Device independent security of quantum key distribution from monogamy-of-entanglement games

Enrique Cervero-Martín[1] and Marco Tomamichel[2]

[1]Centre for Quantum Technologies, National University of Singapore
[2]Centre for Quantum Technologies, National University of Singapore and
Department of Electrical and Computer Engineering, National University of Singapore

We analyse two party non-local games whose predicate requires Alice and Bob to generate matching bits, and their three party extensions where a third player receives all inputs and is required to output a bit that matches that of the original players. We propose a general device-independent quantum key distribution protocol for the subset of such non-local games that satisfy a monogamy-of-entanglement property characterised by a gap in the maximum winning probability between the bipartite and tripartite versions of the game. This gap is due to the optimal strategy for two players requiring entanglement, which due to its monogamy property cannot be shared with any additional players. Based solely on the monogamy-of-entanglement property, we provide a simple proof of information theoretic security of our protocol. Lastly, we numerically optimize the finite and asymptotic secret key rates of our protocol using the magic square game as an example, for which we provide a numerical bound on the maximal tripartite quantum winning probability which closely matches the bipartite classical winning probability. Further, we show that our protocol is robust for depolarizing noise up to about 2.88%, providing the first such bound for general attacks for magic square based quantum key distribution.

Contents

Enrique Cervero-Martín: enrique.cervero@u.nus.edu
Marco Tomamichel: marco.tomamichel@nus.edu

1 Introduction

Device independent quantum key distribution (DIQKD) allows two honest parties (commonly called Alice and Bob) to establish an information theoretic secure key with minimal assumptions on the inner workings of their lab equipment, and in the presence of an eavesdropper (aptly named Eve) who in particular might have distributed, or is otherwise in control of the devices of the honest parties. Even when using such uncharacterised devices, the security of DIQKD can be guaranteed through a large enough violation of a *Bell inequality* [1, 2], as this ensures that the correlations shared amongst the honest parties arise from a quantum behaviour. Such violations are used in DIQKD to certify that the honest parties share an entangled state, which may not be further entangled to an eavesdropper due to the *monogamy of entanglement*, a property of multi-partite quantum systems which asserts that strongly correlated two party states may only be weakly correlated to a third party [3, 4]. Crucially, the monogamy-of-entanglement property asserts that meddling eavesdroppers may not be strongly correlated to the honest parties measurement results if the latter violate a Bell inequality, which implies that the eavesdropper's available information about the honest users' exchanged keys in a DIQKD protocol may be bounded.

To make the latter statement more precise, secrecy of a QKD protocol in the finite round regime requires a lower bound on the smooth min-entropy of an honest party's raw key conditioned on the eavesdropper's side information [5, 6]. Roughly speaking, the smooth min-entropy measures the worst-case uncertainty of Alice's raw key from the perspective of Eve. Lower bounding this quantity is difficult in practice, but dependant on the assumptions of the operations across the rounds of a QKD protocol that produce the raw key, some simplifications are possible. For example, using the *Asymptotic Equipartition Property* [7] if the channels are identical and memoryless, the *Entropy Accumulation Theorem* (EAT) [8, 9] if the channels satisfy a Markov chain condition, or the more recent *Generalised Entropy Accumulation Theorem* (GEAT) [10] if the channels satisfy a no-signalling condition. The EAT and GEAT provide the highest security guarantee as they allow the eavesdropper to hold a transcript of any public discussion and a quantum memory when performing their attack. This is known as a *coherent* or *general* attack. In contrast, *memoryless* (also known as *collective*) attacks force the eavesdropper to apply her attack after each round of measurements by Alice and Bob without any additional classical or quantum side information. Security of DIQKD protocols for general attacks in the finite round regime has been analysed extensively. See for example the framework in [5, 6, 11], the first security proofs in the finite regime [12, 13, 14, 15, 16], security proofs via EAT [17, 18, 11, 19, 20, 21, 22], and via the more recent GEAT in [23]. See also [24, 25, 26] for recent reviews on other tools and techniques, and [22, 27] for experimental realizations of DIQKD.

We remark that monogamy of entanglement can be used directly to prove the secrecy of QKD protocols by bounding the information available to the eavesdropper. To do this, monogamy-of-entanglement games were introduced in [15] to bound the probability with which an eavesdropper is able to make a successful guess of the key sifted by the honest parties in a semi-DIQKD protocol. Informally, monogamy-of-entanglement games are protocols which require the participating parties to produce the same output, but whose success probability decreases as more parties are added. This gap in winning probabilities is due to the optimal strategy for two parties requiring entanglement, which due to monogamy-of-entanglement property cannot be shared with additional parties. In fact, the use of monogamy of-entanglement in security proofs has recently received attention for QKD and various

cryptographic primitives. For example, in [28, 29, 30] the authors use the magic square game, whose bipartite optimal strategy self-tests maximal entanglement [31], to establish secure cryptographic keys. Likewise, the authors in [32, 33] introduce a monogamy-of-entanglement game based on coset states and use it as primitive in a continuous variable QKD protocol. Furthermore, monogamy-of-entanglement games are used in [34] for oblivious transfer, and in [35, 36] for uncloneable encryption.

This begs the question: is it possible to explicitly prove secrecy *of all* DIQKD protocols using arbitrary games which exhibit monogamy of entanglement? Typically, the Clauser-Horne-Shimony-Holt (CHSH) game is chosen due to its simplicity and relative ease of implementation [2, 37, 16, 19, 21], although more general CHSH games [38] and even other games like the magic square game [39, 29, 28, 30] have been considered. In this work, we use GEAT to show it is indeed possible to construct device independent quantum key distributions protocols from any two player non-local game which exhibits the monogamy-of-entanglement property characterised by a sufficiently large gap in the winning probability between two party and three party instances of the game. For this class of games, we show in Theorem 3 that the entropy of Alice's key bit conditioned on Eve's side information in one instance of the non-local game is bounded below by a family of simple affine functions $g : [0, 1] \to \mathbb{R}$. One such example is given by

$$g(p) := \frac{p - \omega_2}{\ln 2 \cdot (1 - \omega_2 + \omega_3)} - \log\big(1 - \omega_2 + \omega_3\big), \tag{1}$$

where ω_2, ω_3 are the optimal quantum winning probabilities of the bipartite and tripartite instances of the non-local game. Further, we highlight that in some monogamy-of-entanglement games, the tripartite quantum strategy does not outperform the classical strategy. For example, this is the case for the monogamy-of-entanglement game in [15], for the CHSH game, and as we show in this work, for the magic square game as well. This is because the optimal bipartite strategies require sharing maximally entangled states which due to the monogamy of entanglement, may not be additionally shared by a third party. The collapse of the tripartite quantum value onto the classical value is of independent theoretical interest but is in fact not a requirement for our security proof, which requires only a gap between the tripartite and bipartite quantum values of the underlying game. There might exist monogamy-of-entanglement games in which the tripartite quantum value exceeds the classical value, for example if the optimal strategy requires a (non-maximally entangled) state which remains entangled after tracing out one of the three parties. We leave the existence of these monogamy-of-entanglement games for future work.

As a result, our framework provides an alternative viewpoint for the security of QKD protocols which relies directly on monogamy of entanglement via a gap between the bipartite-tripartite gap in winning probability. In contrast, the security of QKD protocols often seen in the recent literature [18, 19, 21] relies on the robustness of the shared correlations, which is more indirectly dependent on the monogamy of entanglement. In contrast to these works, we focus mainly on spot-checking QKD protocols with identical testing and generation rounds. An advantage of this approach is that it is simpler to obtain entropy lower bounds for the achievable key rates. Unfortunately, this comes at the cost of a larger error correction cost which in some cases (see Figure 2) irrevocably yields a trivial key rate. To rectify this, it is possible to follow the framework in [2, 37, 18, 21] and add additional measurement settings which differentiate testing rounds from key generation rounds in the QKD protocol. Even though we do not explore additional measurement settings in this work, we remark that our analysis and security proofs largely extends to that framework, and that it suffices to use the entropy lower bounds (specifically *min-tradeoff functions*) found in [2, 37, 18, 21] in place of the ones derived in this work to prove the security of the QKD protocol with additional measurement settings.

We showcase our results with the *magic square game* (also known as the *Mermin-Peres game*) of [40, 41]. For this game, we compute an analytical upper bound on the optimum tripartite winning probability which is arbitrarily close to the maximum bipartite classical winning probability. Further, we use the NPA hierarchy of [42, 43, 44] and the tools from [45] to compute tighter bounds on the min-entropy and von Neumann entropy, respectively, of Alice's key bit conditioned on the eavesdroppers information in one instance of the magic square game. We use these improved bounds to numerically optimize the finite and asymptotic key rates of magic square game based DIQKD, in particular showing robustness for depolarizing noise of up to 2.88%.

We remark that previous works [29, 28, 30] also explore the security of MSG based DIQKD from the viewpoint of parallel repetition of monogamy-of-entanglement games. This article differs from these previous works by extending the analysis to arbitrary monogamy-of-entanglement games and including more detailed analysis of security in the finite regime of sequential MSG based DIQKD, including on

error correction, completeness and numerically optimized key rates. Moreover, the recent work [46] which we only became aware of while concluding our study also explores security of MSG based DIQKD using the numerical tools from [45] and under the memoryless attack assumption. We use the same numerical tools for the computation of the von Neumann entropies, but we generalise on their work by not limiting to security against memoryless eavesdroppers in the asymptotic regime, instead considering security in the finite round regime under general attacks. Further, we also improve over the asymptotic key rates and robustness against depolarizing noise reported in [46].

The remainder of the paper is structured as follows. We start Section 2 by introducing some basic definitions on quantum information, non-local games and quantum key distribution that will be used in the text. In this section we also present and discuss our DIQKD protocol, protocol $\mathcal{P}$ in algorithm 1. In Section 3 we present our main theorems, Theorem 1, Theorem 2 and Theorem 3 for the completeness, correctness and secrecy of $\mathcal{P}$. The proof of these theorems is deferred to Section 4, where we also include a second preliminaries section with more involved definitions and results that are needed in the proofs. Of particular interest is Lemma 3 in Section 4.4, a new result which provides an efficient bound to the smooth max-entropy terms appearing in EAT-based secrecy proofs. Lastly, in Section 3.2 we present the numerically optimized finite and asymptotic key rates for the magic square game based DIQKD protocol using the tailored entropy bounds constructed in Section 5.

2 Quantum key distribution from non-local games

2.1 Preliminaries

In this section we introduce the basic concepts necessary for understanding our main results and refer to Section 4.1 for the definitions required in the proofs. Table 1 contains some notation that will be used through this text and Table 2 specifies the greek letters used to denote the quantum states at different stages of a QKD protocol.

