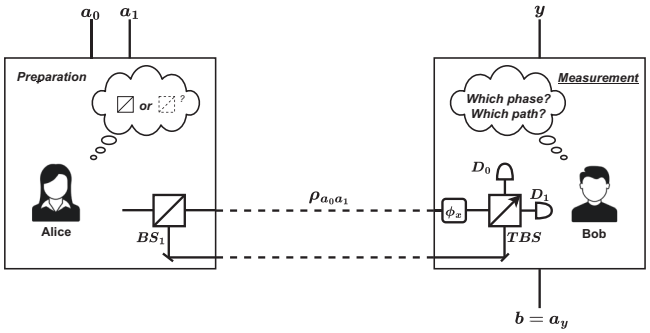

Fig. 1 | SDI Witness and Wave-Particle Games. In the *preparation stage*, Alice receives two classical bits (a_0, a_1) and encodes them into a two-dimensional quantum state $\rho_{a_0a_1}$. This encoding involves a choice of whether to insert an unbiased beam splitter (BS_1) on each computational basis preparation or not. In the *measurement stage*, Bob receives the quantum state, after a phase shift ϕ_x is applied, and performs a measurement based on his chosen input. His setup includes TBS, which allows him to interpolate between particle-like and wave-like observables. Due to WPD and complementarity, Bob faces fundamental limits: he cannot simultaneously extract both which-path and which-phase information with arbitrary precision. These constraints, expressed in terms of interferometric visibility and path distinguishability, provide a basis for evaluating the SDI witness.

interferometric setups. A central result of this work is the connection we establish between these quantities and the SDI witness, which will be discussed in the following sections. Setting Z as the which-path random variable associated with the basis $\mathbb{Z} = \{|z\rangle\langle z|\}$ of an 2-dimensional Hilbert space $\mathcal{H}_A$, and W as the random variable associated with a mutually unbiased basis $\mathbb{W}$ in respect to $\mathbb{Z}$, we employ the framework introduced in ref. 20 which defines interferometric input distinguishability $\mathcal{D}$ in terms of the optimal probability of correctly guessing the which-path information Z

$$\mathcal{D} := 2p_{\text{guess}}(Z) - 1. \tag{5}$$

Operationally, this is estimated by blocking each path (upper U or lower L) and measuring the difference in output detection probabilities p_0 and p_1:

$$\mathcal{D}_{U(L)} := \left[\frac{|p_0 - p_1|}{p_0 + p_1}\right]_{\text{path}U(L)\text{blocked}}, \quad \mathcal{D} := \frac{1}{2}(\mathcal{D}_U + \mathcal{D}_L). \tag{6}$$

The interferometric visibility $\mathcal{V}$ measures coherence via the guessing probability of the output observable $\mathbb{W}$, optimized over all observables in the XY plane[20]

$$\mathcal{V} := \max_{\mathbb{W}\in XY}[2p_{\text{guess}}(W) - 1]. \tag{7}$$

Operationally, $\mathcal{V}$ is determined in binary interferometers by varying a relative phase and recording the maximum and minimum detection probabilities at each output port

$$\mathcal{V}_j := \frac{p_j^{\max} - p_j^{\min}}{p_j^{\max} + p_j^{\min}}, \quad \mathcal{V} := \frac{1}{2}(\mathcal{V}_0 + \mathcal{V}_1). \tag{8}$$

Interestingly, the well-known binary duality relation $\mathcal{D}^2 + \mathcal{V}^2 \le 1$ is proved equivalently to the following informational relation[20,27]

$$H_{\min}(Z) + \min_{\mathbb{W}} H_{\max}(W) \ge 1, \tag{9}$$

where the unconditional min- and max-entropies are respectively defined for a given probability distribution $P = \{p_j\}$ as

$$H_{\max}(P) := 2\log_2 \sum_j \sqrt{p_j}, \tag{10}$$

and

$$H_{\min}(P) := -\log_2 \max_j p_j. \tag{11}$$

For the higher-dimensional case, ref. 21 introduced generalized definitions of interferometric visibility and distinguishability, formulated for scenarios involving symmetric beam splitters where the Fourier transform of the computational basis naturally arises. In such multipath interferometers, visibility extends to

$$\mathcal{V} := \frac{n p_{\text{guess}}^{\max_{\{\phi_k\}}}(W) - 1}{n - 1}, \tag{12}$$

defined in terms of the optimal guessing probability over all controllable relative phases $\{\phi_k\}$. This quantity captures the wave-like behavior associated with coherence across multiple paths and is intrinsically linked, through complementarity, to the generalized distinguishability

$$\mathcal{D} := \frac{n p_{\text{guess}}(Z) - 1}{n - 1}, \tag{13}$$

which quantifies the optimal ability to correctly identify the path information (particle-like behavior). These quantities are shown to follow the complementarity relation $\mathcal{D}^2 + \mathcal{V}^2 \le 1$ with its corresponding entropic version

$$H_{\min}(Z) + \min_{\mathbb{W}} H_{\max}(W) \ge \log_2 n. \tag{14}$$

Mapping SDI witness via wave-particle duality scenarios

We reinterpret this PM protocol as a WPD game, inspired by the delayed-choice-based QKD protocol described in ref. 29. In the cryptographic extension of this scenario, both the first and second unbiased beam splitters play a role, enabling a delayed-choice QKD protocol. In this framework, the key is transmitted when both parties remove their beam splitters, corresponding to the direct preparation and detection of computational basis states. Security is verified by monitoring the interference statistics in the other configurations: when both beam splitters are inserted, the protocol tests resilience against intercept-and-forward attacks; when only one of the beam splitters is inserted, the protocol allows the detection of intercept-and-reprepare strategies. This generalization therefore unifies the control of BS_1 and BS_2, providing both key transmission and security checks within a single delayed-choice-inspired setup. In this scenario, Alice's preparation involves deciding whether or not to include the first beam splitter BS_1, as depicted in Fig. 1. In our experimental setup, this is represented by a PL, please see Fig. 2 and Methods 3 for further details. Specifically, particle-like behavior can only be observed in the MZI when BS_1 is removed (or when the paths are blocked after the first beam splitter); conversely, wave-like behavior is observed when BS_1 is included. Moreover, incorporating a final TBS in the setup, as shown in Figs. 1, 2 and detailed in Methods 2, allows one to interpolate between fully particle-like and fully wave-like behavior. Analogously, without loss of generality, we associate even-parity inputs ($a_0 = a_1$) with particle-like experiments, and odd-parity inputs ($a_0 \neq a_1$) with wave-like experiments. Naturally, the output b corresponds to the detector clicks (D_0 or D_1). Note that while y determines the measurement setting, we consider the relative phase of the MZI, defined as a parameter ϕ_x, shown in Fig. 1, to be later optimized.

To address this parity-based structure within the binary MZI, we adopt the four-state preparation scheme used in both BB84 and[29], given by

$$\begin{aligned} \rho_{00} &= |0\rangle\langle 0|, \quad \rho_{01} = |-\rangle\langle -|, \\ \rho_{10} &= |+\rangle\langle +|, \quad \rho_{11} = |1\rangle\langle 1|, \end{aligned} \tag{15}$$

where $|0\rangle$ and $|1\rangle$ correspond to the two interferometric paths, while $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$ represent path superpositions for the cases where Alice included BS_1. Notice that the states in Eq. (15) follow uniquely from the MZI structure, and this particular choice of encoding ensures that the parity captures either particle-like or wave-like behavior. It is important to stress that this encoding is not restrictive, as any alternate bit-to-state assignment can be mapped to this one via relabeling. This structure provides a natural framework to study the trade-off between $\mathcal{D}$ and $\mathcal{V}$ within the SDI witness (3).

In a PM scenario, the behavior is fully characterized by the prepared state ρ_{a_0,a_1} and the measurement M_y performed. Building on this and following the previously introduced operational definitions, we redefine $\mathcal{D}$ and $\mathcal{V}$ for each configuration (a_0, a_1, y, b) as

$$\mathcal{D}^b_{a_0,a_1,y} := 2p^{a_0,a_1,y}_{\text{path},\phi_x} - 1, \tag{16}$$

$$\mathcal{V}^b_{a_0,a_1,y} := 2p^{b,a_0,a_1,y}_{\max} - 1, \tag{17}$$

where

$$p^{a_0,a_1,y}_{\text{path},\phi_x} \equiv P_{\phi_x}(b = a_0|a_0, a_1, y)\delta_{a_0\oplus a_1,0}, \tag{18}$$

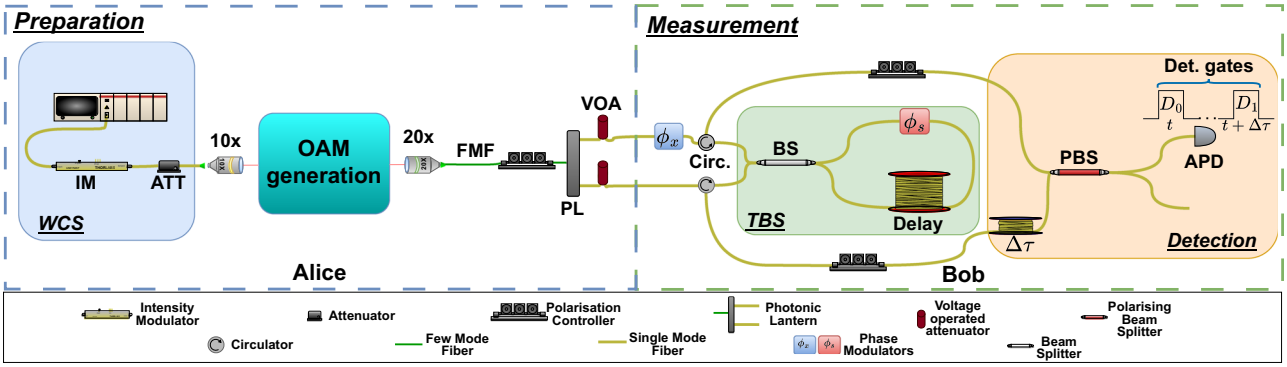

Fig. 2 | SDI witness implementation. Alice prepares OAM weak coherent photonic states (WCS), produced from heavily attenuated optical pulses. The OAM states are coupled onto a few-mode fiber (FMF), which passes through a manual polarization controller wound with the FMF before being connected to a photonic lantern (PL), whose single-mode fiber outputs form a Mach-Zehnder interferometer. The PL splits the OAM state into its two linearly polarized components, $|LP_{11a}\rangle$ and $|LP_{11b}\rangle$, mapped to the two paths of the interferometer. Bob connects the two paths to a TBS, comprised of a fiber-optical Sagnac interferometer, containing a phase modulator ϕ_s and a 300 m fiber-optical delay. When the two Sagnac counter-propagating paths recombine at the fiber beamsplitter (BS), the two outputs are split from the inputs using two optical circulators (Circ.). The two circulator outputs are then multiplexed in time with a fiber delay $\Delta\tau$ in the lower arm before being recombined at a polarization beam splitter (PBS), with the transmission of the two input paths maximized with manual polarization controllers. This allows the use of one single-photon detector, as the two-path outputs of the TBS become distinguishable due to the time separation $\Delta\tau$, effectively and thus matched to two detection times labeled as D_0 and D_1. An additional phase modulator ϕ_x is placed inside the interferometer to perform the visibility measurements. For additional details on the modeling and implementation, please refer to the main text as well as Methods Sections 2 and 3.

$$p_{\max}^{b,a_0,a_1,y} \equiv \max_{\phi_x} P_{\phi_x}(b|a_0,a_1,y)\delta_{a_0\oplus a_1,1}, \tag{19}$$

and $\delta_{i,j}$ denotes Kronecker's delta. The structure of Eq. (18) highlights that, whenever $a_0 = a_1$ the path information is carried by a_0 and a_1, as ensured by the encoding specified in Eq. (15).

We are now equipped to connect the SDI witness S to the wave-particle quantities. Due to the parity-based encoding, we define the path guessing probability as

$$p_{\text{path},\phi_x} = \frac{1}{4}\sum_{a_0,a_1,y} P_{\phi_x}(b = a_0|a_0,a_1,y)\delta_{a_0\oplus a_1,0}, \tag{20}$$

for the cases of particle-like experiments.

Comparing (4), (16) and (20), the SDI witness S_{ϕ_x} can be rewritten as

$$\begin{aligned} S_{\phi_x} = &\sum_{a_0,a_1,y}\left(\frac{\mathcal{D}_{a_0,a_1,y}+1}{2}\right)\delta_{a_0\oplus a_1,0} \\ &-4 + p(0|01,0) + p(1|01,1) + p(1|10,0) + p(0|10,1). \end{aligned} \tag{21}$$

Maximizing over the phase shift ϕ_x (which tunes the interference visibility), and using the definition of visibility in Eq. (17), we finally obtain the core result

$$\begin{aligned} \max_{\phi_x} S_{\phi_x} = &\tfrac{1}{2}\sum_{a_0,a_1,y}\mathcal{D}_{a_0,a_1,y}\,\delta_{a_0\oplus a_1,0} \\ &+\tfrac{1}{2}\sum_{a_0,a_1,y,b}\mathcal{V}^{b}_{a_0,a_1,y}\,\delta_{a_0\oplus a_1,1}\delta_{b,a_y}. \end{aligned} \tag{22}$$

It is important to emphasize that our analysis explores the independence of each experiment under the optimization of ϕ_x, and that $\mathcal{D}_{a_0,a_1,y}$ remains phase-independent due to the parity encoding in (15).