Table 1: Notation

Symbol	*Definition*
A_i^j	collection of registers $A_i, ..., A_j$
$S(A)$ (resp. $S_{\leq}(A)$)	Set of normalized (resp. subnormalised) states on register A
τ_A	Maximally mixed state on register A
$\mathbb{I}_A$	Identity operator on register A
$L^\dagger$	Adjoint of map L
Ω^c	Complement of event Ω
$\neg 0$	Values other than 0
log (resp. ln)	Base-2 (resp. base-e) logarithm
$\mathcal{P}(\mathcal{C})$	Set of probability distributions on alphabet $\mathcal{C}$
$\|\cdot\|_p$	Schatten p-norm

A *quantum state* ρ is a unit trace, positive-definite operator acting on a Hilbert space. The collection of quantum states on Hilbert space A is denoted $S(A)$. We say $\rho \in S(A)$ is pure if it has unit rank, and mixed otherwise. On the other hand, a subnormalised state is a positive-definite operator on Hilbert space A with trace smaller than 1. The set of subnormalised states on A is denoted $S_{\leq}(A)$. In this text we will only consider finite dimensional Hilbert spaces and quantum systems.

To quantify the distance between any two quantum states $\rho, \sigma \in S(A)$ we use the *trace distance*

$$\|\rho - \sigma\|_{\mathrm{Tr}} := \frac{1}{2}\|\rho - \sigma\|_1, \tag{2}$$

Table 2: Quantum states in QKD protocols

State	*Usage*
$\rho_{K_A E}$	State at the end of QKD protocols, contains final key
$\sigma_{S_A E}$	State prior to privacy amplification, contains raw key
$\nu_{Q_A Q_B}$	State in the quantum strategy of bipartite non-local games
$\tilde{\nu}_{Q_A Q_B}$	Noisy state in the quantum strategy of bipartite non-local games
ω_R^i	State in the honest parties' devices during i-th measurement round

where $\|\cdot\|_1$ is the Schatten 1-norm which equals the sum of the singular values of its argument.

A *register* is a quantum system with a fixed orthonormal basis which describes a discrete random variable. For example, if random variable X takes values over alphabet $\mathcal{X}$ with probabilities $x \mapsto p_x$ then a joint *classical-quantum* state $\rho_{XA} \in S(XA)$ is of the form

$$\rho_{XA} = \sum_{x\in\mathcal{X}} |x\rangle\langle x| \otimes \rho_A^x, \tag{3}$$

where $\rho_A^x \in S_{\leq}(E)$ is a subnormalised state with $\mathrm{Tr}[\rho_A^x] = p_x$. Further, if $\Omega \subset \mathcal{X}$ is some event, we define the following conditioned states

$$\rho_{AX\wedge\Omega} := \sum_{x\in\Omega} |x\rangle\langle x| \otimes \rho_A^x, \tag{4}$$

$$\rho_{AX|\Omega} := \frac{\mathrm{Tr}[\rho_{AX}]}{\mathrm{Tr}[\rho_{AX\wedge\Omega}]}\rho_{AX\wedge\Omega}, \tag{5}$$

where of course $\Pr[\Omega]_\rho = \mathrm{Tr}\left[\sum_{x\in\Omega}\rho_A^x\right] = \sum_{x\in\Omega} p_x$. Lastly, we use X_1^n to denote a collection of classical registers $X_1, ..., X_n$ over the same alphabet $\mathcal{X}$.

Maps from states in $S(A)$ to states in $S(B)$ are described by *quantum channels*, which are completely positive and trace preserving mappings (CPTP). We use $\mathrm{CPTP}(A, B)$ to denote the set of quantum channels from A to B. Quantum channels that are of particular interest are *measurements* and *instruments*. Given a positive operator valued measure (POVM) $\{P_x\}_{x\in\mathcal{X}}$ on system A, that is, a set of positive semi-definite operators on A satisfying $\sum_x P_x = \mathbb{I}_A$, then a measurement $\mathcal{M} \in \mathrm{CPTP}(A, X)$ applied to state $\rho_A \in S(A)$ is of the form

$$\mathcal{M} : \rho_A \mapsto \sum_{x\in\mathcal{X}} |x\rangle\langle x|_X \,\mathrm{Tr}[\rho_A P_x]. \tag{6}$$

If the operators $\{P_x\}_x$ additionally satisfy $P_x^2 = P_x$ for all $x \in \mathcal{X}$ then the corresponding set $\{P_x\}_x$ is called a projection valued measure (PVM). On the other hand, if $\mathcal{M}_x \in \mathrm{CP}(A, B)$ are trace non-increasing maps that satisfy $\sum_{x\in\mathcal{X}} \mathrm{Tr}[\mathcal{M}_x(\rho_A)] = \mathrm{Tr}[\rho_A]$ then a quantum instrument is the map $\mathcal{M} \in \mathrm{CPTP}(A, XB)$ given by

$$\mathcal{M} : \rho_A \mapsto \sum_{x\in\mathcal{X}} |x\rangle\langle x|_X \otimes \mathcal{M}_x(\rho_A). \tag{7}$$

If the register X is subsequently measured and outcome $x \in \mathcal{X}$ is observed, we call $\frac{\mathcal{M}_x(\rho_A)}{\mathrm{Tr}[\mathcal{M}_x(\rho_A)]}$ the *post-measurement* state.

2.2 Non-local games

We introduce some basic definitions of *non-local games* and refer to [47] for a review.

Definition 1 (Non-local game)**.** *A two player non-local game is a tuple* $\mathcal{G} = (\pi, \mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, V)$ *of*

- *Finite sets of questions* $\mathcal{X}, \mathcal{Y}$ *and answers* $\mathcal{A}, \mathcal{B}$*,*
- *Probability distribution* $\pi : \mathcal{X} \times \mathcal{Y} \to [0, 1]$*,*
- *Predicate* $V : \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \times \mathcal{B} \to \{0, 1\}$*.*

If π *is uniform,* $\mathcal{G}$ *is known as a free game.*

The definitions of two player non-local games can be generalised to multi-player non-local games in the obvious way.

In an instance of $\mathcal{G}$, the players respectively receive questions $x \in \mathcal{X}, y \in \mathcal{Y}$ with probability $\pi(x, y)$ and output answers $a \in \mathcal{A}, b \in \mathcal{B}$. The players win if $V(x, y, a, b) = 1$ and lose otherwise.

Prior to the start of the game, the players are allowed to prepare a strategy that dictates their behaviour through the game. Once the game begins, they are no longer allowed to communicate.

Definition 2 (Strategy)**.** *A strategy between two honest players is a conditional distribution* $\Pr[a, b|x, y]$*. This strategy may be:*

- *Classical: in which there exists a hidden variable* λ *such that*

$$\Pr[a, b|x, y] = \sum_{\lambda} \Pr[\lambda] \Pr[a|x, \lambda] \Pr[b|y, \lambda]. \tag{8}$$

- *Quantum: in which the conditional distribution is*

$$\Pr[a, b|x, y] = \mathrm{Tr}[\nu_{AB}(P_a^x \otimes Q_b^y)], \tag{9}$$

  for a pre-agreed quantum state $\nu_{AB} \in S(AB)$ *and choice of POVMs* $\left\{\{P_a^x\}_a\right\}_x$ *in Alice's lab and* $\left\{\{Q_b^y\}_b\right\}_y$ *in Bob's lab.*

- *No-signalling: in which the distribution* $\Pr[a, b|x, y]$ *satisfies the constraints*

$$\sum_{a \in \mathcal{A}} \Pr[a, b|x, y] = \sum_{a \in \mathcal{A}} \Pr[a, b|x', y] \qquad \text{for all } a, b, y, \tag{10}$$

$$\sum_{b \in \mathcal{B}} \Pr[a, b|x, y] = \sum_{b \in \mathcal{B}} \Pr[a, b|x, y'] \qquad \text{for all } a, b, x. \tag{11}$$

Definition 3 (Value of the game)**.** *The value of a two player non-local game* $\mathcal{G}$ *is*

$$\omega(\mathcal{G}) = \sup_{\Pr} \sum_{x,y;a,b} \pi(x, y) \Pr[a, b|x, y] V(x, y; a, b), \tag{12}$$

where the supremum is over permissible strategies (classical, quantum or no-signalling).

For classical strategies, we use ω_{C} to denote the *classical value* of $\mathcal{G}$ when $\mathcal{G}$ is inferred from context. Likewise, we use ω_{Q} and ω_{NS} to denote the *quantum* and *no-signalling* values, respectively. For any non-local game, it is clear that $\omega_{\mathrm{C}} \leq \omega_{\mathrm{Q}} \leq \omega_{\mathrm{NS}}$.

For the task of QKD, we focus on two player non-local games $\mathcal{G}_2 = (\pi, \mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, V)$ where X and Y are independent such that $\pi(x, y)$ is a product and the predicate is of the form

$$V(x, y, a, b) = [SK_A(a, x, y) = SK_B(b, x, y)]. \tag{13}$$

Here the square brackets evaluate to 1 if its argument is true, and to 0 otherwise. The function $SK_A : \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \to \{0, 1\}$ (respectively $SK_B : \mathcal{X} \times \mathcal{Y} \times \mathcal{B} \to \{0, 1\}$) is a deterministic function that outputs a single bit on input of x, y and a (respectively, x, y and b). For example, in the well known CHSH game Alice and Bob receive respective binary bits x, y, output respective bits a, b, and win if $x \cdot y = a \oplus b$. With our notation, this is equivalent to setting $SK_A(a, x, y) = a$ and $SK_B(b, x, y) = b \oplus (x \cdot y)$ (see Figure 2 for additional context). On the other hand, for the magic square game introduced in Section 3.2, Alice and Bob receive respective inputs $x, y \in \{0, 1, 2\}$, produce respective bit triples $a, b \in \{0, 1\}^3$

satisfying some parity conditions, and win if Alice's y-th bit equals Bob's x-th bit. In our framework, this is captured by functions $SK_A(a,x,y) = a[y]$ and $SK_B(a,x,y) = b[x]$.

We consider the three player extension $\mathcal{G}_3 = (\pi, \mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, \{0,1\}, \widetilde{V})$ in which the third player receives both the inputs of the original players (x,y) and outputs a single bit $c \in \{0,1\}$. The new predicate in $\mathcal{G}_3$ is of the form

$$\widetilde{V}(x,y,a,b,c) = [SK_A(a,x,y) = SK_B(b,x,y)] \cdot [SK_A(a,x,y) = c]. \tag{14}$$

In the context of QKD, the game $\mathcal{G}_2$ corresponds to the protocol 'played' by the *honest* parties and the functions SK_A, SK_B correspond to the functions used by Alice and Bob to obtain their respective raw keys and the parameter estimation registers. Here, *honest* refers to the behaviour of the players and in particular means that they are playing the game as per the instructions without trying to cheat, disrupt or break the protocol in any malicious way. Consequently, the third player in the game $\mathcal{G}_3$ corresponds to the eavesdropper in a QKD protocol who is attempting to guess Alice's sifted key bits $SK_A(a,x,y)$ during every round after all the inputs have been announced by the honest players.