This decomposition reveals that the SDI witness S directly quantifies the sum of optimal distinguishabilities and visibilities over the relevant configurations of the game. Importantly, this formulation remains valid under minimal assumptions about the underlying physical implementation, requiring only a single parameter to be maximized in the measurement setting.

Moreover, in Methods 1, we present a detailed derivation of an upper bound on the eavesdropper's success probability P_E in terms of Bob's average success probability P_B, refining the SDI security condition originally proposed in ref. 34. The security analysis considers the worst-case scenario in which Bob and Eve collaborate. That is, they may share their respective information about Alice's inputs, so the relevant joint guessing probability P_{BE} lower bounds both Bob's and Eve's success probabilities: $P_{BE}\geq P_B(a_i)$, $P_E(a_i)$. Security follows from the fact that even under this collaborative assumption, Bob's average guessing probability P_B can be made strictly larger than Eve's, thereby ensuring that Eve cannot obtain the key without introducing detectable disturbances. In particular, we obtain,

$$P_E \leq \frac{3+\sqrt{1-2(2P_B-1)^2}}{4}. \tag{23}$$

This inequality implies that secure key distribution (i.e., $P_B > P_E$) is ensured whenever $P_B > 0.833$, thereby improving upon the previous threshold of 0.8415. The full derivation is provided in Methods 1. We now define the experimental context in which the SDI witness is assessed.

Wave-particle duality experiments with a TBS

We focus on the SDI witness within a particular WPD guessing game. This is achieved by analyzing a photonic interferometer equipped with an input 50: 50 beamsplitter (BS), a relative phase shift, and a TBS. We show how data obtained from two specific interferometer configurations characterized by phase shifts ϕ_x and $\phi_x + \pi$ can be used to interpolate the SDI witness and demonstrate non-classicality and security conditions based on the interferometric quantities. We now follow the setup depicted in Fig. 2, and define Bob's measurements in the SDI guessing game as given by

$$\begin{aligned} M_0(\phi_s,\phi_x) &= \cos\phi_s\sigma_z + \sin\phi_s\left(\cos\phi_x\sigma_x + \sin\phi_x\sigma_y\right), \\ M_1(\phi_s,\phi_x) &= M_0(\phi_s,\phi_x+\pi), \end{aligned} \tag{24}$$

where $0 \leq \phi_s \leq \pi/2$, and $\phi_x \in [0, 2\pi N]$ with $N \in \mathbb{N}$, allowing phase scans over multiple cycles. These observables interpolate between wave-like and particle-like behavior depending on the relative phases. Under the symmetry of the interferometer and measurements, we obtain the relations

$$E_{00,0} = E_{00,1}, \quad E_{11,0} = E_{11,1}, \\ E_{01,0} = E_{10,1}, \quad E_{10,0} = E_{01,1}. \tag{25}$$

In addition to these symmetry relations, the constraints imposed by parity-obliviousness and blocking lead to the following normalization conditions

$$E_{00,0} + E_{11,0} = 1, \\ E_{01,0} + E_{10,0} = 1. \tag{26}$$

Here, parity-obliviousness ensures that the encoding does not reveal information about the parity bit $a_0 \oplus a_1$. Blocking is implemented by selectively disabling one of the interferometric paths, which allows marginal probabilities to be determined independently of interference, thereby isolating particle-like behavior.

Particularizing on the states and measurements discussed means exploiting the symmetries $\mathcal{V}^b_{0,1,y} = \mathcal{V}^b_{1,0,y} = \mathcal{V}$ and $\mathcal{D}^b_{0,0,y} = \mathcal{D}^b_{1,1,y} = \mathcal{D}$, which leads to the final compact expression

$$\max_{\phi_x} S_{\phi_x} = 2(\mathcal{D} + \mathcal{V}). \tag{27}$$

In what follows, we present our experimental implementation of the SDI witness via complementary interferometric quantities.

Experimental assessment of the SDI witness via wave-particle quantities

Our experimental setup, shown in Fig. 2 and detailed in Methods 2 and 3, is based on a modified fiber-optical MZI where the input BS is composed of a PL[35] which decomposes two-dimensional OAM states of light into its linearly polarized components in the following way: $|OAM_{+1}\rangle = 1/\sqrt{2}(|LP_{11a}\rangle + i|LP_{11b}\rangle)$[36]. Within the two parallel paths of the interferometer, electro-optical attenuators and a phase modulator are placed, such that we can transform the original balanced superposition into the general path state $\alpha|0\rangle + e^{i\phi_x}\beta|1\rangle$, where the amplitude coefficients α and β are adjusted with the attenuators and ϕ_x with the phase modulator. The interferometer's paths are then superposed on a 50: 50 fiber-optical beamsplitter, whose outputs form a fiber Sagnac interferometer, which works as a TBS, dynamically adjustable by the internal phase modulator ϕ_s. Two circulators are employed to route the outputs from the TBSs to a time-multiplexing fiber arrangement to map the two outputs to the two time slots D_0 and D_1, identifiable by one single-photon detector. Quantum states of light are prepared from a heavily attenuated laser beam and encoded onto the $|OAM_{+1}\rangle$ state with a spatial light modulator, which are coupled to a few-mode fiber, which is then connected to a PL decomposing the state onto the $|LP_{11a}\rangle$ and $|LP_{11b}\rangle$ modes, mapped respectively to the lower and upper paths of the interferometer. For more details on the experimental setup, we refer the reader to Methods 3.

We then proceed to measure the visibility of the $|OAM_{+1}\rangle$ state passing through the interferometer, by scanning ϕ_x for different settings of ϕ_s of the TBS corresponding to changing the measurement operator from particle to wave aspects, quantifying the SDI witness S. The distinguishability is measured in a similar fashion, with the difference that one of the arms of the interferometer is blocked with the electro-optical attenuators. Figure 3 shows that the experimental results match the theoretical framework connecting S and the interferometric quantities $\mathcal{D}$ and $\mathcal{V}$, as developed in this work. Our results show that neither purely particle-like ($\mathcal{D} = 1$) nor purely wave-like behavior ($\mathcal{V} = 1$) is sufficient to violate the classical bound. This highlights the need for a balanced contribution from both aspects to reveal the non-classicality. As depicted in Fig. 3, the optimal violation occurs when $\mathcal{D} = \mathcal{V} = \sqrt{2}/2$, corresponding to a phase setting of $\phi_s = \pi/4$. In Fig. 3 some

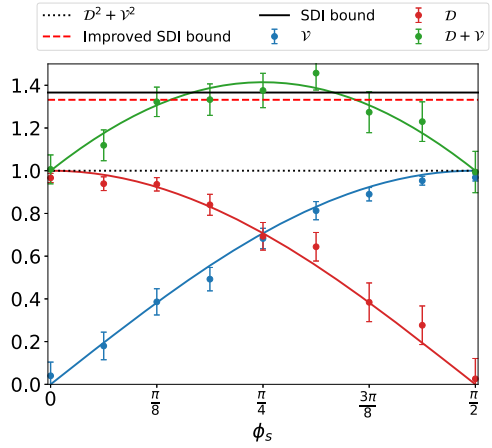

Fig. 3 | SDI witness via wave-particle relation. The blue and red curves represent the average interferometric visibility $\mathcal{V}$ and average distinguishability $\mathcal{D}$, respectively. The green curve shows the SDI witness expressed as $S/2 = \mathcal{D} + \mathcal{V}$. The dotted black line marks the classical bound $\mathcal{D} + \mathcal{V} > 1$, while the dashed and solid lines indicate the two security thresholds: the previously known bound at 1.366 and the improved bound at 1.332. Each data point (circle) represents an experimental value, with error bars obtained via error propagation assuming Poissonian statistics for the detected event counts.

points are deviating slightly from the theoretical predictions, which originates from two main factors: (i) the limited achievable visibility in the interferometer, mainly from the extinction ratio of the photonic lantern, and (ii) finite data obtained from each experimental round stemming from the limitation in the repetition rate of the experiment and the use of passive insulation against environmentally induced phase drifts in the interferometer.

In Fig. 3, we compare two security criteria: the original bound of[34], which, in terms of interferometric quantities, requires $\mathcal{D} + \mathcal{V} > 1.366$ for secure communication, and the improved bound derived in Methods 1, which establishes the condition $\mathcal{D} + \mathcal{V} > 1.332$. This tighter threshold expands the range of parameters for which security can be certified in the experiment. In the following, we exploit the operational equivalence between WPD and the optimized EUR to express the SDI witness directly in the plane defined by min- and max-entropies.

Experimental assessment of the SDI witness in the entropic plane

In cryptographic terms, the min-entropy reflects how well an eavesdropper can guess the raw key, while the max-entropy characterizes the secrecy or uniformity of the key after privacy amplification[37]. In the context of MZI experiments, these entropic quantities can be directly expressed in terms of the interferometric parameters $\mathcal{D}$ and $\mathcal{V}$[20,21]:

$$H_{\min}(Z) = 1 - \log_2(1 + \mathcal{D}), \tag{28a}$$

$$H_{\max}(W) = \log_2\left(1 + \sqrt{1 - \mathcal{V}^2}\right), \tag{28b}$$

which, together with

$$H_{\min}(Z) + H_{\max}(W) \geq 1, \tag{29}$$

naturally recover the quadratic complementarity relation. In this context, the SDI witness (27) can also be rewritten, where the classical bound $S \leq 2$ translates into

$$1 - H_{\min}(Z) \leq \log_2\left(2 - \sqrt{1 - (2^{H_{\max}(W)} - 1)^2}\right). \tag{30}$$

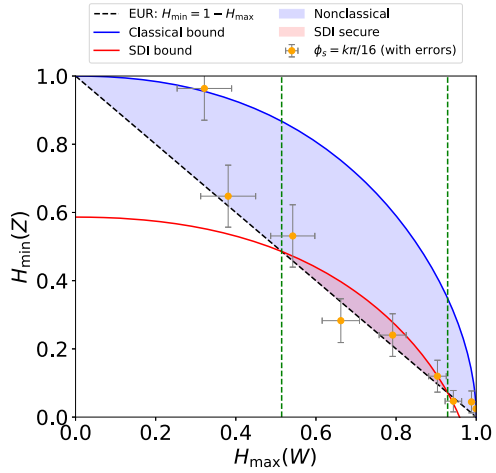

Fig. 4 | Hierarchy bounds on the entropic plane $(H_{max}(W), H_{min}(Z))$. The dashed black line represents the EUR, which is the most general constraint and is always satisfied. The solid blue curve marks the classical boundary corresponding to the inequality $S \leq 2$; the region above it is classically reproducible, while the blue band between the EUR and the classical curve corresponds to nonclassical quantum correlations ($S > 2$). The solid red curve denotes the SDI security bound for the improved threshold, with the shaded red region below it indicating where security can be certified. Vertical green dashed lines mark the compatibility window where the SDI bound and the EUR overlap. Orange points with error bars represent the experimental results obtained at phase settings $\phi_s = k\pi/16$ ($k = 0, \ldots, 8$). Error bars are obtained via propagation assuming Poissonian statistics for the detected event counts.

Interestingly, this condition automatically ensures the EUR (29), since $H_{max} \in [0, 1]$. However, surpassing the classical bound (30) defines a necessary condition for cryptographic security within the SDI framework. As previously discussed, this condition can be achieved in quantum mechanics up to the optimal point when $\mathcal{D} = \mathcal{V} = 1/\sqrt{2}$, which is directly confirmed from (28) never exceeding the saturation of the EUR (29). Consequently, in terms of the quantities $H_{max}(W)$ and $H_{min}(Z)$, the SDI security condition necessarily depends on the intersection between the region defined by the EUR (29) and that defined by the violation of the classicality condition (30) (see Fig. 4). Indeed, from (52) and (4), SDI security is guaranteed whenever $S \gtrsim 2.664$, which in terms of (28) reads as

$$1 - H_{min}(Z) > \log_2\left(2.332 - \sqrt{1 - \left(2^{H_{max}(W)} - 1\right)^2}\right). \tag{31}$$

This analysis is confirmed with the experimental results shown in Fig. 4. Up to the error bars, all experimental points lie within the physically allowed region defined by the EUR (29). As becomes evident, Fig. 4 demonstrates that it is possible to extract cryptographic keys within the SDI framework. In fact, the security condition (31) is satisfied for the range $H_{max}(W) \in [0.5144, 0.9287]$.

Having established the operational connection between the interferometric quantities and the success probability of the $(2 \mapsto 1)$ RAC in the qubit case, both theoretically and experimentally, we now show that this direct relationship also holds for higher-dimensional systems.

Extension to higher dimensions

In extending the analysis to a d-path interferometer, particular care must be taken in defining the relevant interferometric quantities. In higher dimensions, distinct formulations of visibility have been proposed in the literature[21,38], depending on the interferometric configuration. For clarity and consistency with the forthcoming discussion, we restrict our analysis to interferometers employing an initial symmetric beam splitter. In this multipath setting, Alice's preparations are described in terms of the computational and Fourier bases, corresponding to the particle-like and wave-like regimes, respectively:

$$\begin{aligned} &|j\rangle, \quad \text{where} \quad j \in \{0, 1, \ldots, d-1\}; \\ &|k\rangle = \tfrac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{kj} |j\rangle, \quad \text{where} \quad k \in \{0, 1, \ldots, d-1\}. \end{aligned} \tag{32}$$

Here, $d-1$ paths acquire respective phases $\phi_{x_1}, \phi_{x_2}, \ldots, \phi_{x_{d-1}}$. Following the approach from the two-path case, we can relate this interferometer to the RAC task. Equation (32) defines $2d$ interferometrically well-defined preparations for Alice, naturally leading to the $(2 \mapsto 1, d)$ RAC scenario, where Alice holds two d-its and communicates a single d-dimensional quantum state to Bob. The success probability is given by[39]:

$$p_{suc} = \frac{1}{2d^2} \sum_{a_0, a_1, y} p(b = a_y | a_0, a_1, y). \tag{33}$$

To establish a meaningful correspondence with the interferometer, we introduce an encoding strategy that captures both particle-like and wave-like regimes while ensuring a consistent operational interpretation of the interferometric quantities. Specifically, Alice prepares states in the computational basis whenever $a_0 \oplus_d a_1$ is even and in the Fourier basis whenever it is odd, where $\oplus_d$ denotes addition modulo d. This rule ensures that both types of experiments are included while keeping the set of preparations restricted to the $2d$ interferometrically well-defined states in (32).