For the rest of the article, we let $\omega_2 = \omega_{\mathrm{Q}}(\mathcal{G}_2)$, $\omega_3 = \omega_{\mathrm{Q}}(\mathcal{G}_3)$. Lastly, we introduce $\omega_{\mathrm{exp}} \in [\omega_3, \omega_2]$, the expected winning probability of the two honest parties in an instance of $\mathcal{G}_2$. For example, the discrepancy between ω_2 and ω_{exp} may be due to the noise present in the physical quantum devices which Alice and Bob use to distribute or measure their shared quantum states.

2.3 Security definitions of QKD

In this text we focus on entanglement based device independent QKD protocols between two honest parties, Alice and Bob, and a potential eavesdropper, Eve.

A QKD protocol is an interactive multi-round protocol between Alice and Bob, characterised by a sequence of local (classical or quantum) operations and classical communication (LOCC). In *entanglement based* protocols, a source produces a joint quantum system and distributes it amongst the honest parties Alice and Bob, who subsequently perform measurements on it with randomly and independently chosen measurement settings.

Before discussing the meaning of *device independent* protocols, we state some necessary assumptions of QKD protocols without which security guarantees are not applicable.

- All parties are bound by quantum mechanics[1];
- The devices of Alice and Bob are spatially separated. In particular, this allows us to describe operations in Alice's, Bob's or Eve's labs as a tensor product of local operations in the respective Hilbert spaces;
- The devices used by the honest parties do not communicate or leak information to any eavesdropper or to each other. Further, the honest parties have control over what their respective devices receive as inputs. In practice, these assumption can be enforced by shielding the devices and/or by ensuring space-like separation between the honest parties;
- The honest parties have access to trusted sources of randomness;
- The honest parties have access to an authenticated classical channel. In practice this is not a problem if the honest parties share a small amount of secret information [49, 50]. We remark that the communication passing through this channel is public and as such must be included in the eavesdropper's side information.

In addition to the above and for the sake of technical convenience, we will also assume all Hilbert spaces are finite dimensional.

In *device independent* quantum key distribution (DIKD) protocols, we further assume that the devices used by Alice and Bob are uncharacterized. Formally, a device $\mathcal{D}$ is an object capable of holding a quantum state and performing quantum instruments dependent on a classical input, producing a classical output and updating this state.

[1] We remark that existing results suggest security of device independent QKD is possible if quantum theory is replaced by a more general no-signalling theory [48]

Definition 4 (Quantum Device). *An $(\mathcal{X}, \mathcal{A}, R)$-device is characterised by a set $\mathcal{X}$ (the inputs), a set $\mathcal{A}$ (the outputs), a finite-dimensional quantum system R (the memory), as well as a collection of quantum instruments $\{\mathcal{M}^{a|x} : a \in \mathcal{A},\ x \in \mathcal{X}\}$ where $\mathcal{M}^{a|x}$ are completely positive maps such that $\sum_{a\in\mathcal{A}} \mathcal{M}^{a|x} \in \mathrm{CPTP}(R, R)$ for every $x \in \mathcal{X}$. The device takes as input a state ω_R^0 and then behaves in the following way when interacted with for the i-th time:*

- *Upon receiving an input $x_i \in \mathcal{X}$ it outputs $a_i \in \mathcal{A}$ with probability $\mathrm{Tr}\big[\mathcal{M}^{a_i|x_i}(\omega_R^{i-1})\big]$.*
- *The internal memory is updated to $\omega_R^i = \frac{\mathcal{M}^{a_i|x_i}(\omega_R^{i-1})}{\mathrm{Tr}\big[\mathcal{M}^{a_i|x_i}(\omega_R^{i-1})\big]}$.*

Note that this device model is very general. For honest implementations the quantum system R may contain an index register that is updated every time the device is used so that fresh entangled states can be used each time the game is played. Moreover, via this index register and memory registers, the instrument can be made dependent on all the inputs and outputs of previous rounds. In particular, this notation removes the need of an additional label i on the register R or the quantum instruments $\mathcal{M}^{a|x}$. While the internal state and the quantum instruments are usually specified for honest implementations our security guarantees are meant to be device-independent, that is, they do not depend on the state ω_R (and its potential extensions) or on the quantum instrument used to update this state and produce the classical outputs.[2]

A (device independent) QKD protocol takes as input the pair of devices $\mathcal{D}_A$ for Alice and $\mathcal{D}_B$ for Bob, which hold respective (and possibly entangled) quantum registers R_A and R_B.

Definition 5 (QKD Protocol). *A (n, ℓ)-QKD protocol $\mathcal{P}_{\mathcal{D}_A,\mathcal{D}_B}$ for a game $\mathcal{G} = (\mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, V)$ for two parties (Alice and Bob) takes as argument a $(\mathcal{X}, \mathcal{A}, R_A)$-device $\mathcal{D}_A$ for Alice and a $(\mathcal{Y}, \mathcal{B}, R_B)$-device $\mathcal{D}_B$ for Bob. The protocol $\mathcal{P}_{\mathcal{D}_A,\mathcal{D}_B}$ is a CPTP map taking as input a state $\omega^0_{R_AR_B} \in \mathcal{S}(R_AR_B)$ that initialises the devices. At the end of the protocol, either Alice and Bob output a string of ℓ bits in respective registers K_A and K_B, or they abort the protocol with output $K_A = K_B = |\perp\rangle\langle\perp|$. The QKD protocol is comprised of local operations and classical communication (LOCC) over the authenticated channel. Both parties also have access to trusted sources of randomness. Alice can interact n times with $\mathcal{D}_A$ and Bob can interact n times with $\mathcal{D}_B$, where n is the number of rounds.*

While the above is quite generic, usual protocols proceed in well-defined rounds and are then followed by a post-processing phase comprised of parameter estimation, error correction and privacy amplification. In each of the n measurement rounds of a DIQKD protocol, Alice and Bob use their local sources of randomness to independently generate measurement settings $X_i \in \mathcal{X}$ and $Y_i \in \mathcal{Y}$ which they input to their respective devices $\mathcal{D}_A$ and $\mathcal{D}_B$ to receive classical outputs $A_i \in \mathcal{A}$ and $B_i \in \mathcal{B}$. See Figure 1 for a diagram of a QKD protocol using a $(\mathcal{X}, \mathcal{A}, R_A)$-device $\mathcal{D}_A$ for Alice and a $(\mathcal{Y}, \mathcal{B}, R_B)$-device $\mathcal{D}_B$ for Bob. Usual protocols may abort in the parameter estimation or error correction phases, and throughout the text we use Ω to denote the event that the protocol *does not abort*. Consequently, Ω^c is the event that the protocol *aborts*.

We call a pair of devices $\mathcal{D}_A^{\mathrm{hon}}$ and $\mathcal{D}_B^{\mathrm{hon}}$ together with an initial state $\omega^{\mathrm{hon}}_{R_AR_B}$ *honest* with respect to a game $\mathcal{G}$ if the rounds are independent and, in each round, they win $\mathcal{G}$ with sufficiently high probability ω_{exp}. With these definitions, and following [18], we say that a QKD protocol is complete if the following holds.

Definition 6 (Completeness). *An (n, ℓ)-QKD protocol $\mathcal{P}_{\cdot,\cdot}$ for a game $\mathcal{G}$ is $\varepsilon_{\mathrm{com}}$-complete if, for any honest triple $(\mathcal{D}_A^{\mathrm{hon}}, \mathcal{D}_B^{\mathrm{hon}}, \omega^{\mathrm{hon}}_{R_AR_B})$, we have*

$$\Pr[\Omega^c]_\rho \leq \varepsilon_{\mathrm{com}}\,, \qquad \textit{where} \qquad \rho_{K_AK_B} = \mathcal{P}_{\mathcal{D}_A^{\mathrm{hon}},\mathcal{D}_B^{\mathrm{hon}}}(\omega^{\mathrm{hon}}_{R_AR_B}). \tag{15}$$

Completeness is purely a statement about the noise resilience of the protocol. Intuitively, a protocol is complete if the error correction and parameter estimation phases are designed so that in an honest implementation of the protocol subject to noise specified by some noise model, the probability of not aborting is higher than $1 - \varepsilon_{\mathrm{com}}$.

[2] We could even define a universal device that determines its behaviour after reading out a program from a classical register in R; however, this perspective does not seem to simplify our arguments significantly.

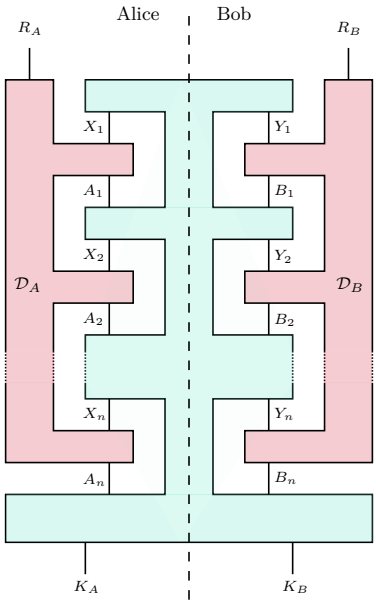


Figure 1: An (n, ℓ)-QKD protocol $\mathcal{P}_{\mathcal{D}_A,\mathcal{D}_B}(\cdot)$. The 'combs' on the left and right correspond to the devices used by Alice and Bob, respectively. On the other hand, the central part represents the operations by the honest parties, which include generation of the inputs fed to the combs during the measurement phase and the post-measurement classical processing after receipt of outputs A_n, B_n to produce the final keys K_A, K_B.

For the remaining security definitions we need to consider the scenario in which the devices are not honest and in which a potential eavesdropper is actively tampering with the QKD protocol in order to guess the keys generated by the honest parties. In particular, we consider devices $\mathcal{D}_A$ and $\mathcal{D}_B$ that are prepared by the eavesdropper, and denote the initial state shared amongst the two devices by $\omega^0_{R_A R_B E}$, where E is additionally held by the eavesdropper[3]. The normalised state at the end of a QKD protocol $\mathcal{P}$ using such devices is

$$\rho_{K_A K_B E} = \mathcal{P}_{\mathcal{D}_A,\mathcal{D}_B}(\omega^0_{R_A R_B E}) = \Pr[\Omega]_\rho \cdot \rho_{K_A K_B E|\Omega} + \Pr[\Omega^c]_\rho \cdot |\perp\perp\rangle\langle\perp\perp|_{K_A K_B} \otimes \rho_{E|\Omega^c}. \tag{16}$$

Without loss of generality, we also assume that the eavesdropper is passive. That is, the eavesdropper stores all public communication and maintains her own quantum register, but does not perform any operations on her quantum state until after the protocol is terminated. Indeed, a data processing inequality asserts that her available (quantum or classical) information is maximised in this way.

Having established this notation, we define what it means for a QKD protocol receiving uncharacterised devices $\mathcal{D}_A$ and $\mathcal{D}_B$ as inputs to be *secure*. We adopt the security definitions from [18] which are based on the definitions from [51].

Definition 7 (Soundness)**.** *An (n, ℓ)-QKD protocol $\mathcal{P}_{\cdot,\cdot}$ for a game $\mathcal{G}$ is ε_{sou}-sound if for any triple $(\mathcal{D}_A, \mathcal{D}_B, \omega^0_{R_A R_B E})$, the post-protocol state $\rho_{K_A K_B E}$ as defined in Eq.* (16) *satisfies*

$$\left\| \rho_{K_A K_B E \wedge \Omega} - \frac{1}{2^\ell} \sum_{i=0}^{2^\ell - 1} |ii\rangle\langle ii|_{K_A K_B} \otimes \rho_{E \wedge \Omega} \right\|_{\text{Tr}} \leq \varepsilon_{\text{sou}}\,. \tag{17}$$

In [6] and [18] it is proven that soundness is guaranteed by the following simpler conditions:

Definition 8 (Correctness)**.** *An (n, ℓ)-QKD protocol $\mathcal{P}_{\cdot,\cdot}$ for a game $\mathcal{G}$ is $\varepsilon_{\text{corr}}$-correct if for any triple $(\mathcal{D}_A, \mathcal{D}_B, \omega^0_{R_A R_B E})$, the post-protocol state $\rho_{K_A K_B E}$ as defined in Eq.* (16) *satisfies*

$$\Pr[K_A \neq K_B \wedge \Omega]_\rho \leq \varepsilon_{\text{corr}}\,. \tag{18}$$

[3]Without loss of generality we can assume that this state is pure, but this only clutters notation here.

Definition 9 (Secrecy)**.** *An (n, ℓ)-QKD protocol $\mathcal{P}_{\cdot,\cdot}$ for a game $\mathcal{G}$ is ε_{sec}-secret if for any triple $(\mathcal{D}_A, \mathcal{D}_B, \omega_{R_A R_B E})$, the post-protocol state $\rho_{K_A K_B E}$ as defined in Eq.* (16) *satisfies*

$$\|\rho_{K_A E \wedge \Omega} - \tau_{K_A} \otimes \rho_{E \wedge \Omega}\|_{\text{Tr}} \leq \varepsilon_{\text{sec}} \tag{19}$$

where τ_{K_A} is the maximally mixed state of dimension 2^ℓ.

In particular, if a protocol is $\varepsilon_{\text{corr}}$-correct and ε_{sec}-secret then it is $(\varepsilon_{\text{corr}} + \varepsilon_{\text{sec}})$-sound.

2.4 The NLG-DIQKD protocol

In this section, we introduce a device independent quantum key distribution protocol for arbitrary non-local games with suitable extensions as defined in Section 2.2. We prove security of this protocol for the family of non-local games satisfying $\omega_2 > \omega_3$, a *monogamy-of-entanglement* property arising from the fact that the optimal strategy for $\mathcal{G}_2$ requires the players to distribute entanglement and as such may not be further strongly correlated to the third player in $\mathcal{G}_3$ [3, 4].

Before describing the protocol, we introduce the following definition.

Definition 10 (2-universal hash function)**.** *Let $\mathcal{H} := \{H : \{0,1\}^m \to \{0,1\}^l\}$ be a family of hash functions. The family $\mathcal{H}$ is 2-universal if for any $H \in \mathcal{H}$ chosen uniformly*

$$\Pr[H(x) = H(x')]_H \leq \frac{1}{2^l}, \tag{20}$$

for all distinct $x, x' \in \{0,1\}^m$. We refer to l as the length of the outputs of the hash family.

For the DIQKD protocol, fix a game $\mathcal{G} := (\pi, \mathcal{X}, \mathcal{Y}, \mathcal{A}, \mathcal{B}, V)$, where $\pi(x, y)$ is a product on distributions on $\mathcal{X}$ and $\mathcal{Y}$, and the predicate is of the form in Eq. (13) for functions $SK_A : \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \to \{0,1\}$ and $SK_B : \mathcal{X} \times \mathcal{Y} \times \mathcal{B} \to \{0,1\}$. Let ω_2 be the quantum value of $\mathcal{G}$ and let ω_3 be the quantum value of its tripartite extension as described in Section 2.2. Protocol $\mathcal{P}$ is presented in algorithm 1 below. We discuss its components separately.

Measurement: In each round of the measurement phase, Alice and Bob use their respective devices $\mathcal{D}_A, \mathcal{D}_B$ to measure the state in the quantum register R with independently chosen measurement settings $X_i \in \mathcal{X}, Y_i \in \mathcal{Y}$ to obtain classical outputs $A_i \in \mathcal{A}, B_i \in \mathcal{B}_i$. We focus on protocols where the measurements inputs in testing rounds (when $T_i = 1$) and generation rounds (when $T_i = 0$) are the same (see discussion following Figure 2);

Sifting: In the sifting step, Alice and Bob announce all their measurement settings to subsequently compute raw keys as given by the respective assignments $SK_A : \mathcal{X} \times \mathcal{Y} \times \mathcal{A} \to \{0,1\}$ and $SK_B : \mathcal{X} \times \mathcal{Y} \times \mathcal{B} \to \{0,1\}$. Recall that the non-local game's winning condition was defined in Eq. (13) as the Boolean $[SK_A(x, y, a) = SK_B(x, y, b)]$ which captures the intuition that the sifted keys match whenever the non local game is won.

Parameter Estimation (PE): Here, Alice announces her output for the measurement rounds in which $T_i = 1$ which Bob uses to test the predicate of the non-local game in order to detect a potential eavesdropper. At this stage, Bob can abort if the number of unsuccessful instances of the non-local game is above a certain threshold from the tolerated winning probability of the game $\mathcal{G}$ due to noise ω_{exp}, up to certain tolerance δ_{tol}. We use Ω_{PE} to denote the event that the PE check passes.

The parameter estimation step is characterised by the tuple $\mathbf{pe} = (\gamma, \omega_{\text{exp}}, \delta_{\text{tol}})$.

Error Correction (EC): In this step, Alice and Bob apply an error correction scheme characterised by functions $\text{Synd} : \{0,1\}^n \to \{0,1\}^{\lambda_{\text{EC}}}$ and $\text{Corr} : \{0,1\}^n \times \{0,1\}^{\lambda_{\text{EC}}} \to \{0,1\}^n$. Alice computes $\text{Synd} : S_A \mapsto Z = \text{Synd}(S_A) \in \{0,1\}^{\lambda_{\text{EC}}}$ and sends the resultant syndrome to Bob, who applies $\text{Corr} : (S_B, Z) \mapsto \hat{S}_B$ to obtain an estimate for Alice's raw key. The length λ_{EC} of the syndrome is a parameter of the error correction protocol which needs to be chosen so that for a protocol instantiated with the

Algorithm 1: A sequential protocol for DIQKD from non-local games: $\mathcal{P}$

Input : Devices $\mathcal{D}_A, \mathcal{D}_B$

Parameters : Number of rounds n
PE parameters, $\mathbf{pe} = (\gamma, \omega_{\text{exp}}, \delta_{\text{tol}})$
EC parameters, $\mathbf{ec} = (\text{Synd}, \text{Corr}, \mathcal{H}_{\text{EC}}, l_{\text{EC}})$
PA parameters, $\mathbf{pa} = (\mathcal{H}_{\text{PA}}, l_{\text{key}})$

1. Measurement;
for $i = 1$ *to* n **do**
  Bob chooses $T_i \in \{0, 1\}$ with $\Pr[T_i = 1] = \gamma$;
  Alice chooses $X_i \in \mathcal{X}$ and inputs it to $\mathcal{D}_A$ to receive $A_i \in \mathcal{A}$;
  Bob chooses $Y_i \in \mathcal{Y}$ and inputs it to $\mathcal{D}_B$ to receive $B_i \in \mathcal{B}$;
end
2. Sifting;
Bob announces T_1^n;
Alice and Bob respectively announce X_1^n, Y_1^n;
Alice sets $S_A = \{SK_A(X_i, Y_i, A_i)\}_{i=1}^n$;
Bob sets $S_B = \{SK_B(X_i, Y_i, B_i)\}_{i=1}^n$;
3. Parameter Estimation;
Alice sets $T_{\text{test}} = \{i \ : \ T_i = 1\}$ and sends $S_{A,T_{\text{test}}} = \{S_{A,i} \ : \ i \in T_{\text{test}}\}$ to Bob ;
Bob sets $C_i = V(A_i, B_i, X_i, Y_i)$ for all $i \in T_{\text{test}}$ and $C_i = \perp$ for all $i \in \{1, ..., n\} \backslash T_{\text{test}}$;
if $|\{i \ : \ C_i = 0\}| \leq (1 - \omega_{\text{exp}} + \delta_{\text{tol}}) \cdot \gamma n$ **then**
  Bob announces $F_{\text{PE}} = \checkmark$;
else
  Bob announces $F_{\text{PE}} = \times$, both parties output $K_A = K_B = |\perp\rangle\langle\perp|$;
end
4. Error Correction;
Alice sends $Z = \text{Synd}(S_A)$, $H_A = H_{\text{EC}}(S_A)$ and choice of $H_{\text{EC}} \in \mathcal{H}_{\text{EC}}$ to Bob;
Bob computes guess $\hat{S}_B = \text{Corr}(S_B, Z)$ and $H_B = H_{\text{EC}}(\hat{S}_B)$;
if $H_A = H_B$ **then**
  Bob announces $F_{\text{EC}} = \checkmark$;
else
  Bob announces $F_{\text{EC}} = \times$, both parties output $K_A = K_B = |\perp\rangle\langle\perp|$;
end
5. Privacy Amplification;
Alice and Bob agree on $H_{\text{PA}} \in \mathcal{H}_{\text{PA}}$;
Alice outputs $K_A = H_{PA}(S_A)$ of length l_{key};
Bob outputs $K_B = H_{PA}(\hat{S}_B)$ of length l_{key}

honest tuple $(\mathcal{D}_A^{\text{hon}}, \mathcal{D}_B^{\text{hon}}, \omega_{R_A R_B}^{\text{hon}})$ winning $\mathcal{G}$ with a probability ω_{exp} which depends on the noise model, then

$$\Pr\Big[S_A \neq \hat{S}_B\Big]_{\text{hon}} \leq \varepsilon_{\text{com}}^{\text{EC}}, \tag{21}$$

for a given completeness parameter $\varepsilon_{\text{com}}^{\text{EC}} \in (0, 1]$. In the above, the probability is over the distribution generated by the honest triple $(\mathcal{D}_A^{\text{hon}}, \mathcal{D}_B^{\text{hon}}, \omega_{R_A R_B}^{\text{hon}})$ input to the protocol. Theoretical lower bounds for the length λ_{EC} achieving the condition above are explored in [52] and [53, Theorem 1]. In practice, for the values of n and $\varepsilon_{\text{com}}^{\text{EC}}$ typically considered in QKD protocols, it suffices to take $\lambda_{\text{EC}} = \xi n h(Q)$ for $\xi \in [1.05, 1.12]$ since this achieves the condition in Eq. (21) and it is what practical error correcting codes communicate —see the discussion in [53] or [6, Footnote 10]. Here $h(p) := -p\log(p) - (1-p)\log(1-p)$ is the binary entropy of a Bernoulli variable, and Q is known as the *quantum bit error rate* (QBER) and corresponds to the probability that a bit needs to be corrected—in a QKD protocol this occurs when the i-th key bits do not match, i.e., when $S_{A,i} \neq \hat{S}_{B,i}$.