Given Alice's encoding within her initial dits we can rewrite the guessing probabilities $p_{guess}(Z)$ and $p_{guess}(W)$, extending (18) and (19) to the multipath interferometer case. In fact, for a fixed preparation $a_0 a_1$ and measurement y, we have:

$$p_{guess}(Z) = p(b = a_y | a_0 \oplus_d a_1 = n_{even}, y), \tag{34}$$

$$p_{guess}(W) = p(b = a_y | a_0 \oplus_d a_1 = n_{odd}, y), \tag{35}$$

where

$$p_{guess}^{\max_{\{\phi_k\}}}(W) \equiv \max_{\phi_{x_1}, \phi_{x_2}, \ldots, \phi_{x_{d-1}}} p_{guess}(W). \tag{36}$$

In this case, (34) naturally follows from the encoding on the computational basis, while Eq. (35) holds because $p_{guess}(W)$ denotes Bob's probability of rightly guessing which detector clicks[21], a quantity determined by Alice's preparation in the Fourier basis. This establishes a one-to-one correspondence between the detector clicking, b, and the initial dits, a_y. That is, $p_{guess}(W) = \max_b p(b | a_0 \oplus_d a_1 = n_{odd}, y) = p(b = a_y | a_0 \oplus_d a_1 = n_{odd}, y)$. Under this encoding discussed above and the multipath definitions of $\mathcal{D}$ and $\mathcal{V}$, Eq. (33) can be expressed as

$$\begin{aligned} \max_{\phi_{x_1}, \phi_{x_2}, \ldots, \phi_{x_{d-1}}} p_{suc} = \tfrac{1}{2d^2} \sum_y \Bigg[&\sum_{a_0 \oplus_d a_1 = n_{even}} \frac{(d-1)\mathcal{D}_{a_0 a_1, y} + 1}{d} \\ &+ \sum_{a_0 \oplus_d a_1 = n_{odd}} \frac{(d-1)\mathcal{V}_{a_0 a_1, y} + 1}{d} \Bigg]. \end{aligned} \tag{37}$$

Although this encoding is not the optimal quantum strategy for the $(2 \mapsto 1, d)$ RAC, which would require d^2 distinct preparations, it retains a clear operational meaning for $\mathcal{D}$ and $\mathcal{V}$, making it suitable for an interferometric framework while still offering quantum advantage over classical devices. It becomes especially evident when assuming the particular case where $\mathcal{D}_{a_0, a_1, y} = \mathcal{D}$ and $\mathcal{V}_{a_0, a_1, y} = \mathcal{V} \forall a_0, a_1, y$. In this case Eq. (37) simplifies to

$$\max_{\phi_{x_1}, \phi_{x_2}, \ldots, \phi_{x_{d-1}}} p_{suc} = \frac{1}{2d}[(d-1)(\mathcal{D} + \mathcal{V}) + 2]. \tag{38}$$

This relation connects the interferometric quantities $\mathcal{D}$ and $\mathcal{V}$ directly to the RAC performance. If the classicality condition $\mathcal{D}+\mathcal{V}\leq 1$ holds, the success probability in (38) reaches at most the classical bound $(1+1/d)/2$. Conversely, whenever $\mathcal{D}+\mathcal{V}>1$, a quantum advantage emerges.

To ensure consistency with the fundamental quantum limit of the $(2\mapsto 1, d)$ RAC, we impose that the success probability (38) cannot exceed the optimal quantum value:

$$p_{\text{suc}}^{(\text{quantum})}\leq \frac{1}{2}\left(1+\frac{1}{\sqrt{d}}\right). \tag{39}$$

Substituting Eq. (38) into the above expression yields a dimension-dependent constraint on the allowed combinations of distinguishability and visibility:

$$\mathcal{D}+\mathcal{V}\leq \frac{d-2+\sqrt{d}}{d-1}. \tag{40}$$

This inequality represents a quantum-restricted complementarity relation for multipath interferometers. Note that, by setting $d=2$ we recover the explored optimal two-path limit $\mathcal{D}+\mathcal{V}\leq\sqrt{2}$. Interestingly, the bound in Eq. (40) is tight, as it is saturated by the optimal quantum strategies achieving the maximal RAC success probability in dimension d. Finally, one can explore the equivalence between WPDRs and EURs to write a lower bound of the min-entropy for a given fixed max-entropy for multipath interferometers

$$H_{\min}(Z)\geq 1-\log_2\left(1+\frac{d-2+\sqrt{d}}{d-1}-\sqrt{1-\left(2^{H_{\max}(W)}-1\right)^2}\right). \tag{41}$$

Equation (41) provides a lower bound on the min-entropy associated with the path observable Z given the observed wave entropy $H_{\max}(W)$. Operationally, this means that the path information retains an irreducible amount of uncertainty, even in the presence of maximal interference visibility allowed by quantum mechanics. Although no explicit environment or side information is included here, the structure of Eq. (41) mirrors that of entropic uncertainty relations used in quantum cryptography. In this sense, the relation captures an intrinsic and dimension-dependent informational constraint, which forms the basis upon which semi-device-independent security can potentially be built, even though a full cryptographic interpretation would require incorporating side information explicitly.

Discussion

Recent developments have revealed that WPD can be understood as an optimized EUR involving min- and max-entropies[20,27], providing it with a clear operational meaning rooted in information theory. This perspective bridges a foundational concept, central to debates on the nature of light and the interpretation of quantum mechanics, including the famous EPR-Bohr debate with the language of communication theory. It reinforces the view that quantum mechanics is fundamentally an informational theory. Building on this insight, our work establishes a direct theoretical connection between WPD, quantified by generic input distinguishabilities ($\mathcal{D}$) and interferometric visibilities ($\mathcal{V}$), and the SDI QKD framework, linking duality to classical dimension bounds and security conditions relevant to quantum communication.

To illustrate our main result, we focused on a symmetric scenario involving two measurements realized through a TBS in the measurement setting. This choice allowed us to express a SDI witness in a simple form: $S=2(\mathcal{D}+\mathcal{V})$. This relation offers a clear and physically meaningful way to interpret quantum behavior in communication tasks such as the QRAC. Notably, it reveals that neither extreme particle-like behavior ($\mathcal{D}=1$, $\mathcal{V}=0$) nor extreme wave-like behavior ($\mathcal{D}=0$, $\mathcal{V}=1$) suffices to certify non-classicality in the SDI framework, highlighting that quantum advantage arises from a balanced interplay between these complementary aspects. This insight is consistent with previous findings, such as the demonstrated insecurity of the BB84 protocol in SDI scenarios[34]. Consequently, schemes that rely solely on extreme wave-particle behaviors, such as the delayed-choice cryptographic protocol[29], also fail to provide SDI-certified quantum advantage.

Importantly, the same experimental assessment can be expressed directly in terms of entropic quantities $H_{\max}(W)$ and $H_{\min}(Z)$, providing an alternative formulation of the SDI witness. In this entropic plane, surpassing the classical bound defines a necessary condition for cryptographic security within the SDI framework, which is achieved in quantum mechanics up to the optimal point $\mathcal{D}=\mathcal{V}=1/\sqrt{2}$. SDI security is determined by the intersection between the region allowed by the entropic uncertainty relation and the region defined by the security bound. Our experimental results (Fig. 4) confirm this behavior, showing that security is guaranteed for a wide range of $H_{\max}(W)$ values. This provides a complementary perspective on quantum advantage, now expressed entirely in terms of entropic quantities rather than visibility and distinguishability.

As a proof of principle, we experimentally demonstrated the SDI certification of non-classicality in a prepare-and-measure scenario based on complementary measures of distinguishability $\mathcal{D}$ and visibility $\mathcal{V}$ of a quantum state. Our experiment was based on a dynamic fiber-optical platform in which we are able to continuously change between $\mathcal{D}$ and $\mathcal{V}$ measurement operators, and furthermore further demonstrates the experimental possibilities of performing quantum information processing using OAM states within an optical fiber platform. By expressing the SDI witness in terms of $\mathcal{D}$ and $\mathcal{V}$, our work connects foundational principles of quantum mechanics with operationally relevant quantities. It shows that WPD, when treated quantitatively and beyond its idealized extremes, can serve as a useful tool for certifying quantum behavior in practical communication tasks.

The results presented here not only deepen the conceptual understanding of duality-based experiments but also inform a new design of SDI-secure quantum technologies. From a foundational viewpoint, the SDI framework relaxes the fully device-independent approach, enabling scalable cryptographic security even in extreme adversarial settings where sources and devices are completely untrusted and uncharacterized[34,40]. Building on this perspective, our work paves the way for further advances in SDI-QKD under realistic conditions. A promising direction for future work is to explore whether this interferometric decomposition offers advantages over standard SDI approaches, particularly in the presence of no-click events and potential eavesdropping strategies. Further strengthening of the bounds presented here could be achieved by employing amplification and post-processing protocols.

We have established a consistent theoretical foundation for multi-path interferometers, integrating the generalized definitions of distinguishability and visibility proposed in ref. 21 for systems with an initial symmetric beam splitter into our framework. However, deriving explicit key-rate formulas for d-dimensional protocols remains an open problem. Addressing this challenge in future work could not only provide a quantitative security characterization for higher-dimensional SDI-QKD but also further elucidate the operational role of interferometric complementarity in quantum communication. Additionally, exploring the framework under more general eavesdropping scenarios, such as collective or coherent attacks, or extending it to the certification of quantum random number generation (QRNG), represents a natural extension of this work.

Methods

Improving the security bound in the SDI scenario

The security framework of ref. 34 establishes that in a 2-to-1 QRAC scenario, security is guaranteed if $P_B>0.8415$, where P_B denotes the probability that Bob correctly infers the bit sent by Alice. In this section, we derive a tighter security bound on P_B refining the condition for secure SDI-QKD. Consider the success probability of Bob and Eve (the eavesdropper), trying

to guess $a_0 \oplus a_1$. We have,

$$P_{B,E}(a_0 \oplus a_1) \geq P_{B,E}(a_0, a_1) \tag{42}$$

$$\geq P_{B,E}(a_0) + P_{B,E}(a_1) - 1. \tag{43}$$

where $P_{B,E}(a_0, a_1)$ (equivalently,$P_{B,E}(a_0 \cap a_1)$) is the likelihood that Bob and Eve guess both a_0 and a_1 correctly. The second inequality follows from the identity $P_{B,E}(a_0 \oplus a_1) = P_{B,E}(a_0 \cup a_1) - P_{B,E}(a_0 \cap a_1)$ along with the upper bound $P_{B,E}(a_0 \cup a_1) = P_{B,E}(a_0) + P_{B,E}(a_1) - P_{B,E}(a_0 \cap a_1) \leq 1$.

For simplicity, we assume that a_0 and a_1 are uniformly distributed random variables, implying $P_{B,E}(a_0) = P_{B,E}(a_1)$, therefore (43) becomes,

$$P_{B,E}(a_0 \oplus a_1) \geq 2P_{B,E}(a_0) - 1 \tag{44}$$

$$= 2P_{B,E} - 1. \tag{45}$$

where $P_{B,E}$ denotes Bob's average success probability. We consider the worst-case scenario where Bob and Eve collaborate under the constraints: $P_{B,E}(a_i) \geq P_B(a_i)$ and $P_{B,E}(a_i) \geq P_E(a_i)$. Using these constraints (45) becomes,

$$P_{B,E}(a_0 \oplus a_1) \geq 2P_E - 1 \tag{46}$$

To derive a better bound on P_B, we employ an inequality on the expectation values of a_0, a_1, and $a_0 \oplus a_1$

$$[E(a_0)]^2 + [E(a_1)]^2 + [(E(a_0 \oplus a_1)]^2 \leq 1. \tag{47}$$

This inequality first appeared in[41]. Here we provide an independent proof to ensure completeness and clarity.

Without loss of generality, one can write $\rho = \frac{1}{2}(I + \mathbf{n}.\boldsymbol{\sigma})$, where $\mathbf{n}$ is the Bloch vector and $\boldsymbol{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ are the Pauli matrices. Similarly, the measurement operators along the direction $\mathbf{m}_i$ (where $i = \{0, 1, 2\}$) can be described by $M_i = \frac{1}{2}(I + \mathbf{m}_i.\boldsymbol{\sigma})$. Thus, the expectation value corresponding to each measurement i is given by

$$E_i = 2\,\mathrm{Tr}[\rho \mathrm{M_i}] - 1 = (\mathbf{n}.\mathbf{m}_i). \tag{48}$$

Now, we consider the expectation values $E_i(f_j)$ of the function f_j, estimated from Bob's collected statistics, where $f_j = \{a_0, a_1, a_0 \oplus a_1\}$. In this case, we have:

$$\begin{aligned} \sum_{i=a_0,a_1,a_0\oplus a_1} [E_i(f_i)]^2 &= [E(a_0)]^2 + [E(a_1)]^2 + [E(a_0 \oplus a_1)]^2 \\ &= \sum_i (\mathbf{n}.\mathbf{m}_i)^2 \leq |n|^2 \sum_i \mathbf{m}_i. \end{aligned} \tag{49}$$

Since $\sum_i \mathbf{m}_i \leq 1$, and $|n|^2 \leq 1$, we have (47) as a result.