The hash function $H_{\text{EC}} \in \mathcal{H}_{\text{EC}}$ agreed upon by Alice and Bob is subsequently used to produce hashes of length l_{EC} to verify whether the error correction was successful and $S_A = \hat{S}_B$. Indeed, the defining property of 2-universal hash functions (Definition 10) asserts that

$$\Pr\Big[H_{\text{EC}}(S_A) = H_{\text{EC}}(\hat{S}_B) \mid S_A \neq \hat{S}_B\Big] \leq \frac{1}{2^{l_{\text{EC}}}}, \tag{22}$$

where the probability is over the choice of the hash function $H_{\text{EC}} \in \mathcal{H}_{\text{EC}}$. We use Ω_{EC} to denote the event that this verification passes.

Overall, the error correction is characterised by the tuple $\mathbf{ec} = (\text{Synd}, \text{Corr}, \mathcal{H}_{\text{EC}}, l_{\text{EC}})$, where the function Synd produces a syndrome of length λ_{EC}. As an important remark, we note that the error correction scheme is applied to the raw key bits of *all* rounds, not just generation rounds.

Privacy Amplification (PA): Finally, Alice and Bob apply an agreed upon hash function $H_{\text{PA}} \in \mathcal{H}_{\text{PA}}$ to produce final keys K_A, K_B of length l_{key}. The privacy amplification step is crucial to the secrecy of the protocol as is inferred from the *Leftover Hashing Lemma* [5] stated later in Lemma 2. Intuitively, the Leftover Hashing Lemma guarantees that the key K_A output by Alice is close to a perfect key provided that the sifted key S_A is sufficiently random from Eve's point of view, as quantified by a conditional entropy measure.

The privacy amplification is characterised by the tuple $\mathbf{pa} = (\mathcal{H}_{\text{PA}}, l_{\text{key}})$.

Before stating our main theorems, let us discuss some important notation of the protocol. We use $\rho = \mathcal{P}_{(\mathcal{D}_A, \mathcal{D}_B), (n, \mathbf{pe}, \mathbf{ec}, \mathbf{pa})}(\omega_{R_A R_B Q_E}^0)$ to denote the state shared by Alice, Bob and Eve at the end of the protocol initialised with input devices $\mathcal{D}_A, \mathcal{D}_B$ sharing initial state $\omega_{R_A R_B Q_E}^0 \in S(R_A R_B E)$, as well as parameters $\mathbf{pe}, \mathbf{ec}, \mathbf{pa}$ respectively for parameter estimation, error correction and privacy amplification. The output state ρ contains the following registers:

$$\underbrace{A_1^n B_1^n X_1^n Y_1^n}_{\text{game}} \underbrace{S_A S_B \hat{S}_B}_{\text{raw keys}} \underbrace{C_1^n T_1^n S_{A,T_{\text{test}}}}_{\text{PE}} \underbrace{H_A H_B Z H_{\text{EC}}}_{\text{EC}} \underbrace{H_{\text{PA}} K_A K_B}_{\text{secret keys}} \underbrace{F_{\text{PE}} F_{\text{EC}}}_{\text{flags}} Q_E, \tag{23}$$

where Q_E is Eve's quantum side information. Note that register $S_{A,T_{\text{test}}}$ containing Alice's classical outputs in testing rounds is redundant as $S_{A,T_{\text{test}}} \subset S_A$ but we include it to emphasize that it is announced and as such, Eve has access to it. In general, Eve's total side information in an instance of protocol $\mathcal{P}_{(\mathcal{D}_A, \mathcal{D}_B), (n, \mathbf{pe}, \mathbf{ec}, \mathbf{pa})}$ is

$$E = X_1^n Y_1^n T_1^n S_{A,T_{\text{test}}} H_A Z H_{\text{EC}} H_{\text{PA}} F_{\text{PE}} F_{\text{EC}} Q_E. \tag{24}$$

Further, we use σ to denote the state prior to the privacy amplification step. The state σ contains the same registers as the state ρ at the end of the protocol minus K_A and K_B.

3 Main results

3.1 Security for general monogamy-of-entanglement games

In this section we state and discuss our main results, which we prove later in Section 4. We remark that the only *inputs* to the protocol are the physical uncharacterised devices $\mathcal{D}_A$ and $\mathcal{D}_B$ of the honest

parties, whereas all variables appearing in the theorems are *parameters* of the protocol, chosen to achieve appropriate security and/or maximize key rate.

Theorem 1 (Completeness)**.** *Let $n \in \mathbb{N}$, $\epsilon_{\text{com}}^{\text{PE}}, \epsilon_{\text{com}}^{\text{EC}} \in (0,1]$. For any honest triple $(\mathcal{D}_A^{\text{hon}}, \mathcal{D}_B^{\text{hon}}, \omega_{R_A R_B}^{\text{hon}})$ which plays the game $\mathcal{G}$ independently in every round and wins with probability ω_{exp}, the protocol $\mathcal{P}_{(\mathcal{D}_A^{\text{hon}}, \mathcal{D}_B^{\text{hon}}),(n,\mathbf{pe},\mathbf{ec},\mathbf{pa})}$ with parameters $\mathbf{ec} = (\text{Synd}, \text{Corr}, \mathcal{H}_{\text{EC}}, l_{\text{EC}})$ and $\mathbf{pe} = (\gamma, \omega_{\text{exp}}, \delta_{\text{tol}})$ is $(\varepsilon_{\text{com}}^{\text{PE}} + \varepsilon_{\text{com}}^{\text{EC}})$-complete if $\mathbf{ec}$ is chosen so that*

$$\Pr\Big[S_A \neq \hat{S}_B\Big]_{\rho^{\text{hon}}} \leq \varepsilon_{\text{com}}^{\text{EC}}, \qquad \text{where} \qquad \rho^{\text{hon}} = \mathcal{P}_{(\mathcal{D}_A^{\text{hon}}, \mathcal{D}_B^{\text{hon}}),(n,\mathbf{pe},\mathbf{ec},\mathbf{pa})}(\omega_{R_A R_B}^{\text{hon}}) \tag{25}$$

and if

$$\gamma \geq \frac{2(1-\omega_{\text{exp}}) + \delta_{\text{tol}}}{{\delta_{\text{tol}}}^2 n} \ln \frac{1}{\varepsilon_{\text{com}}^{\text{PE}}}. \tag{26}$$

Intuitively, Eq. (25) induces a requirement on the error correction protocol specified by the tuple $\mathbf{ec} = (\text{Synd}, \text{Corr}, \mathcal{H}_{\text{EC}}, l_{\text{EC}})$, given the honest triple $(\mathcal{D}_A^{\text{hon}}, \mathcal{D}_B^{\text{hon}}, \omega_{R_A R_B}^{\text{hon}})$. The value ω_{exp} differs from the maximal two player winning probability ω_2 by an amount characterised by the underlying noise in the devices used to distribute and interact with the quantum states over registers $R_A R_B$. The overall quantum bit error rate for any noise model is defined by $Q = 1 - \omega_{\text{exp}}$, such that the number of errors follows a binomial distribution with probability Q and overall expected number of errors nQ. As such, the error correction protocol $\mathbf{ec}$ is designed to correct this random number of errors with high probability (in this case, $1 - \varepsilon_{\text{com}}^{\text{EC}}$). In practice, the choice of error correcting code is heuristic, although it is shown in [53, Theorem 1] that for any parameter $\varepsilon_{\text{com}}^{\text{EC}}$, there exists an error correction scheme satisfying Eq. (25).

On the other hand, Eq. (26) is a requirement on the parameter estimation stage. In particular, for the triple $(\mathcal{D}_A^{\text{hon}}, \mathcal{D}_B^{\text{hon}}, \omega_{R_A R_B}^{\text{hon}})$ as above, we require the testing probability γ and tolerance δ_{tol} to be chosen so that the number of losses in an instance of $\mathcal{P}$ does not fall far above the expected number of loses $(1 - \omega_{\text{exp}})n\gamma$ except with small probability. In essence, Eq. (26) is derived from a 'tail bound' on the probability that the tolerated number of loses deviates from the expected number of losses, and δ_{tol} is chosen to make this probability small (by $\varepsilon_{\text{com}}^{\text{PE}}$). Given the value of γ in the theorem, the value of δ_{tol} is chosen so that δ_{tol} and γ vanish as n approaches infinity. In practice, we set $\delta_{\text{tol}} = n^{-1/3}$ so that asymptotically, $\delta_{\text{tol}}, \gamma \in O(n^{-1/3})$.

Theorem 2 (Correctness)**.** *Let $n \in \mathbb{N}$ and $\varepsilon_{\text{corr}} \in (0,1]$. For any triple $(\mathcal{D}_A, \mathcal{D}_B, \omega_{R_A R_B Q_E}^0)$, the protocol $\mathcal{P}_{(\mathcal{D}_A, \mathcal{D}_B),(n,\mathbf{pe},\mathbf{ec},\mathbf{pa})}$ with $\mathbf{ec} = (\text{Synd}, \text{Corr}, \mathcal{H}_{\text{EC}}, l_{\text{EC}})$ is $\varepsilon_{\text{corr}}$-correct if $l_{\text{EC}} \geq \log \frac{1}{\varepsilon_{\text{corr}}}$.*

In our protocol, correctness is ensured by comparing random hashes of Alice's raw key S_A and Bob's guess $\hat{S}_B$. Thus, this theorem does not need to refer to the actual error correction protocol $(\text{Synd}, \text{Corr})$.

Theorem 3 (Secrecy)**.** *Let $n \in \mathbb{N}$ and $\varepsilon_{\text{sec}} \in (0,1]$. For any triple $(\mathcal{D}_A, \mathcal{D}_B, \omega_{R_A R_B Q_E}^0)$, protocol $\mathcal{P}_{(\mathcal{D}_A, \mathcal{D}_B),(n,\mathbf{pe},\mathbf{ec},\mathbf{pa})}$ with $\mathbf{pe} = (\gamma, \omega_{\text{exp}}, \delta_{\text{tol}})$, $\mathbf{ec} = (\text{Synd}, \text{Corr}, \mathcal{H}_{\text{EC}}, l_{\text{EC}})$ and $\mathbf{pa} = (\mathcal{H}_{\text{PA}}, l_{\text{key}})$ is ε_{sec}-secret if*

$$l_{\text{key}} \leq ng(\omega_{\text{exp}} - \delta_{\text{tol}}) - d_1\sqrt{n} - d_0 - (2 - \omega_{\text{exp}} + \delta_{\text{tol}})n(\gamma + \kappa) - 2\vartheta\left(\frac{\varepsilon_s}{4}\right) \tag{27}$$

$$- l_{\text{EC}} - \lambda_{\text{EC}} - 2\log\frac{1}{\varepsilon_{\text{sec}} - 2\varepsilon_s}, \tag{28}$$

where $\varepsilon_s \in \left(0, \frac{1}{2}\varepsilon_{\text{sec}}\right)$ is a variable to be optimised, $\kappa \geq \frac{1}{\sqrt{n}}\sqrt{\ln 8 - \ln \varepsilon_s}$, $g : [0,1] \to \mathbb{R}$ is the affine function defined by

$$g(p) := \frac{p - \beta}{\ln 2 \cdot (1 - \beta + \omega_3)} - \log\left(1 - \beta + \omega_3\right) \tag{29}$$

for $\beta \in [\omega_3, \omega_2]$ to be optimised, and the coefficients d_1, d_0 depend only on ε_{sec}, ε_s and β and are respectively as in Eqs. (161) *and* (162)*. Lastly, $\vartheta(\delta) = -\log\left(1 - \sqrt{1 - \delta^2}\right)$.*

In particular, the protocol is $(\varepsilon_{\text{corr}} + \varepsilon_{\text{sec}})$-sound, provided $\mathbf{pe}, \mathbf{ec}, \mathbf{pa}$ are chosen as per Theorem 2 and Theorem 3.

We now discuss the variables appearing in the these theorems. The variable ε_s corresponds to a bound on the probability that the error correction is successful (i.e. that $S_A = \hat{S}_B$) provided that the parameter estimation check is successful. The variable κ is necessary to ensure the number of testing rounds does not exceed $n(\gamma + \kappa)$ except with negligible probability. The variables $\varepsilon_s \in (0, \frac{1}{2}\varepsilon_{\text{sec}})$ and $\beta \in [\omega_3, \omega_2]$ are to be optimised to maximize the key rate $\frac{1}{n} l_{\text{key}}$.

On the other hand, the function g appearing in Eq. (27) intuitively represents the amount of randomness that is secret from Eve which Alice is able to generate in every round of the protocol. The function g presented in Eq. (80) is derived solely from the fact that the non-local game satisfies the monogamy-of-entanglement property $\omega_3 < \omega_2$ (see Section 4.4.3). In principle, it is possible to tailor g to specific non-local games to achieve better key rates without altering the underlying secrecy proof. For example, see Section 3.2 for improved key rates for the magic square game, and Section 5 for the respective constructions.

3.1.1 Asymptotic analysis

In the following, we briefly analyse the asymptotic behaviour of l_{key} in Eq. (27) for an honest implementation of the protocol.

Firstly, we note that in an honest implementation the n measurement rounds are independently and identically distributed (i.i.d.) and that the devices utilise the optimal quantum strategy for $\mathcal{G}_2$. Formally, let $\mathcal{S} = \{\nu_{Q_A Q_B}, \{\{P_a^x\}_a\}_x, \{\{Q_b^y\}_b\}_y\}$ be the strategy that maximizes ω_2, where $\nu_{Q_A Q_B} \in S(Q_A Q_B)$ is Alice's and Bob's bipartite state and $\{P_a^x\}_a, \{Q_b^y\}_b$ are POVMs on Q_A, Q_B with outputs over sets $\mathcal{A}, \mathcal{B}$ and inputs over sets $\mathcal{X}, \mathcal{Y}$, respectively. The state $\nu_{Q_A Q_B}$ may be subject to noise which in QKD is usually modelled using the depolarizing channel

$$\mathcal{E}_q : \nu_{Q_A Q_B} \mapsto \tilde{\nu}_{Q_A Q_B} = (1 - 2q)\nu_{Q_A Q_B} + 2q\tau_{Q_A Q_B}, \tag{30}$$

where $q \in [0, \frac{1}{2}]$ and $\tau_{Q_A Q_B} = \frac{\mathbb{I}_{Q_A Q_B}}{\dim Q_A \dim Q_B}$ is the maximally mixed state in $Q_A Q_B$. Therefore, in an honest implementation of the QKD protocol the devices $\mathcal{D}_A^{\text{hon}}, \mathcal{D}_B^{\text{hon}}$ share the i.i.d. state $\omega_{R_A R_B}^{\text{hon}} = \tilde{\nu}_{Q_A Q_B}^{\otimes n}$. In the following, we omit the round indexes since the behaviour is i.i.d.. Then, on input of X by Alice and Y by Bob, the respective devices $\mathcal{D}_A^{\text{hon}}$ and $\mathcal{D}_B^{\text{hon}}$ apply the local measurements given by

$$\mathcal{M}_A^{x,\text{hon}} \otimes \mathcal{M}_B^{y,\text{hon}} : \tilde{\nu}_{Q_A Q_B} \mapsto \sum_{a \in \mathcal{A}} \sum_{b \in \mathcal{B}} |ab\rangle\langle ab|_{AB} \otimes \text{Tr}[\tilde{\nu}_{Q_A Q_B}(P_a^x \otimes Q_b^y)]. \tag{31}$$

It follows that the expected winning probability of Alice and Bob is precisely

$$\omega_{\text{exp}} = \sum_{x,y,a,b} \pi(x,y) V(a,b,x,y) \,\text{Tr}[\tilde{\nu}_{Q_A Q_B}(P_a^x \otimes Q_b^y)], \tag{32}$$

where $V(a,b,x,y)$ is the non-local game's predicate as in Eq. (13). The quantum bit error rate is therefore given by $Q := 1 - \omega_{\text{exp}}$. To determine the length of the error correction syndrome λ_{EC}, note that [53, Theorem 1] implies the existence of error correction protocol $\mathbf{ec} = (\text{Synd}, \text{Corr}, \mathcal{H}_{\text{EC}}, l_{\text{EC}})$ which asymptotically satisfies[4] $\frac{\lambda_{\text{EC}}}{n} = h(Q) + \Theta\left(\frac{\log n}{n}\right)$ and achieves $\Pr\left[S_A \neq \hat{S}_B\right]_{\rho^{\text{hon}}} \leq \varepsilon_{\text{com}}^{\text{EC}}$. Further, note that choosing

$$\delta_{\text{tol}} = \frac{1}{n^{1/3}} \qquad \text{and} \qquad \gamma = \frac{2(1 - \omega_{\text{exp}}) + \delta_{\text{tol}}}{{\delta_{\text{tol}}}^2 n} \ln \frac{1}{\varepsilon_{\text{com}}^{\text{PE}}} \tag{33}$$

as per Theorem 1, we asymptotically obtain $\delta_{\text{tol}}, \gamma \in O\big(n^{-1/3}\big)$.

With this choice of $\lambda_{\text{EC}}, \gamma$ and δ_{tol} we have $(\varepsilon_{\text{com}}^{\text{EC}} + \varepsilon_{\text{com}}^{\text{PE}})$-completeness, and from Eq. (27) we arrive at

$$\lim_{n \to \infty} \frac{l_{\text{key}}}{n} = g(\omega_{\text{exp}}) - h(Q). \tag{34}$$

[4]Here, we use $g(n) \in \Theta(f(n))$ to denote both $g(n) \in O(f(n))$ and $g(n) \in \Omega(f(n))$.

The first term encapsulates the amount of Alice's key that is secret from Eve, whereas the second relates to the cost of information reconciliation between Alice and Bob. We remark that this asymptotic key rate retrieves the *Devetak-Winter rate* [54] if g is chosen to be a sufficiently tight bound on the von Neumann entropy.

In Figure 2 we compute the range of values of ω_2 and ω_3 for which Eq. (34) using g as in Eq. (80) gives positive asymptotic key rates. In particular, we highlight two games: the *magic square game* (MSG) which we consider in the next section with better optimized functions g, and the *Clauser-Horne-Simone-Holt* (CHSH) game which most DIQKD protocols use as primitive. In the latter game, Alice and Bob produce binary inputs x, y and generate binary outputs a, b, and win or lose if $a = b \oplus (x \cdot y)$. In the tripartite extension, the third player receives both x, y and produces bit c. The three parties win if $a = b \oplus (x \cdot y) = c$. In this case it is known that $\omega_2 = \frac{2+\sqrt{2}}{4} \approx 0.85$ and it can be shown that $\omega_3 \approx \frac{3}{4}$ (see [55]). Using our framework, the difference between ω_2 and ω_3 in the CHSH game is not sufficient to offset the cost of error correction. Indeed, in the noiseless case practical codes require $1.1h(1 - \frac{2+\sqrt{2}}{4}) \approx 0.661$ bits of error correction per round of the protocol. To circumvent this problem, it is possible to use different measurement settings in testing and generation rounds in such a way that the generation settings produce highly correlated outcomes for Alice and Bob, thereby reducing the cost of error correction—see for example the framework in [2, 37, 18, 21]. We do not explore this route here as it has already been extensively analysed in the aforementioned works, but remark that the functions which bound the amount of randomness of Alice which is secret from Eve obtained in the works of [18, 21] may directly replace the function g in Eq. (27) of Theorem 3 to yield equivalent secrecy guarantees and positive key rates for the CHSH game.