Since $E(a_0 \oplus a_1) = 2P_{B,E}(a_0 \oplus a_1) - 1$, $E(a_0) = 2P_{B,E}(a_0) - 1$ and $E(a_1) = 2P_{B,E}(a_1) - 1$, (47) simplifies to,

$$P_{B,E}(a_0 \oplus a_1) \leq \frac{1 + \sqrt{(1 - 2(2P_{B,E} - 1)^2)}}{2} \tag{50}$$

$$\leq \frac{1 + \sqrt{(1 - 2(2P_B - 1)^2)}}{2} \tag{51}$$

Using (46), we derive an upper bound on P_E

$$P_E \leq \frac{3 + \sqrt{(1 - 2(2P_B - 1)^2)}}{4}. \tag{52}$$

This implies that $P_B > P_E$ as long as $P_B > 0.833$. In the following, we present our experimental verification of the SDI witness in terms of interferometric distinguishability and visibility.

Interferometric model

The interferometric setup under analysis is illustrated in Fig. 2. Each optical component is modeled by its corresponding matrix operator

$$BS_1 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & i \\ i & 1 \end{pmatrix}, \quad BS_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} i & -1 \\ -1 & i \end{pmatrix}, \tag{53}$$

$$PM_1 = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi_x} \end{pmatrix}, \quad PM_2 = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\phi_s} \end{pmatrix}. \tag{54}$$

By applying these transformations, the output state becomes

$$\begin{aligned} |\psi\rangle = \tfrac{1}{2\sqrt{2}} \big[& i\big((1 + e^{i\phi_s}) + e^{i\phi_x}(1 - e^{i\phi_s})\big)|D_0\rangle \\ & + \big((e^{i\phi_s} - 1) - e^{i\phi_x}(1 + e^{i\phi_s})\big)|D_1\rangle \big] \end{aligned} \tag{55}$$

The detection probabilities at detectors D_0 and D_1 are then given by

$$p_0 = |\langle D_0|\psi\rangle|^2 = \frac{1}{2}(1 + \sin\phi_x \sin\phi_s) \tag{56}$$

$$p_1 = |\langle D_1|\psi\rangle|^2 = \frac{1}{2}(1 - \sin\phi_x \sin\phi_s) \tag{57}$$

Maximizing and minimizing these probabilities allows us to extract the interferometric visibility:

$$\mathcal{V} = \sin\phi_s \tag{58}$$

To compute the distinguishability, we consider blocking one of the interferometric paths. If the upper path is blocked, the resulting state is

$$|\psi\rangle = \frac{1}{2}\big[i(1 + e^{i\phi_s})|D_0\rangle + (1 - e^{i\phi_s})|D_1\rangle\big] \tag{59}$$

Since the phase ϕ_x becomes irrelevant when only one path is available, the distinguishability becomes

$$\mathcal{D} = \cos\phi_s \tag{60}$$

Experiment

The experimental setup resorts to a fiber-optical MZI where the input BS is composed of a PL, which takes a few-mode fiber (FMF) as an input, and splits the corresponding linearly polarized (LP) modes supported by the FMF. The FMF employed is a 3-mode fiber from OFS, supporting the fundamental Gaussian $|LP_{01}\rangle$ mode, as well as $|LP_{11a}\rangle$ and $|LP_{11b}\rangle$. In our case we only use the two higher-order ones, as they form the linear decomposition of the $|OAM_{+1}\rangle$ mode. The $|OAM_{+1}\rangle$ state itself is generated from heavily attenuated laser pulses generated from an electro-optical $LiNbO_3$ fiber pigtailed amplitude modulator connected to the output of a direct feedback (DFB) laser diode emitting at the wavelength of 1546 nm. The amplitude modulator is driven from a signal generator creating 40 ns wide optical pulses at 150 kHz repetition rate. The attenuator is adjusted such that there is an average photon number per pulse of $\mu = 0.2$ following the poissonian distribution $P(n) = \mu^n e^{-\mu}/n!$ just before the TBS, which is where the measurement operation takes place. The detector has an overall detection efficiency of 10% and coupled with the experimental detection losses, no-click events are discarded based on the fair sampling assumption.

The OAM state is generated with a free-space setup based on a spatial light modulator (SLM). A 10 × objective is used to collimate the light beam

before passing through a polarizer to prepare a horizontal polarization state before impinging onto the SLM, which has an appropriate forked hologram displayed, creating the $|OAM_{+1}\rangle$ on the first diffraction order. A 4f optical system is employed together with a pinhole spatially filtering the reflected beam from the SLM, and then coupled into the FMF with a 20 × objective. A manual polarization controller with the FMF wound through the paddles is used to compensate for the disturbances of spatial distribution on the FMF, ensuring optimal splitting of the $|LP_{11a}\rangle$ and $|LP_{11b}\rangle$. The employed PL (Phoenix Photonics) gives around 16 dB of extinction ratio between the used outputs, and around 5 dB of average insertion loss.

Following the interferometer, the TBS is implemented through a fiber-optical Sagnac interferometer. The two counter propagating directions in the Sagnac loop recombine back at the input beamsplitter, and depending on the relative phase difference ϕ_s between the two directions, the detection probability at detectors D_0 and D_1 (following the optical circulators) is proportional to $cos^2(\phi_s)$ and $sin^2(\phi_s)$ respectively. An optical fiber delay inside the Sagnac loop (300 m long for convenience) is employed to ensure that the modulator ϕ_s only acts in one of the opposing internal propagation directions. Following the circulators we employ one single-photon detector (SPD) module based on an avalanche InGaAs photodiode in gated mode (IdQuantique id210). In order to be able to detect both outputs with a single-detector, we resort to a time-multiplexing scheme, where a $\Delta\tau = 1250$ ns optical fiber delay is inserted onto one of the outputs, and then both are recombined with a polarizing beam splitter (PBS) and the output connected to the SPD. This time delay was chosen based on the internal deadtime of the detector, which is set to minimize false counts from afterpulsing events. Manual polarization controllers are employed to maximize transmission through both inputs of the PBS. This scheme effectively maps the two outputs from the interferometer onto a single detector, with the drawback of limiting the repetition rate of the experiment.

Data availability

Data is provided within the manuscript or supplementary information files.

Received: 4 June 2025; Accepted: 4 December 2025;
Published online: 23 December 2025

References

1. Dieguez, P. R., Guimarães, J. R., Peterson, J. P., Angelo, R. M. & Serra, R. M. Experimental assessment of physical realism in a quantum-controlled device. *Commun. Phys.* **5**, 82 (2022).
2. Saunders, S. Complementarity and scientific rationality. *Found. Phys.* **35**, 417–447 (2005).
3. Young, T. The Bakerian Lecture. experiments and calculations relative to physical optics. *Philos. Trans. R. Soc.* **94**, 1–16 (1804).
4. King, B., Di Piazza, A. & Keitel, C. H. A matterless double slit. *Nat. Photonics* **4**, 92–94 (2010).
5. Tirole, R. et al. Double-slit time diffraction at optical frequencies. *Nat. Phys.* **19**, 999–1002 (2023).
6. THOMSON, G. & REID, A. Diffraction of cathode rays by a thin film. *Nature* **119**, 890 (1927).
7. Zimmermann, B. et al. Localization and loss of coherence in molecular double-slit experiments. *Nat. Phys.* **4**, 649–655 (2008).
8. Liu, X.-J. et al. Einstein–Bohr recoiling double-slit gedanken experiment performed at the molecular level. *Nat. Photonics* **9**, 120–125 (2015).
9. Wheeler, J. A. & Zurek, W. H.*Quantum theory and measurement*, vol. 15 (Princeton University Press, 2014).
10. Peres, A. & Terno, D. R. Quantum information and relativity theory. *Rev. Mod. Phys.* **76**, 93–123 (2004).
11. Kaiser, F., Coudreau, T., Milman, P., Ostrowsky, D. B. & Tanzilli, S. Entanglement-enabled delayed-choice experiment. *Science* **338**, 637–640 (2012).
12. Auccaise, R. et al. Experimental analysis of the quantum complementarity principle. *Phys. Rev. A* **85**, 032121 (2012).
13. Catani, L., Leifer, M., Scala, G., Schmid, D. & Spekkens, R. W. What is nonclassical about uncertainty relations? *Phys. Rev. Lett.* **129**, 240401 (2022).
14. Catani, L., Leifer, M., Scala, G., Schmid, D. & Spekkens, R. W. Aspects of the phenomenology of interference that are genuinely nonclassical. *Phys. Rev. A* **108**, 022207 (2023).
15. Dieguez, P. R. & Angelo, R. M. Information-reality complementarity: The role of measurements and quantum reference frames. *Phys. Rev. A* **97**, 022107 (2018).
16. Lustosa, F. R., Dieguez, P. R. & da Paz, I. G. Irrealism from fringe visibility in matter-wave double-slit interference with initial contractive states. *Phys. Rev. A* **102**, 052205 (2020).
17. Lustosa, F. et al. Emergence of realism through quantum discord suppression in photonic weak measurements. *New J. Phys.* **27**, 054503 (2025).
18. Jaeger, G., Shimony, A. & Vaidman, L. Two interferometric complementarities. *Phys. Rev. A* **51**, 54–67 (1995).
19. Englert, B.-G. Fringe visibility and which-way information: An inequality. *Phys. Rev. Lett.* **77**, 2154–2157 (1996).
20. Coles, P. J., Kaniewski, J. & Wehner, S. Equivalence of wave-particle duality to entropic uncertainty. *Nat. Commun.* **5**, 5814 (2014).
21. Coles, P. J. Entropic framework for wave-particle duality in multipath interferometers. *Phys. Rev. A* **93**, 062111 (2016).
22. Coles, P. J., Berta, M., Tomamichel, M. & Wehner, S. Entropic uncertainty relations and their applications. *Rev. Mod. Phys.* **89**, 015002 (2017).
23. Scarani, V. et al. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301 (2009).
24. Berta, M., Christandl, M., Colbeck, R., Renes, J. M. & Renner, R. The uncertainty principle in the presence of quantum memory. *Nat. Phys.* **6**, 659–662 (2010).
25. Mizutani, A., Sasaki, T., Kato, G., Takeuchi, Y. & Tamaki, K. Information-theoretic security proof of differential-phase-shift quantum key distribution protocol based on complementarity. *Quantum Sci. Technol.* **3**, 014003 (2017).
26. Zhang, X., Zeng, P., Ye, T., Lo, H.-K. & Ma, X. Quantum complementarity approach to device-independent security. *Phys. Rev. Lett.* **131**, 140801 (2023).
27. Spegel-Lexne, D. et al. Experimental demonstration of the equivalence of entropic uncertainty with wave-particle duality. *Sci. Adv.* **10**, eadr2007 (2024).
28. Koashi, M. Simple security proof of quantum key distribution based on complementarity. *N. J. Phys.* **11**, 045018 (2009).
29. Ardehali, M. Quantum cryptography based on Wheeler's delayed choice experiment. *Phys. Lett. A* **217**, 301–304 (1996).
30. Acín, A., Gisin, N. & Masanes, L. From Bell's theorem to secure quantum key distribution. *Phys. Rev. Lett.* **97**, 120405 (2006).
31. Scarani, V. et al. Secrecy extraction from no-signaling correlations. *Phys. Rev. A* **74**, 042339 (2006).
32. Primaatmaja, I. W. et al. Security of device-independent quantum key distribution protocols: a review. *Quantum* **7**, 932 (2023).
33. Saha, D., Oszmaniec, M., Czekaj, L., Horodecki, M. & Horodecki, R. Operational foundations for complementarity and uncertainty relations. *Phys. Rev. A* **101**, 052104 (2020).
34. Pawłowski, M. & Brunner, N. Semi-device-independent security of one-way quantum key distribution. *Phys. Rev. A—At., Mol., Optical Phys.* **84**, 010302 (2011).
35. Birks, T. A., Gris-Sánchez, I., Yerolatsitis, S., Leon-Saval, S. G. & Thomson, R. R. The photonic lantern. *Adv. Opt. Photon.* **7**, 107–167 (2015).
36. Alarcón, A., Argillander, J., Lima, G. & Xavier, G. Few-mode-fiber technology fine-tunes losses in quantum communication systems. *Phys. Rev. Appl.* **16**, 034018 (2021).
37. Konig, R., Renner, R. & Schaffner, C. The operational meaning of min- and max-entropy. *IEEE Trans. Inf. theory* **55**, 4337–4347 (2009).

38. Qureshi, T. Interference visibility and wave-particle duality in multipath interference. *Phys. Rev. A* **100**, 042105 (2019).
39. Farkas, M. & Kaniewski, J. M. K. Self-testing mutually unbiased bases in the prepare-and-measure scenario. *Phys. Rev. A* **99**, 032316 (2019).
40. Mironowicz, P. et al. Quantum randomness protected against detection loophole attacks. *Quant. Info. Proc.* **20**, https://doi.org/10.1007/s11128-020-02948-3 (2021).
41. Pawłowski, M. & Winter, A. "hyperbits": The information quasiparticles. *Phys. Rev. A* **85**, 022331 (2012).

Acknowledgements

This work was supported by Zenith Linköping University and the Wallenberg Center for Quantum Technologies. This work was partially supported by the Foundation for Polish Science (IRAP project, ICTQT, contract No. MAB/218/5, co-financed by EU within the Smart Growth Operational Programme). M.P., C.R., and P.R.D. acknowledge support from the NCN Poland, ChistEra-2023/05/Y/ST2/00005 under the project Modern Device Independent Cryptography (MoDIC). A.C. acknowledges financial support by NCN grant SONATINA 6 (contract No. UMO-2022/44/C/ST2/00081). This work is partially carried out under IRA Programme, project no. FENG.02.01-IP.05-0006/23, financed by the FENG program 2021-2027, Priority FENG.02, Measure FENG.02.01., with the support of the FNP.

Author contributions

P.R.D. proposed the project. C.J., T.P., A.C., L.P., M.P., and P.R.D. developed the theoretical results. D.S.L., S.G., J.A., A.A., and G.B.X. performed the experiment. All authors contributed to writing and data analysis.

Competing interests

The authors declare no competing interests.

Additional information

Correspondence and requests for materials should be addressed to Guilherme B. Xavier or Pedro R. Dieguez.

Entanglement is not sufficient for most practical entanglement-based QKD protocols

Shubhayan Sarkar[1], Tushita Prasad[2], and Karol Horodecki[1]
[1]*Institute of Informatics, Faculty of Mathematics, Physics and Informatics, University of Gdansk, Wita Stwosza 57, 80-308 Gdansk, Poland*
[2]*ICTQT, University of Gdansk, Wita Stwosza 57, 80-308 Gdansk, Poland*

Quantum key distribution (QKD) is the most explored application of quantum information theory. A central problem in entanglement-based QKD (EB-QKD), is whether every entangled state can be used to extract a key. We observe that entanglement is not sufficient for standard practical EB-QKD protocols where the input choices are announced by the parties that want to share a secure key, such as E91 or entanglement-based BB84 type protocols, when even an arbitrarily small amount of leakage of classical side information occurs. We do this by identifying a class of two-qubit isotropic states that are entangled but cannot be used to distil the key under such protocols for any possible measurement by the parties. Counter-intuitively, this gap persists even when the leakage occurs from the "junk" rounds of the protocol, i.e, rounds that cannot be used to generate any key. We then extend this result to arbitrary dimensions and parties by identifying a class of isotropic states that are not useful to extract a secure key under such protocols, even if they are entangled. Finally, we demonstrate that our approach provides a tool to upper-bound the scalability of repeater-based QKD architectures in a protocol-independent manner. Interestingly, we find that allowing for even a tiny noise in the preparation drastically reduces the scalability of the QKD network.

Introduction—Quantum Key Distribution (QKD) is one of the most prominent practical applications of quantum information science, enabling information-theoretically secure communication between spatially separated users based on the laws of quantum mechanics. The first QKD protocol, BB84 [1], relies on encoding information in non-orthogonal quantum states, ensuring that any eavesdropping attempt necessarily introduces detectable disturbances. This paradigm was later extended to entanglement-based schemes, such as E91 [2], which relates security to the violation of Bell inequalities, and BBM92 [3], the entanglement-based version of BB84, where key generation is achieved through measurements on shared entangled states.

Security proofs of essentially all standard device-dependent QKD protocols including the six-state protocol [4], B92 [5], decoy-state BB84 [6], and measurement-device-independent QKD [7] are based on an equivalent entanglement-based description. Indeed, it was shown in Ref. [8] that a necessary condition for secure key distribution is that the legitimate users can certify entanglement in the effectively distributed quantum state. Relatedly, protocols that rely on Bell inequality violations [9, 10] necessarily require entangled sources. These results firmly establish entanglement as the fundamental resource underlying quantum key distribution.

This naturally raises a foundational question: Is the presence of entanglement sufficient to guarantee secure key distribution? In other words, can every entangled state be used to establish a secret key between spatially separated parties? Remarkably, Ref. [11] shows that even bound entangled states, from which pure entanglement cannot be distilled, can nevertheless yield a secure key. Moreover, the distillable key was later shown to be upper-bounded by the relative entropy of entanglement and refined in terms of the intrinsic information of an adversary [12]. Since these quantities are entanglement monotones [13], one might be tempted to conclude that entanglement alone suffices for QKD.

In this work we show that this intuition breaks down once one moves beyond the idealized setting. Practical QKD implementations are inevitably subject to imperfections and classical side-channel leakage. Experimental demonstrations and implementation-level attacks have shown how such leakage can compromise security [14–18]. On the theoretical side, a substantial body of work has analysed QKD under specific leakage models arising from imperfect or flawed sources, including leaky modulators, Trojan-horse attacks, and model-dependent imperfections [19–23]. Nevertheless, these works focus on particular leakage mechanisms and protocol-specific settings, leaving open a more fundamental question regarding the role of entanglement in the presence of general classical side information.

Addressing these aspects, we develop a general quantitative framework to analyze *classical side-channel leakage* in standard EB-QKD protocols and allows us to compute upper-bound to key rate in presence of leakage. Within this framework, we quantify a fundamental separation between entanglement and key extractability: even arbitrarily small leakage can create a gap between states that are entangled and states from which a secret key can actually be distilled. This gap persists even if the leakage occurs only from "junk" rounds of the protocol, that is, rounds from which no secure key could be extracted. By standard protocols, we mean those in which users directly extract the secret key from their measurement outcomes after publicly announcing their inputs, such as entanglement-based BB84 (BBM92), E91, and related schemes. These protocols may also be referred to

as quantum-memoryless protocols, since the key is extracted via direct measurements on the received subsystems combined with public communication, without requiring quantum memory. Protocols that rely on additional iterative quantum procedures, such as the Gottesman–Lo protocol [24], fall outside this framework and are not considered here.

To establish this separation between entanglement and key extractability explicitly, we apply our framework to entanglement-based protocols using isotropic states. We then explicitly construct an attack that renders the secret-key rate zero for a class of entangled states under arbitrarily small leakage. We extend the analysis to higher-dimensional and multipartite isotropic states and further derive numerical upper bounds on the maximal key rate achievable from any entangled state in the presence of leakage. We illustrate these bounds for isotropic states [25] in dimensions two and three, thereby obtaining quantitative, protocol-independent limits on key generation under classical side information.

Finally, to demonstrate the general applicability of our approach, we also consider repeater-based QKD architectures, which aim to overcome channel loss by dividing long communication distances into shorter elementary links connected via intermediate nodes. Using our approach, we derive fundamental bounds on the maximum number of repeaters that can be concatenated while still enabling secure key generation over standard protocols in the presence of classical side-channel leakage. These results provide operational limits on the scalability of practical QKD networks under leakage, highlighting how even a small amount of leaked information can drastically reduce the maximum achievable distance and number of repeaters, which is pivotal for the design of future quantum communication technologies.

Entanglement-based QKD— Consider a scenario with N parties, labeled A_i for $i = 1, \ldots, N$, who aim to establish a shared secret key. In an EB-QKD protocol, each party receives a subsystem from a quantum source and performs measurements with freely chosen inputs x_i, producing outcomes a_i. For compactness, we denote the full set of inputs and outcomes as $\vec{x} = \{x_1, \ldots, x_N\}$ and $\vec{a} = \{a_1, \ldots, a_N\}$, respectively. The source prepares a joint state $\rho_{A_1 \ldots A_N}$, and the measurement operators of party A_i are $\{M_{a_i|x_i}\}$. The resulting correlations are captured by the joint probability distribution

$$\vec{p} = \{p(\vec{a}|\vec{x})\}, \quad p(\vec{a}|\vec{x}) = \mathrm{Tr}\left(\bigotimes_{i=1}^{N} M_{a_i|x_i} \, \rho_{A_1 \ldots A_N} \right).$$

In this work, we focus on standard entanglement-based protocols in which the inputs of both parties are publicly announced. Such protocols are the most studied ones in QKD [for instance see Refs. [2, 26–31]].

The execution of such protocols is typically divided into parameter estimation rounds and key generation rounds. In the parameter estimation stage, a randomly chosen subset of the raw data is publicly disclosed and used to estimate the relevant channel parameters, such as the quantum bit error rate (QBER) or correlations needed for security proofs. This step provides a statistical guarantee against potential eavesdropping and determines whether the protocol should be aborted. The undisclosed portion of the data constitutes the key generation rounds, from which the raw key is distilled. Subsequent post-processing steps, namely error correction and privacy amplification, are then applied to transform this raw key into a secure final secret key.

The above description assumes that the adversary's information is limited to what can be obtained through interaction with the quantum channel and the publicly announced communication. In practice, however, one can never negate the existence of classical side channels. For instance, when a detector produces a classical bit, that outcome is encoded in electrical signals such as current spikes, voltage changes, timing signals, or electromagnetic emissions. If these physical signatures differ even slightly depending on the measurement result, an eavesdropper may infer partial information about the outcome without directly interacting with the quantum channel . In security terms, such leakage creates additional correlations between the key and the adversary, effectively increasing Eve's information. To model this effect quantitatively, we consider that each measurement outcome is leaked to the adversary with a finite probability $\mathcal{L}$.

Convex combination attacks— Consider now that there is an adversary, Eve, who wants to intrude on the protocol and guess the key established between the parties. There exist a variety of attacks that allow Eve to remain undetected during the parameter-estimation rounds while still being able to access the key (see, e.g., Refs. [30, 31] for a review). Here, we consider the simplest yet one of the most realistic adversarial attacks, known as convex combination (C.C.) attack. Originally introduced in [32, 33] for the device-independent setting, the C.C. strategy adapted here to the device-dependent setup involves reproducing correlations between Alice and Bob by mixing correlations generated by separable and entangled states, that is, given a correlation $\{p(\vec{a}|\vec{x})\}$ it can be expressed as,

$$p(\vec{a}|\vec{x}) = q_{\mathcal{S}} p^{\mathcal{S}}(\vec{a}|\vec{x}) + (1 - q_{\mathcal{S}}) p^{\mathcal{E}}(\vec{a}|\vec{x}) \tag{1}$$

where $\{p^{\mathcal{S}}(\vec{a}|\vec{x})\}$ can be realised using a separable state and $\{p^{\mathcal{E}}(\vec{a}|\vec{x})\}$ can be realised using an entangled state with $0 \leq q_{\mathcal{S}} \leq 1$.

We introduce a classical variable $e \in \{\mathcal{S}, \mathcal{E}\}$ that tells Eve which part of the mixture is being distributed in

the current round, the separable state or the entangled state. Using this labeling, we can now quantify the maximum key extractable from the protocol in terms of Eve's knowledge. This is captured by the intrinsic information $I(A_1, A_2, \ldots, A_N \downarrow e)$, [12, 34, 35] where

$$I(A_1 \ldots A_N \downarrow e)_\rho = \inf_{\rho' = (\mathbb{1}_{A_1 \ldots A_N} \otimes \Lambda_E)\rho} I(A_1 \ldots A_N | e)_{\rho'}. \tag{2}$$

Here, Λ_E is any operation that can be performed by Eve with $I(A_1 \ldots A_N|e)_{\rho'}$ denoting the mutual information of all parties conditioned on Eve. If the shared state is separable, then Eve can perfectly predict the outcomes associated with the separable component, thereby precluding the establishment of any secure key among the parties. As a result, $I(A_1 \ldots A_N \downarrow e)_{\rho^S} = 0$ for any separable state. Here, we do not minimize the conditional mutual information over all possible maps of Eve but only consider the specific C.C. attack by Eve. Consequently, we obtain the upper bound to the key, denoted as $I(A_1 \ldots A_N|e, C.C.)$. Moreover, as the conditional mutual information is convex over e, the key rate R is upper-bounded by

$$R \leq \frac{1}{N-1} \sum_e \sum_{\vec{x}} p_{\vec{x}} p(e|\vec{x}) I_{\vec{x}}(A_1 \ldots A_N|e, C.C.) \tag{3}$$

where $I_{\vec{x}}(A_1 \ldots A_N|e, C.C.)$ is the conditional mutual information of all parties given inputs $\vec{x}$. We now present the main results of this work.

Bipartite scenario— For simplicity, we first consider the bipartite scenario, where two parties A_1, A_2 want to establish a key among themselves using an EB-QKD protocol. Suppose now that the source prepares a two-qubit isotropic state,

$$\rho_v = v|\phi^+\rangle\langle\phi^+| + (1-v)\mathbb{1}/4. \tag{4}$$

It is well-known that this state is entangled for $v \geq 1/3$ and separable otherwise [36]. The correlations $\{p^v(a_1, a_2|x_1, x_2)\}$ are computed as $p^v(a_1, a_2|x_1, x_2) = \mathrm{Tr}(M_{a_1|x_1} \otimes M_{a_2|x_2} \rho_v)$.

Theorem 1. *Consider the QKD protocol described above with a leakage paramter $\mathcal{L}$, which is implemented using the isotropic state ρ_v (4). Then, for any two-outcome measurements with all parties, Eve can find a C.C. attack such that no secure key can be extracted for (i) $v \leq \frac{1}{3} + \frac{2\mathcal{L}}{3-2\mathcal{L}}$ for uniform leakage, (ii) $v \leq \frac{1}{3} + \frac{2\mathcal{L}}{3(\mathcal{L}+3)}$ for leakage only from "junk".*

We provide a brief sketch of the proof, with full details deferred to Theorem 1 in the appendix. The isotropic state ρ_v can be expressed as a convex combination of the maximally entangled state and the separable isotropic state $\rho_{1/3}$. The latter can then be expressed as a convex mixture of product states. Accordingly, Eve controls the source and distributes these product states, together with the maximally entangled state to the parties. A flag is attached to indicate which state has been sent. The local probability that outcomes leak is $\mathcal{L}$. Considering the worst-case scenario, that is, outcomes are leaked in the same rounds for both parties, Eve has complete knowledge of Alice's and Bob's measurement outcomes in those rounds. Consequently, she assigns her knowledge as $e = (a_1, a_2)$, corresponding to the outcomes at A_1 and A_2. In contrast, when the maximally entangled state is sent, Eve assigns $e =?$.