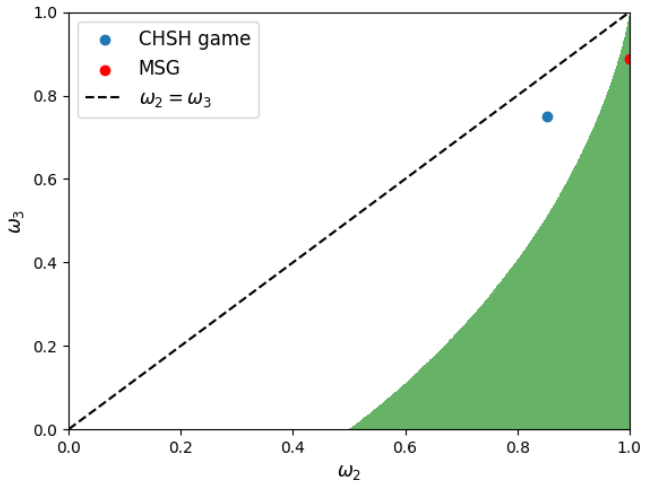


Figure 2: Shaded green area corresponds to the range of bipartite winning probabilities ω_2 and tripartite winning probabilities ω_3 from which Eq. (34) yields a positive asymptotic key rate.

3.2 Application with the magic square game

In this section, we apply our NLG-DIQKD protocol to the magic square game which we briefly describe in the following.

The two party magic square game MSG_2 proceeds as follows:

- Alice receives $x \in \{0, 1, 2\}$ with uniform probability and outputs $a \in \{0, 1\}^3$ s.t. $\bigoplus_k a[k] = 0$.
- Bob receives $y \in \{0, 1, 2\}$ with uniform probability and outputs $b \in \{0, 1\}^3$ s.t. $\bigoplus_k b[k] = 1$.

Alice and Bob win if $a[y] = b[x]$, where $a[k]$ (respectively $b[k]$) denotes the k-th bit in a (b).

It is known [40, 41] that $\omega_C(\mathrm{MSG}_2) = \frac{8}{9}$ and $\omega_Q(\mathrm{MSG}_2) = 1$. The best classical strategy consists of preparing a 3×3 grid of bits such that the rows satisfy Alice's parity condition and the columns

satisfy Bob's parity condition. Any 3×3 grid filled in this way always has one square which is impossible to fill, so Alice and Bob always lose when their inputs x, y correspond to that square. The quantum strategy achieving $\omega_{\mathrm{Q}}(\mathrm{MSG}_2) = 1$ requires the honest parties to share $|\Phi^+\rangle_{Q_{A_1}Q_{B_1}} \otimes |\Phi^+\rangle_{Q_{A_2}Q_{B_2}}$ —that is, two copies of the maximally entangled Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$— and perform the following observables on their respective halves:

	$y=0$	$y=1$	$y=2$
$x=0$	$\mathbb{I} \otimes Z$	$Z \otimes \mathbb{I}$	$Z \otimes Z$
$x=1$	$X \otimes \mathbb{I}$	$\mathbb{I} \otimes X$	$X \otimes X$
$x=2$	$-X \otimes Z$	$-Z \otimes X$	$Y \otimes Y$

(35)

Namely, on input of x for Alice (respectively, y for Bob), she applies the three commuting observables in the x-th row (y-th column) on her halves of $|\Phi^+\rangle_{Q_{A_1}Q_{B_1}} \otimes |\Phi^+\rangle_{Q_{A_2}Q_{B_2}}$. Since the overlap of the x-th row and y-th column contains the same observables for Alice and Bob, they are guaranteed to obtain the same bit. Further, since the product of each row (respectively, each column) equals $\mathbb{I} \otimes \mathbb{I}$ (respectively $-\mathbb{I} \otimes \mathbb{I}$), the parity conditions are satisfied.

In the tripartite extension MSG_3, the third player receives both inputs $x, y \in \{0, 1, 2\}$ and produces the single bit c. The new predicate checks whether $a[y] = c$ in addition to $a[y] = b[x]$. It is easy to see that $\omega_{\mathrm{C}}(\mathrm{MSG}_3) = \frac{8}{9}$ and in Section 5 we use numerical optimization tools to show[5] $\omega_{\mathrm{Q}}(\mathrm{MSG}_3) \lesssim \frac{8.00077}{9}$.

Now, let us discuss the honest behaviour of MSG-DIQKD to compute finite and asymptotic key rates. In an honest implementation, the devices $\mathcal{D}_A^{\mathrm{hon}}, \mathcal{D}_B^{\mathrm{hon}}$ of Alice and Bob behave in an i.i.d. way and adhere to the optimal strategy of the bipartite magic square game: $\mathcal{S} = \{\nu_{Q_AQ_B}, \{\{P_a^x\}_a\}_x, \{\{Q_b^y\}_b\}_y\}$. In this strategy $\nu_{Q_AQ_B} = |\Phi^+\rangle\langle\Phi^+|_{Q_{A_1}Q_{B_1}} \otimes |\Phi^+\rangle\langle\Phi^+|_{Q_{A_2}Q_{B_2}}$ and $\{P_a^x\}_{a\in\mathcal{A}}$, $\{Q_b^y\}_{b\in\mathcal{B}}$ for $\mathcal{A} = \{000, 011, 101, 110\}$, $\mathcal{B} = \{001, 010, 100, 111\}$, are the POVMs associated to the observables in Eq. (35).

For the noise model, we assume that each of the two Bell states in $\nu_{Q_AQ_B}$ suffers from identical depolarising noise, resulting in the state

$$\tilde{\nu}_{Q_AQ_B} = \left((1-2q)\left|\Phi^+\right\rangle\!\left\langle\Phi^+\right| + 2q\tau\right)_{Q_{A_1}Q_{B_1}} \otimes \left((1-2q)\left|\Phi^+\right\rangle\!\left\langle\Phi^+\right| + 2q\tau\right)_{Q_{A_2}Q_{B_2}}, \tag{36}$$

where $q \in [0, \frac{1}{2}]$ and $\tau_{Q_{A_1}Q_{B_1}}, \tau_{Q_{A_2}Q_{B_2}}$ are the maximally mixed states of dimension four. The devices $\mathcal{D}_A^{\mathrm{hon}}, \mathcal{D}_B^{\mathrm{hon}}$ therefore share the state $\omega_{R_AR_B}^{\mathrm{hon}} = \tilde{\nu}_{Q_AQ_B}^{\otimes n}$. Standard calculations then show that overall QBER and expected winning probability for the bipartite magic square game are respectively

$$Q = \frac{2}{9}q(7-5q) \qquad \text{and} \qquad \omega_{\mathrm{exp}} = 1 - \frac{2}{9}q(7-5q). \tag{37}$$

Formally, this is because the state $\tilde{\nu}_{Q_AQ_B}$ is a mixture containing the state $\left|\Phi^+\right\rangle\!\left\langle\Phi^+\right|^{\otimes 2}$ with probability $(1-2q)^2$, the state $\tau^{\otimes 2}$ with probability $4q^2$, and the states $|\Phi^+\rangle\langle\Phi^+| \otimes \tau$ and $\tau \otimes |\Phi^+\rangle\langle\Phi^+|$ with probability $2q(1-2q)$ each. It's clear that the probabilities of winning when sharing $\left|\Phi^+\right\rangle\!\left\langle\Phi^+\right|^{\otimes 2}$ and $\tau^{\otimes 2}$ are 1 and $\frac{1}{2}$, respectively. On the other hand, when sharing the state $|\Phi^+\rangle\langle\Phi^+| \otimes \tau$, it is only possible to win with probability 1 when $(x, y) \in \{(0, 1), (1, 0)\}$ (corresponding to product observables $Z \otimes \mathbb{I}$ and $\mathbb{I} \otimes X$), which occurs with probability $\frac{2}{9}$ over the choice of inputs. All remaining inputs result in a winning probability of $\frac{1}{2}$. Similarly, when sharing the sate $\tau \otimes |\Phi^+\rangle\langle\Phi^+|$, inputs $(x, y) \in \{(0, 0), (1, 1)\}$ yield winning probability 1, whereas all other inputs yield $\frac{1}{2}$. Overall, linearity of the trace over this mixture of states gives

$$\omega_{\mathrm{exp}} = (1-2q)^2 \cdot 1 + 2 \cdot 2q(1-2q)\left(\frac{7}{9} \cdot \frac{1}{2} + \frac{2}{9} \cdot 1\right) + (2q)^2 \cdot \frac{1}{2} = 1 - \frac{2}{9}q(7-5q). \tag{38}$$

[5] In addition, we use the linear program specified in [56, Section 3] to show $\omega_{\mathrm{NS}}(\mathrm{MSG}_3) = 1$.

Now, we apply Theorem 1, Theorem 2 and Theorem 3 to compute the achievable finite sized key rates for the MSG-DIQKD protocol under this noise model and with optimized affine functions g derived in Section 5. Results are shown in Figure 3.

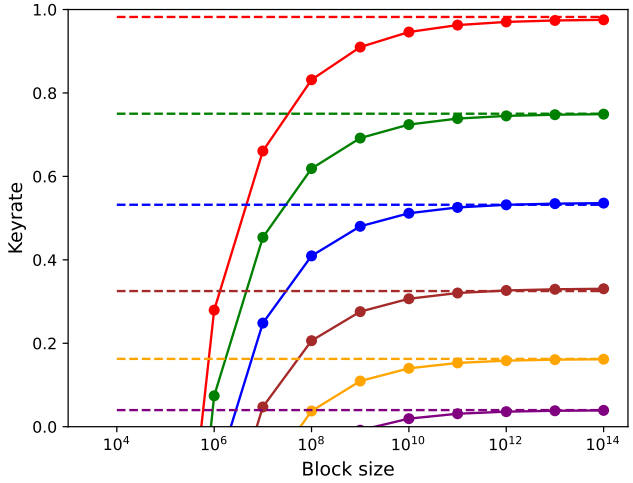


Figure 3: Keyrates for MSG-DIQKD protocol as a function of block size (i.e. number of rounds) under depolarizing noise. The curves correspond to depolarizing noise for $q \in \{0, 0.005, 0.01, 0.015, 0.02, 0.025\}$ (red, green, blue, brown, orange and purple, respectively), testing probability γ and noise tolerance δ_{tol} chosen as per Eq. (33). The key rates for $q \in \{0, 0.005, 0.01, 0.015\}$ (respectively $q \in \{0.02, 0.025\}$) were obtained using the min-tradeoff functions computed with the von Neumann entropy bounds of Eq. (196) (respectively min-entropy bounds of Eqs. (147),(183)). The parameter λ_{EC} is set to $1.1h(Q)$ and the security parameters are chosen as $\varepsilon_{\text{com}} = 10^{-2}$ and $\varepsilon_{\text{sou}} = 10^{-6}$. The dashed horizontal lines correspond to the asymptotic behaviour given by Eq. (34). See [55] for Python script used to generate this figure.