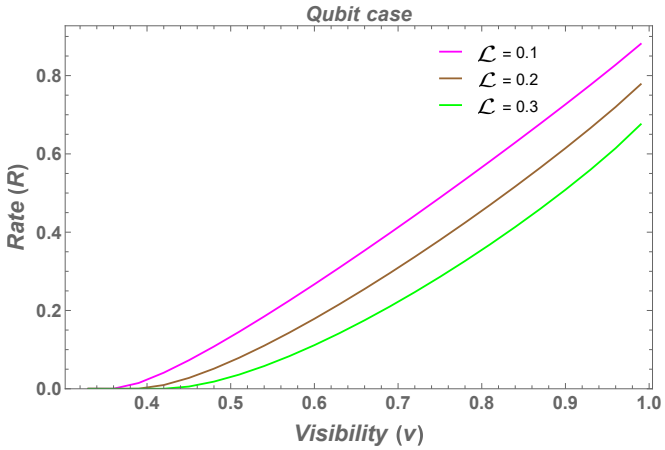

FIG. 1. Under the uniform leakage model, each of the three curves represents the upper bound on the secure key rate achievable in any protocol where both parties publicly announce their measurement inputs (when measuring the isotropic state), for leakage values $\mathcal{L} = 0.1, 0.2$ and 0.3.

We now consider two different leakage models: (i) uniform leakage, where the leakage of outcomes is independent of Eve's flag. In this case, outcomes leak with probability $\mathcal{L}$ in every round, so the fraction of leaked outcomes equals $\mathcal{L}$. (ii) leakage only from "junk", where outcomes leak only when Eve sends the separable state, i.e., from rounds that cannot generate secure key anyway. In this case, the fraction of leaked outcomes is $3\mathcal{L}(1-v)/2$ for any v, which is smaller than in the uniform leakage model. We refer to these rounds as "junk", since whenever Eve sends the separable part of the state, no secure key is generated in those rounds.

Coming back to the proof, since no secure key can be generated from product distributions, Eve's strategy to weaken the overall QKD protocol is to minimise the intrinsic information $I(A_1, A_2|e =?)$. To this end, she reassigns a fraction γ_{a_1,a_2} of events, originally arising from the separable state and yielding outcomes (a_1, a_2) to the class $e =?$. This strategy allows Eve to reduce the intrinsic information to zero, i.e., $I(A_1, A_2|e =?) = 0$. This occurs for all $v \leq 1/3 + 2\mathcal{L}/(3 - 2\mathcal{L})$ in the case of uniform leakage, and for $v \leq 1/3 + 2\mathcal{L}/[3(\mathcal{L}+3)]$ when leakage occurs only from junk rounds.

We observe that for any non-zero leakage $\mathcal{L}$, there is a

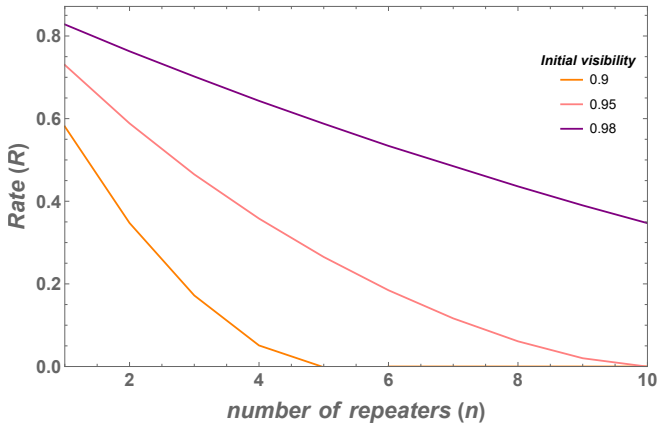

FIG. 2. Considering the uniform leakage model, we illustrate the dependence of the secure key rate R on the number of repeaters n for various initial visibilities for a particular leakage $\mathcal{L} = 0.1$, showing the rapid degradation of the rate with increasing number of repeaters.

gap between entangled states and key extractable states. Remarkably, we also observe that this effect persists even if the leakage occurs from the part of the state that could not be used to generate key. Consequently, we can conclude that even if there is an arbitarily small leakage in standard QKD protocols, every entangled state can not be used to generate secure key.

Using a similar strategy, we find the maximal value of the key that can be securely obtained from any two-qubit isotropic state. Unlike the usual approaches, we do not restrict ourselves to any particular protocol. Instead, we derive a general upper bound to the secure key rate that applies to all standard protocols where both parties announce their inputs [see Appendix B for details]. We now utilize this framework to analyze repeater-based QKD setups.

Repeater-based QKD— A quantum repeater enables QKD over very long distances by addressing a core limitation of quantum communication: photon loss and noise in optical fibers. Unlike classical signals, quantum states cannot be amplified due to the no-cloning theorem, which makes direct long-distance QKD nearly impossible beyond a few hundred kilometers. Quantum repeaters solve this problem by breaking a long channel into several shorter elementary links, creating entanglement over each short segment, and then extending that entanglement step by step using Bell-state measurements (BSMs). In this way, rather than trying to send a fragile quantum state across the full distance, the repeater constructs long-range entanglement in a modular fashion. Once the endpoints share the entanglement, they can run a standard EB-QKD protocol (e.g., E–91) to generate a secure key [37–41].

The simplest configuration with a single repeater between Alice and Bob consists of two sources generating entangled states. The first source prepares the state ρ_{AR_1}, sending one subsystem to Alice and the other to the repeater, while the other source generates another entangled state ρ_{R_1B}, sending one subsystem to the repeater and the other to Bob. In realistic channels, both sources distribute imperfect entangled states, typically modelled as isotropic states with visibility v (4). At this point, Alice and Bob are not entangled with each other; both are only connected to the repeater.

To extend entanglement across the full distance, the repeater performs a Bell-state measurement (BSM) on the subsystems $R_1^{(1)}$ and $R_1^{(2)}$. The measurement swaps the entanglement from the measurement to Alice and Bob, up to a local Pauli correction that depends on the BSM outcome and can be communicated classically. Crucially, however, when the two initial links have visibility v, the shared state that results after swapping is another isotropic state but with reduced visibility v^2. Consequently, a chain of n repeaters yields a final visibility v^{2n} on the state shared by Alice and Bob. Consequently, we conclude from Theorem 1 that one cannot obtain a secure key for $v^{2n} \leq 1/3 + 2\mathcal{L}/(3 - 2\mathcal{L})$ (considering a uniform leakage model). Therefore, for a given visibility v, the maximum number of repeater nodes $n_{\max}$ compatible with secure key

$$n_{\max} \leq \frac{\log_2(1/3 + 2\mathcal{L}/(3 - 2\mathcal{L}))}{2\log_2 v}. \tag{5}$$

As is clear from this expression, in an idealised error-free scenario, any standard protocol would, in principle, allow an arbitrarily large number of repeater nodes.

Strikingly, introducing even a modest imperfection in state preparation, on the order of only five percent (corresponding to $v = .95$) and $\mathcal{L} = .1$, drastically limits this scalability, restricting the generation of a secure key to at most ten repeaters. This highlights the extreme sensitivity of long-distance repeater-based QKD to small preparation errors. Note that in the device-independent setting, the maximal number of repeaters when restricting to the CHSH protocol was found in [42].

In Fig. 2, we illustrate this behaviour, as the key rate decreases rapidly as the number of repeaters increases. As discussed earlier, after n repeaters an initial isotropic-state visibility v is reduced to an effective visibility v^{2n}. For each value of v^{2n}, the secure key rate is computed by optimising the C.C. strategy (capturing the worst-case eavesdropping scenario), and then subsequently maximizing over Alice's and Bob's measurement settings to determine the highest achievable secure key rate consistent with that attack. Repeating this procedure for initial visibilities $v = 0.9, 0.95$, and 0.98 with $\mathcal{L} = .1$ yields the curves displayed in Fig. 2.

Generalisation to arbitrary dimension and number of parties— We now consider the most general QKD scenario as discussed above, where arbitrary number of

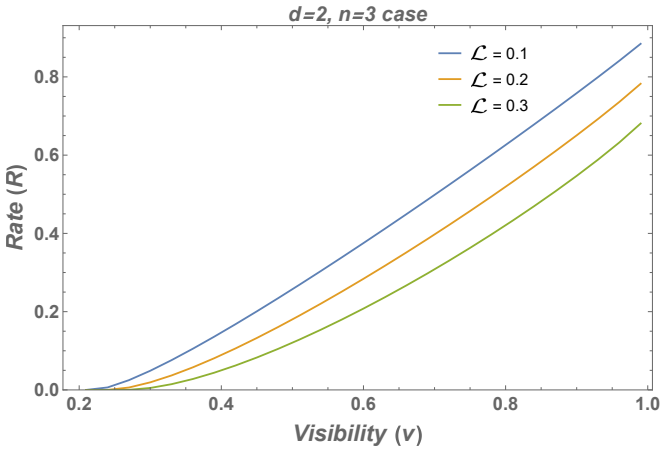

FIG. 3. Under the uniform leakage model, the three curves depict upper bounds on the secure key rate as a function of the visibility v of the isotropic state ρ_v for the $d = 2, N = 3$ scenario, with each curve corresponding to a specific leakage value.

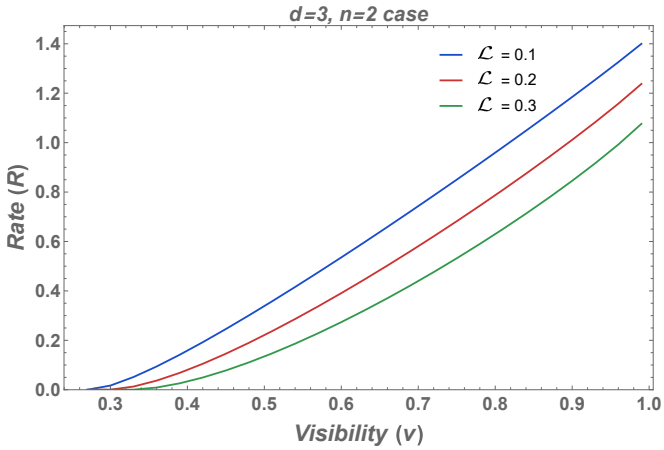

FIG. 4. Considering the uniform leakage model, we illustrate the upper bounds on the secure key rate as a function of the visibility v of the isotropic state ρ_v for the $d = 3, N = 2$ scenario, shown three different leakage values. Here, the secret key rate can exceed one bit, since a three-dimensional quantum system can, in principle, generate a three-level key symbol per round, allowing up to $\log_2 3$ bits of secret key.

parties want to establish a key among themselves using arbitrary-dimensional systems. Recall that we consider protocols where the parties announce their inputs. To this end, suppose that the source prepares a N-qudit isotropic state

$$\rho_v = v|\phi_{d,N}\rangle\langle\phi_{d,N}| + (1-v)\frac{\mathbb{1}}{d^N} \tag{6}$$

where $|\phi_{d,N}\rangle$ is the generalised GHZ state given by

$$|\phi_{d,N}\rangle = \frac{1}{\sqrt{d}}\sum_{i=0}^{d-1}|i\rangle^{\otimes N}. \tag{7}$$

It is well-known that the above state is fully separable for $v \leq 1/(1+d^{N-1})$ and entangled across some bipartition otherwise [25]. The correlations $\{p^v(\vec{a}|\vec{x})\}$ are computed as $p^v(\vec{a}|\vec{x}) = \mathrm{Tr}(\bigotimes_{i=1}^N M_{a_i|x_i}\rho_v)$.

Theorem 2. *Consider the QKD protocol described above with a leakage parameter $\mathcal{L}$, which is implemented using the isotropic state ρ_v (6). Then, for any $d-$outcome measurements with all parties, Eve can find a C.C. attack such that no secure key can be extracted for (i) $v \leq \frac{1}{1+d^{N-1}} + \frac{d^{N-1}\mathcal{L}}{(1+d^{N-1})(1-\mathcal{L})+\mathcal{L}}$ for uniform leakage, (ii) $v \leq \frac{1}{1+d^{N-1}} + \frac{d^{N-1}\mathcal{L}}{(1+d^{N-1})(\mathcal{L}+1+d^{N-1})}$ for leakage only from "junk".*

The proof of the above theorem is provided in Theorem 1 in the appendix. For the special cases $d = 3, N = 2$ and $d = 2, N = 3$, we compute the upper bound on the secure key rate achievable with standard QKD protocols for an isotropic state (see Fig. 3). The computation is based on finding the best CC attack by Eve, given arbitrary projective measurements performed by the parties [see Appendix B for details].

Discussions— Our findings highlight a fundamental limitation in the practical use of entanglement for QKD. While entanglement is widely regarded as the essential resource enabling quantum security, our results demonstrate that it is not, by itself, sufficient for secure key generation in standard entanglement-based practical QKD protocols. In particular, we have shown that when the input choices are publicly announced, as in the E91 and entanglement-based BB84 schemes, even an arbitrarily small amount of leakage of classical side information implies that there exist entangled states that fail to yield any secret key. Counter-intuitively, we find that this gap persists even if the leakage happens only from "junk" rounds. This means that even if leakage occurs only in rounds from which no secure key can be generated, it is still sufficient to reveal a gap between entangled states and key-generating states.

To do this, we identified a class of two-qubit isotropic states that are entangled yet useless for key distillation under most protocols, thereby underscoring the practical distinction between entanglement and key-generating capability. Extending this observation, we showed that a similar limitation arises in higher-dimensional and multipartite systems, where certain isotropic states are entangled but cannot be used to extract a secure key. These results suggest that the mere presence of entanglement does not guarantee practical advantage for cryptographic tasks. They further point towards the need to identify operational properties beyond entanglement that determine whether a state can support secure key generation in realistic settings. Finally, we demonstrated that even a small noise in the source drastically reduces the scalability of repeater-

based QKD architectures.

Several questions arise from our findings. A key direction is to develop a general criterion distinguishing entangled states that can yield a secret key from those that cannot under realistic conditions. Extending these ideas to other settings, such as measurement-device-independent or prepare-and-measure protocols, is important for understanding the fundamental resources enabling secure key generation. In particular, applying the C.C. attack in prepare-and-measure scenarios would be interesting, since the source is held by one of the parties and cannot be accessed or manipulated by the adversary, which changes the structure of possible attacks. In this work, we considered one of the simplest possible attacks; however, under more sophisticated attacks, an even larger set of entangled states could be shown to be useless for secure key generation.

Acknowledgements— This project was funded within the National Science Centre, Poland, grant Opus 25, UMO-2023/49/B/ST2/02468.

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in **Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing** (Bangalore, India, 1984) pp. 175–179.

[2] A. K. Ekert, Quantum cryptography based on bell's theorem, Physical Review Letters **67**, 661 (1991).

[3] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum cryptography without bell's theorem, Physical Review Letters **68**, 557 (1992).

[4] D. Bruß, Optimal eavesdropping in quantum cryptography with six states, Physical Review Letters **81**, 3018 (1998).

[5] C. H. Bennett, Quantum cryptography using any two nonorthogonal states, Physical Review Letters **68**, 3121 (1992).

[6] K. Tamaki, H.-K. Lo, and C.-H. F. Fung, Decoy-state quantum key distribution with a biased basis choice and its application to the b92 protocol, Physical Review A **77**, 032341 (2008).

[7] H.-K. Lo, M. Curty, and B. Qi, Measurement-device-independent quantum key distribution, Physical Review Letters **108**, 10.1103/physrevlett.108.130503 (2012).

[8] M. Curty, M. Lewenstein, and N. Lütkenhaus, Entanglement as a precondition for secure quantum key distribution, Phys. Rev. Lett. **92**, 217903 (2004).

[9] I. W. Primaatmaja, K. T. Goh, E. Y.-Z. Tan, J. T.-F. Khoo, S. Ghorai, and C. C.-W. Lim, Security of device-independent quantum key distribution protocols: a review, Quantum **7**, 932 (2023).

[10] V. Zapatero, T. van Leent, R. Arnon-Friedman, W.-Z. Liu, Q. Zhang, H. Weinfurter, and M. Curty, Advances in device-independent quantum key distribution, npj Quantum Information **9**, 10 (2023).

[11] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, Secure key from bound entanglement, Phys. Rev. Lett. **94**, 160502 (2005).

[12] U. Maurer and S. Wolf, The intrinsic conditional mutual information and perfect secrecy, in **Proceedings of IEEE International Symposium on Information Theory** (1997) pp. 88–.

[13] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2009).

[14] V. Makarov, A. Anisimov, and J. Skaar, Effects of detector efficiency mismatch on security of quantum cryptosystems, Physical Review A **74**, 022313 (2006).

[15] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nature Photonics **4**, 686 (2010).

[16] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, J. Skaar, and V. Makarov, Device calibration impacts security of quantum key distribution, Physical Review Letters **107**, 110501 (2011).

[17] Y. Zhao, C.-H. F. Fung, B. Qi, and H.-K. Lo, Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems, Physical Review A **78**, 042333 (2008).

[18] P. Kocher, J. Jaffe, and B. Jun, Differential power analysis, in **Proceedings of CRYPTO '99**, Lecture Notes in Computer Science, Vol. 1666 (Springer, 1999) pp. 388–397.

[19] K. Tamaki, M. Curty, and M. Lucamarini, Decoy-state quantum key distribution with a leaky source, New J. Phys. **18**, 065008 (2016).

[20] M. Pereira, M. Curty, and K. Tamaki, Quantum key distribution with flawed and leaky sources, NPJ Quantum Inf. **5**, https://doi.org/10.1038/s41534-019-0180-9 (2019).

[21] W. Wang, K. Tamaki, and M. Curty, Measurement-device-independent quantum key distribution with leaky sources, Sci. Rep. **11**, 1678 (2021).

[22] Á. Navarrete and M. Curty, Improved finite-key security analysis of quantum key distribution against trojan-horse attacks, Quantum Sci. Technol. **7**, 035021 (2022).

[23] K. Horodecki, M. Studziński, R. P. Kostecki, O. Sakarya, and D. Yang, Upper bounds on the leakage of private data and an operational approach to markovianity, Physical Review A **104**, 10.1103/physreva.104.052422 (2021).

[24] D. Gottesman and H. Lo, Proof of security of quantum key distribution with two-way classical communications, IEEE Transactions on Information Theory **49**, 457 (2003).

[25] W. Dür and J. I. Cirac, Classification of multiqubit mixed states: Separability and distillability properties, Physical Review A **61**, 042314 (2000).

[26] C. H. Bennett, G. Brassard, and N. D. Mermin, Quantum cryptography without bell's theorem, Physical Review Letters **68**, 557 (1992).

[27] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Tight finite-key analysis for quantum cryptography, Nature Communications **3**, 10.1038/ncomms1631 (2012).

[28] M. Masini and S. Sarkar, One-sided di-qkd secure against coherent attacks over long distances (2024), arXiv:2403.11850 [quant-ph].

[29] M. Tomamichel and A. Leverrier, A largely self-contained and complete security proof for quantum key distribution, Quantum **1**, 14 (2017).

[30] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, The security of practical quantum key distribution, Rev. Mod. Phys. **81**, 1301 (2009).

[31] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).

[32] A. Acín, N. Gisin, and L. Masanes, From bell's theorem to secure quantum key distribution, Phys. Rev. Lett. **97**, 120405 (2006).

[33] A. Acín, S. Massar, and S. Pironio, Efficient quantum key distribution secure against no-signalling eavesdroppers, New Journal of Physics **8**, 126–126 (2006).

[34] M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, and R. Renner, Unifying classical and quantum key distillation (2007), arXiv:quant-ph/0608199 [quant-ph].

[35] K. Horodecki, M. Winczewski, and S. Das, Fundamental limitations on the device-independent quantum conference key agreement, Phys. Rev. A **105**, 022604 (2022).

[36] R. F. Werner, Quantum states with einstein-podolsky-rosen correlations admitting a hidden-variable model, Journal of Mathematical Physics **28**, 1529 (1987).

[37] K. Azuma, S. E. Economou, D. Elkouss, P. Hilaire, L. Jiang, H.-K. Lo, and I. Tzitrin, Quantum repeaters: From quantum networks to the quantum internet, Rev. Mod. Phys. **95**, 045006 (2023).

[38] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Quantum repeaters: The role of imperfect local operations in quantum communication, Phys. Rev. Lett. **81**, 5932 (1998).

[39] L.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Long-distance quantum communication with atomic ensembles and linear optics, Nature **414**, 413 (2001).

[40] N. Sangouard, C. Simon, H. de Riedmatten, and N. Gisin, Quantum repeaters based on atomic ensembles and linear optics, Rev. Mod. Phys. **83**, 33 (2011).

[41] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, Ultrafast and fault-tolerant quantum communication across long distances, Phys. Rev. Lett. **112**, 250501 (2014).

[42] A. Sadhu, M. A. Somayajula, K. Horodecki, and S. Das, Practical limitations on robustness and scalability of quantum internet (2024), arXiv:2308.12739 [quant-ph].

[43] G. M. D'Ariano, P. L. Presti, and P. Perinotti, Classical randomness in quantum measurements, Journal of Physics A: Mathematical and General **38**, 5979–5991 (2005).

[44] S. Sarkar, J. J. Borkała, C. Jebarathinam, O. Makuta, D. Saha, and R. Augusiak, Self-testing of any pure entangled state with the minimal number of measurements and optimal randomness certification in a one-sided device-independent scenario, Physical Review Applied **19**, 10.1103/physrevapplied.19.034038 (2023).

Appendix A: Proof of the main theorem

Theorem 1. *Consider the QKD protocol described above with a leakage parameter $\mathcal{L}$, which is implemented using the isotropic state ρ_v (6). Then, for any $d-$outcome measurements with all parties, Eve can find a C.C. attack such that no secure key can be extracted for (i) $v \leq \frac{1}{1+d^{N-1}} + \frac{d^{N-1}\mathcal{L}}{(1+d^{N-1})(1-\mathcal{L})+\mathcal{L}}$ for uniform leakage, (ii) $v \leq \frac{1}{1+d^{N-1}} + \frac{d^{N-1}\mathcal{L}}{(1+d^{N-1})(\mathcal{L}+1+d^{N-1})}$ for leakage only from "junk".*

Proof. Let us construct the convex combination attack. For this purpose, the state generated by the source is mixed with a fully separable and entangled state as

$$\rho_v = \frac{q_v}{(1+d^{N-1})}\left(|\phi_{d,N}\rangle\langle\phi_{d,N}| + \frac{1}{d}\mathbb{1}\right) + (1-q_v)|\phi_{d,N}\rangle\langle\phi_{d,N}| \tag{8}$$

which implies that $q_v = \frac{(1+d^{N-1})(1-v)}{d^{N-1}}$. It is thus straightforward to observe that the statistics with all parties remain invariant under this mixing. The fully separable isotropic state can further be represented by a convex combination of product states as

$$\rho^{\text{sep}} = \frac{1}{(1+d^{N-1})}\left(|\phi_{d,N}\rangle\langle\phi_{d,N}| + \frac{1}{d}\mathbb{1}\right) = \sum_i p_i \bigotimes_{j=1}^{N} |\mu_i^{(j)}\rangle\langle\mu_i^{(j)}| \tag{9}$$

where $|\mu_i^{(j)}\rangle \in \mathbb{C}^d$. Consequently, Eve sends each product state with a flag $f = f_i$ and the entangled state with a flag $f =?$ thus the joint state is

$$\rho^v_{A_1\ldots A_N E} = q_v\left(\sum_i p_i \bigotimes_{j=1}^{N} |\mu_i^{(j)}\rangle\langle\mu_i^{(j)}| \otimes |f_i\rangle\langle f_i|_E\right) + (1-q_v)|\phi^+\rangle\langle\phi^+| \otimes |?\rangle\langle?|_E. \tag{10}$$

Now, in any practical scenario, there is always some leakage of side information to the adversary. Here, we suppose that for any party, the outcomes in the key generating rounds are leaked with a probability $\mathcal{L}$. Let us first consider the uniform leakage model, that is, leakage happens independently of the flag with the same probability $\mathcal{L}$. Equivalently, one can understand $\mathcal{L}$ as the fraction of the number of outcomes leaked out versus the total number of outcomes for each party in the key generation rounds. In the worst-case scenario, Eve learns the outcomes of all

parties in the same round, and thus, $\mathcal{L}$ fraction of the time, the outcomes of all parties are known to Eve when any state is sent. Consequently, the joint probability distribution of all parties along with Eve is given by

$$\begin{aligned} p^v(\vec{a},e|\vec{x}) &= q_v(1-\mathcal{L})\left(\sum_i p_i p^i(\vec{a}|\vec{x})\delta_{e,f_i}\right) + q_v\mathcal{L}p^{\text{sep}}(\vec{a}|\vec{x})\delta_{e,(\vec{a})} \\ &+ (1-q_v)(1-\mathcal{L})p^{\text{ent}}(\vec{a}|\vec{x})\delta_{e,?} + (1-q_v)\mathcal{L}p^{\text{ent}}(\vec{a}|\vec{x})\delta_{e,(\vec{a})}. \end{aligned} \tag{11}$$

Here $p^i(\vec{a}|\vec{x})$ are product distributions as they are generated using the states $\bigotimes_{j=1}^N |\mu_i^{(j)}\rangle\langle\mu_i^{(j)}|$ and $p^{\text{ent}}(\vec{a}|\vec{x}), p^{\text{sep}}(\vec{a}|\vec{x})$ is the probability distribution when the underlying state is maximally entangled and the separable isotropic state respectively.

Let us introduce a mixing parameter $\gamma_{\vec{a},\vec{x}}$, based on which the outcomes from the leaked part of $p^{\text{sep}}(\vec{a}|\vec{x})$ are mixed with ?. After mixing, the new probability distribution of all parties and Eve is given by

$$\begin{aligned} p(\vec{a},e|\vec{x}) = q_v(1-\mathcal{L})\left(\sum_i p_i p^i(\vec{a}|\vec{x})\delta_{e,f_i}\right) + q_v\mathcal{L}(1-\gamma_{\vec{a},\vec{x}})p^{\text{sep}}(\vec{a}|\vec{x})\delta_{e,\vec{a}} + (1-q_v)\mathcal{L}p^{\text{ent}}(\vec{a}|\vec{x})\delta_{e,\vec{a}} \\ +q_v\mathcal{L}\gamma_{\vec{a},\vec{x}}p^{\text{sep}}(\vec{a}|\vec{x})\delta_{e,?} + (1-q_v)(1-\mathcal{L})p^{\text{ent}}(\vec{a}|\vec{x})\delta_{e,?}. \end{aligned} \tag{12}$$

As described in the manuscript, the key rate is upper-bounded as

$$R \leq \frac{1}{N-1}\sum_e\sum_{\vec{x}} p_{\vec{x}}p(e|\vec{x})I_{\vec{x}}(A_1\dots A_N|e,\text{C.C.}) \tag{13}$$

Let us observe that $I_{\vec{x}}(A_1\dots A_N|e = f_i,\text{C.C.}) = 0$ for all i, as $p^i(\vec{a}|\vec{x})$ are product distributions along with $I_{\vec{x}}(A_1\dots A_N|e = \vec{a},\text{C.C.}) = 0$ as the outcomes are known to Eve. Consequently, we can immediately conclude that key rate is upper bounded as

$$R \leq \frac{1}{N-1}\sum_{\vec{x}} p_{\vec{x}}p(e =?|\vec{x})I_{\vec{x}}(A_1\dots A_N|e =?,\text{C.C.}). \tag{14}$$

We now find conditions when $I_{\vec{x}}(A_1\dots A_N|e =?,\text{C.C.}) = 0$, that is, we find q_v for which there is a well-defined mixing parameter $\gamma_{\vec{a},\vec{x}}$ such that $0 \leq \gamma_{\vec{a},\vec{x}} \leq 1$ for any $\vec{a},\vec{x}$. For this purpose, we first observe that for any $\vec{x}$ we can always find a set of outputs $\vec{a'}$ such that $p^{\text{ent}}(\vec{a'}|\vec{x}) = \max_{\vec{a}}\{p^{\text{ent}}(\vec{a}|\vec{x})\}$. Evaluating the conditional probability distribution, $p^v(\vec{a}|e =?,\vec{x})$ using the Bayes rule $p^v(\vec{a}|e =?,\vec{x}) = p(\vec{a},e =?|\vec{x})/p(e =?|\vec{x})$ to obtain that

$$p^v(\vec{a}|e =?,\vec{x}) = \frac{1}{p(e =?|\vec{x})}\left(q_v\mathcal{L}\gamma_{\vec{a},\vec{x}}p^{\text{sep}}(\vec{a}|\vec{x}) + (1-q_v)(1-\mathcal{L})p^{\text{ent}}(\vec{a}|\vec{x})\right). \tag{15}$$

The simplest criteria for $I_{\vec{x}}(A_1,\dots,A_N|e =?) = 0$ is that all the conditional probabilities $p^v(\vec{a}|e =?,\vec{x})$ are equal to each other, that is, the mixing parameters are adjusted such that all the conditional probabilities in Eq. (15) for each $\vec{a},\vec{x}$ are equal. Consequently, we get the condition for all $\vec{a},\vec{x}$

$$\begin{aligned} (1-q_v)(1-\mathcal{L})p^{\text{ent}}(\vec{a'}|\vec{x}) &= q_v\mathcal{L}\gamma_{\vec{a},\vec{x}}p^{\text{sep}}(\vec{a}|\vec{x}) + (1-q_v)(1-\mathcal{L})p^{\text{ent}}(\vec{a}|\vec{x}) \\ \implies \gamma_{\vec{a},\vec{x}} &= \frac{(1-\mathcal{L})(1-q_v)(p^{\text{ent}}(\vec{a'}|\vec{x}) - p^{\text{ent}}(\vec{a}|\vec{x}))}{q_v\mathcal{L}p^{\text{sep}}(\vec{a}|\vec{x})}. \end{aligned} \tag{16}$$

The problem now simplifies to finding a $\gamma_{\vec{a},\vec{x}} \in [0,1]$. If there exists such a $\gamma_{\vec{a},\vec{x}}$, then Eve can use the above described strategy to guess the key. Since it is clear from the above expression that $\gamma_{\vec{a},\vec{x}} \geq 0$, we need to only establish conditions under which $\gamma_{\vec{a},\vec{x}} \leq 1$.

Let us now recall that for $d-$outcome projective measurements, we have that $p^{\text{ent}}(\vec{a'}|\vec{x}) \leq 1/d$ and $p^{\text{sep}}(\vec{a'}|\vec{x}) = \frac{1}{1+d^{N-1}}(p^{\text{ent}}(\vec{a}|\vec{x}) + 1/d)$. Thus, $\gamma_{\vec{a},\vec{x}}$from (16) is upper-bounded as follows

$$\gamma_{\vec{a},\vec{x}} = \frac{(1+d^{N-1})(1-\mathcal{L})(1-q_v)(p^{\text{ent}}(\vec{a'}|\vec{x}) - p^{\text{ent}}(\vec{a}|\vec{x}))}{q_v\mathcal{L}(p^{\text{ent}}(\vec{a}|\vec{x}) + 1/d)} \leq \frac{(1+d^{N-1})(1-\mathcal{L})(1-q_v)(1/d)}{q_v\mathcal{L}/d}. \tag{17}$$

As the above quantity needs to be less than or equal to 1, we find that

$$q_v \geq \frac{(1+d^{N-1})(1-\mathcal{L})}{(1+d^{N-1})(1-\mathcal{L})+\mathcal{L}} \tag{18}$$

which on recalling that $q_v = \frac{(1+d^{N-1})(1-v)}{d^{N-1}}$ gives us

$$v \leq 1 - \frac{d^{N-1}(1-\mathcal{L})}{(1+d^{N-1})(1-\mathcal{L})+\mathcal{L}} = \frac{1}{1+d^{N-1}} + \frac{d^{N-1}\mathcal{L}}{(1+d^{N-1})(1-\mathcal{L})+\mathcal{L}}. \tag{19}$$

Consequently, for any $\mathcal{L} \geq 0$, Eve can obtain a mixing parameter $\gamma_{\vec{a},\vec{x}}$ such that the intrinsic information is 0 even from an entangled state and thus no secure key can be extracted.

Let us consider now that the leakage only happens from "junk" rounds, that is, from rounds when separable state is sent by Eve. Thus, the joint probability distribution of all parties and Eve after the leakage is almost the same as (11), but since there is no leakage when the flag is ?, we get

$$p^v(\vec{a},e|\vec{x}) \;=\; q_v(1-\mathcal{L})\left(\sum_i p_i p^i(\vec{a}|\vec{x})\delta_{e,f_i}\right) + q_v\mathcal{L}p^{\text{sep}}(\vec{a}|\vec{x})\delta_{e,(\vec{a})} + (1-q_v)p^{\text{ent}}(\vec{a}|\vec{x})\delta_{e,?}. \tag{20}$$

Consequently, the fraction of outcomes leaked is $\mathcal{L}q_v$, which is lower than the former case. Following the same steps as above from Eq. (12) to (18), we obtain

$$q_v \geq \frac{1+d^{N-1}}{1+d^{N-1}+\mathcal{L}} \tag{21}$$

which on recalling that $q_v = \frac{(1+d^{N-1})(1-v)}{d^{N-1}}$ gives us

$$v \leq \frac{1}{1+d^{N-1}} + \frac{d^{N-1}\mathcal{L}}{(1+d^{N-1})(\mathcal{L}+1+d^{N-1})}. \tag{22}$$

Consider now general $d-$outcome measurements acting on $d-$dimensional Hilbert space. As shown in [43], any POVM can be written as a convex combination of extremal POVM's. Some examples of such extremal POVMs in arbitrary dimensions and number of outcomes can be found in [44]. For $d-$outcome measurements, the extremal POVMs are projective measurements. Thus, any $d-$outcome POVM $\{N_a\}$ can be expressed as $\sum_i p_i\{M_a^i\}$ where M_a^i are projectors. As intrinsic information (2) with general measurements can be expressed as a convex combination of intrinsic information via projective measurements if Eve knows the mixing labels i, that is,

$$I_{\vec{x}}(A_1\ldots A_N\downarrow e)_{\{N_a\}} \leq \sum_i p_i I_{\vec{x}}(A_1\ldots A_N\downarrow e)_{\{M_a^i\}}. \tag{23}$$

Now, Eve can straightaway know the labels i as she can attach a flag on the states which activate particular label at the parties. Consequently, we can straightaway conclude that if the secure key obtainable using $d-$outcome projective measurements is 0, then $d-$outcome general measurements do not help. Moreover, one can also understand this by noting that, with POVMs, the correlations between Alice and Bob decrease, and thus the optimal strategy for finding the key is via projective measurements. This completes the proof.

Appendix B: Maximum obtainable rate for any isotropic state using projective measurements

Let us recall from Eq. (3) of the manuscript that the maximal achievable rate when Eve performs a C.C. attack is given by,

$$R \leq \frac{1}{N-1}\sum_e\sum_{\vec{x}} p_{\vec{x}}p(e|\vec{x})I_{\vec{x}}(A_1\ldots A_N|e,\text{C.C.}) \tag{24}$$

where $I_{\vec{x}}(A_1\ldots A_N|e,\text{C.C.})$ is the conditional mutual information of all parties given inputs $\vec{x}$.

Eve's strategy to execute the C.C. attack is explicitly given in the proof of theorem 1. Using this as stated above in Eq. (24), the upper bound to the key rate is given by

$$R \leq \frac{1}{N-1} \sum_{\vec{x}} p_{\vec{x}} p(e=?|\vec{x}) I_{\vec{x}}(A_1, A_2, \ldots, A_N|e=?) \leq \frac{1}{N-1} \max_{\vec{x}} I_{\vec{x}}(A_1, A_2, \ldots, A_N|e=?). \tag{25}$$

In Fig. 1 of the manuscript, we find the maximal rate for the case when $d = 2, N = 2$. To do this, we first express the conditional mutual information $I_{\vec{x}}(A_1, A_2|e=?)$ as

$$I_{\vec{x}}(A_1, A_2|e=?) = H(A_1|e=?) + H(A_2|e=?) - H(A_1, A_2|e=?) \tag{26}$$

where $H(.)$ is the Shannon entropy. The Shannon entropy can be expressed in terms of the conditional joint probability distribution $p^v(\vec{a}|e=?, \vec{x})$ as

$$I^v_{x_1,x_2}(A_1, A_2|e=?) = \sum_{a_1,a_2=0,1} p^v(e=?) p^v(a_1, a_2|e=?, x_1, x_2) \log \frac{p^v(a_1, a_2|e=?, x_1, x_2)}{p^v(a_1|e=?, x_1) p^v(a_2|e=?, x_2)} \tag{27}$$

where the superscript v signifies that the quantities are computed for isotropic state (6) for $d = 2, N = 2$ with a visibility v. Referring back to the proof of theorem 1, we observe that Eve's best strategy relies on finding the mixing parameters $\gamma_{\vec{a},\vec{x}}$ such that the conditional mutual information is minimised. Consequently, expressing the conditional probability distribution $p^v(a_1, a_2|e=?, x_1, x_2)$ as done in Eq. (15) and then using the fact that A_1, A_2 correlations are no-signalling, we obtain from (27) that $I^v_{x_1,x_2}(A_1, A_2|e=?)$ is a function of the mixing parameters $\gamma_{\vec{a},\vec{x}}$ such that $0 \leq \gamma_{\vec{a},\vec{x}} \leq 1$. Thus, the maximal rate for any visibility v is given by

$$R \leq \max_{\vec{x}} \min_{\gamma_{\vec{a},\vec{x}}} I^v_{\vec{x}}(A_1, A_2|e=?)(\gamma_{\vec{a},\vec{x}}). \tag{28}$$

One can straightaway generalise the above statement for any d, N for any isotropic state of visibility v to obtain

$$R \leq \frac{1}{N-1} \max_{\vec{x}} \min_{\gamma_{\vec{a},\vec{x}}} I^v_{\vec{x}}(A_1, \ldots, A_N|e=?)(\gamma_{\vec{a},\vec{x}}). \tag{29}$$

Notice that for higher N one has to use the chain rule to obtain $I^v_{\vec{x}}(A_1, \ldots, A_N|e=?)$ from (27) which is technically involving.

Below, we describe the numerical procedure used to obtain the key-rate plots shown in Figs. 1, 3, and 4. All figures are computed under the uniform leakage model. Each figure contains three curves, corresponding to different leakage values, with each curve obtained using the same numerical optimization procedure described below. We consider three scenarios, namely (i) $d = 2, N = 2$, (ii) $d = 2, N = 3$, and (iii) $d = 3, N = 2$. In all cases, the secret key rate is evaluated as a function of the visibility using the same two-step max–min optimization strategy: we first minimize over Eve's parameters $\gamma_{\vec{a},\vec{x}}$ and then maximize over the honest parties' measurement settings. The resulting curves therefore capture both the optimal honest-party strategy and the worst-case eavesdropping attack. For the case $d = 2, N = 2$, shown in Fig. 1, we consider the bipartite qubit scenario. The horizontal axis represents the visibility, while the vertical axis shows the optimized key rate obtained through the above optimization procedure. For $d = 2, N = 3$, shown in Fig. 3, we consider the tripartite qubit scenario. Alice performs measurements in the Z basis, while Bob and Charlie use projective measurements in the X–Z plane parametrized by angles θ_1 and θ_2. In the numerical optimization, without loss of generality, Alice's and Bob's measurements are fixed to the Z basis, and the maximization is performed only over θ_2. The optimized key rate is then plotted as a function of the visibility.

Finally, for the bipartite qutrit case ($d = 3, N = 2$), shown in Fig. 4, both Alice and Bob perform projective measurements in the qutrit Z basis. Applying the same max–min optimization procedure described above, we compute the key rate as a function of the visibility.

□