Following the finite key rates, we turn our attention to the asymptotic key rates of the MSG-DIQKD protocol. For the remainder of this section, we ignore round indexes and use X, Y, A, B to respectively denote the inputs and the outputs of Alice and Bob in an instance of the MSG. Further, we use S_A and S_B for the singular raw key bits generated from A and Y, and B and X, respectively. Since Alice's key bits are generated using arbitrary inputs of both Alice and Bob, and the error correction in the protocol is one-way, the asymptotic key rate of MSG-DIQKD is given by the Devetak-Winter bound [54]

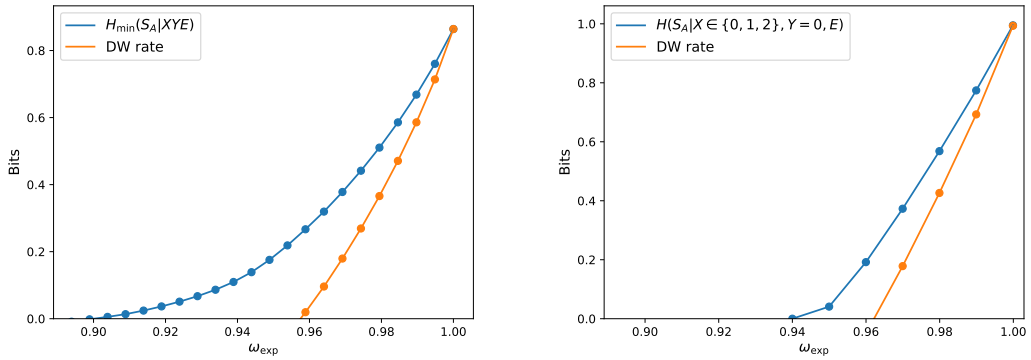
$$r \geq H(S_A|XYE)_{\hat{\nu}} - H(S_A|XYS_B)_{\hat{\nu}}, \tag{39}$$

where $\hat{\nu} \in S(S_A S_B XYE)$ is the post-measurement classical-quantum state shared by Alice, Bob and the eavesdropper Eve after one instance of the magic square game with the initial quantum state $\tilde{\nu} \in S(Q_A Q_B E)$ which extends the state in Eq. (36). Further, $H(\cdot|\cdot)$ is the conditional von Neumann entropy which for a bipartite state $\rho \in S(AB)$ is defined as $H(A|B)_\rho := H(AB)_\rho - H(B)_\rho$, for $H(A)_\rho := -\operatorname{Tr}[\rho \log \rho]$. In the Devetak-Winter rate, the first entropy term intuitively corresponds to the amount of Alice's randomness that is secret from Eve, whereas the second entropy term encapsulates the cost of error correction for Alice and Bob and equals the binary entropy of the QBER.

We present two bounds to the Devetak-Winter rate in Figure 4. In Figure 4a we use a bound on the min-entropy (defined in Section 4.1) to bound the first term in the Devetak-Winter rate. On the other hand, in Figure 4b we use the numerical bounds on the von Neumann entropy $H(S_A|X \in \{0,1,2\}, Y = 0; E)_{\hat{\nu}}$ specified in Eq. (194)[6]. Further, in Figure 5 we compare our asymptotic rates with those reported in the recent paper [46].

Note that in these figures the min-entropy bound yields better key rates in the regime with higher quantum bit error rate, whereas the von Neumann bounds perform better in the regime where $\omega_{\text{exp}} \gtrsim$

[6]The reduced choice of measurement settings in the von Neumann entropy is done to make the underlying optimization problem tractable. We remark that $H(S_A|X \in \{0,1,2\}, Y = 0; E)_{\hat{\nu}} \leq H(S_A|XYE)_{\hat{\nu}}$.



(a) Bounds with min-entropy.

(b) Bounds with von Neumann entropy.

Figure 4: Device independent bounds for MSG-DIQKD. Blue and orange lines respectively correspond to bounds on the conditional entropy and the asymptotic key rate. See [55] for Python script used to generate this figure.

0.985. This is purely a consequence of the reduced choice of measurement inputs in the optimization of Eq. (194) due to computational complexity of the optimization problem —indeed it is expected that $H(S|XYE) \geq H_{\min}(S|XYE)$.

The asymptotic rates using the min-entropy bounds from Section 5.2 suggest that positive key rate is only possible for quantum bit error rate lower than approximately 0.044, which corresponds to depolarizing noise of about 2.88% as per Eq. (37). The recent work [46, Figure 1 in Supp. Material] applies identical techniques to lower bound the entropy $H(S|X = 0, Y = 0; E)$, which they use to claim security of MSG-DIQKD against collective attacks in the asymptotic regime with robustness against depolarizing noise of about 1.6%[7].

4 Finite key security proof

Before delving into the proofs of completeness, correctness and secrecy of $\mathcal{P}$ (algorithm 1) we will need various definitions and prior results, presented in the following Preliminaries section.

4.1 Preliminaries

We will require some measures of closeness between different states. The *fidelity* between quantum states $\rho, \sigma \in S(A)$ is given by

$$F(\rho, \sigma) := \left(\operatorname{Tr} \left| \sqrt{\rho}\sqrt{\sigma} \right| \right)^2. \tag{40}$$

On the other hand, the *generalised fidelity* for subnormalised states $\rho, \sigma \in S_{\leq}(A)$ is given by

$$F_*(\rho, \sigma) := \left(\operatorname{Tr} \left| \sqrt{\rho}\sqrt{\sigma} \right| + \sqrt{(1 - \operatorname{Tr}\rho)(1 - \operatorname{Tr}\sigma)} \right)^2. \tag{41}$$

From the generalised fidelity we define the *purified distance*

$$P(\rho, \sigma) := \sqrt{1 - F_*(\rho, \sigma)}. \tag{42}$$

[7] We remark that the constraint originally used in [46] to bound $H(S|X = 0, Y = 0; E)$ correspond to Alice and Bob's winning probability take away Alice and Bob's losing probability. Hence, the original claimed results of [46, Figure 1 in Supp. Material] were horizontally scaled by a factor of $2x - 1$. We calculate the noise robustness of 1.6% of the protocol in [46] taking this error into consideration. We have notified the authors and these mistakes have been corrected in the latest version of [46].

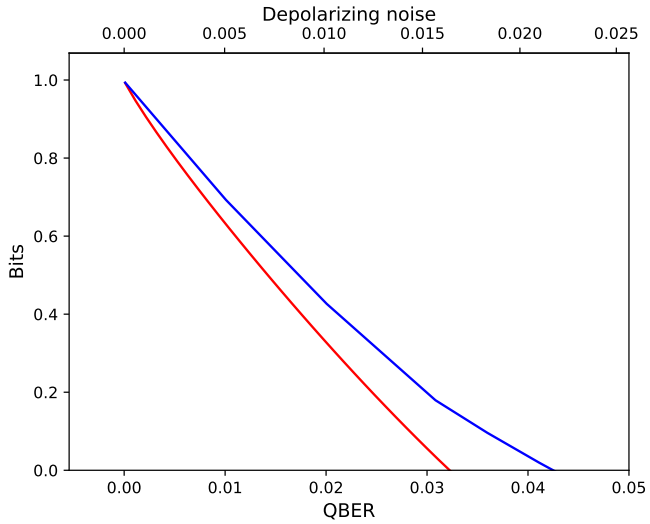


Figure 5: Comparison of Devetak-Winter rates as a function of QBER (bottom horizontal axis) and its corresponding depolarizing noise (top horizontal axis). Blue line is computed using $\max\{H_{\min}(S|XYE), H(S|X \in \{0,1,2\}, Y = 0; E)\}$ and red line is computed with $H(S|X = 0, Y = 0; E)$ and matches the key rates reported in [46] (see footnote 7).

Following the formalism from [57] we also introduce various entropies. For a subnormalized state $\rho_{AB} \in S_{\leq}(AB)$, the *min-entropy* and the *max-entropy* of A given B are

$$H_{\min}(A|B)_\rho := \max_{\substack{\sigma_B \in S_{\leq}(B): \\ \ker(\sigma_B) \subseteq \ker(\rho_B)}} -\log \left\| \left(\mathbb{I}_A \otimes \sigma_B^{-\frac{1}{2}}\right) \rho_{AB} \left(\mathbb{I}_A \otimes \sigma_B^{-\frac{1}{2}}\right) \right\|_\infty \tag{43}$$

$$H_{\max}(A|B)_\rho := \max_{\sigma_B \in S_{\leq}(B)} \log F(\rho_{AB}, \mathbb{I}_A \otimes \sigma_B). \tag{44}$$

In the case $\rho_{XE} = \sum_{x \in \mathcal{X}} p_x \, |x\rangle\langle x| \otimes \rho_E^x$ is a classical-quantum state in $S(XE)$ then

$$H_{\min}(X|E)_\rho = -\log p_{\text{guess}}(X|E)_\rho, \tag{45}$$

where $p_{\text{guess}}(X|E)_\rho := \sup_{\{M_x\}_x} \sum_x p_x \operatorname{Tr}[\rho_E^x M_x]$ is the guessing probability and the supremum is over POVMs on register E.

We also define the *smooth-min entropy* and the *smooth-max entropy* of A given B for a subnormalized state $\rho_{AB} \in S_{\leq}(AB)$ and a smoothing parameter $\varepsilon \in [0, \sqrt{\operatorname{Tr} \rho_{AB}}]$:

$$H_{\min}^\varepsilon(A|B)_\rho := \max_{\substack{\tilde{\rho}_{AB} \in S_{\leq}(AB): \\ P(\rho_{AB}, \tilde{\rho}_{AB}) \leq \varepsilon}} H_{\min}(A|B)_{\tilde{\rho}} \tag{46}$$

$$H_{\max}^\varepsilon(A|B)_\rho := \min_{\substack{\tilde{\rho}_{AB} \in S_{\leq}(AB): \\ P(\rho_{AB}, \tilde{\rho}_{AB}) \leq \varepsilon}} H_{\max}(A|B)_{\tilde{\rho}}. \tag{47}$$

The smooth min-entropy is a generalisation of the min-entropy which takes into account states that are close to ρ_{AB} in purified distance. Likewise for the smooth max-entropy. Both of these smooth entropies satisfy the following *data processing inequality* [57, Section 6.3.3]: for $\mathcal{E} \in \text{CPTP}(B, B')$ and $\tilde{\rho} = (\mathbb{I}_A \otimes \mathcal{E})(\rho_{AB})$, then

$$H_{\min}^\varepsilon(A|B)_\rho \leq H_{\min}^\varepsilon(A|B')_{\tilde{\rho}}, \qquad \text{and} \qquad H_{\max}^\varepsilon(A|B)_\rho \leq H_{\max}^\varepsilon(A|B')_{\tilde{\rho}}. \tag{48}$$

4.1.1 Min-tradeoff functions

Min-tradeoff functions bound the amount of randomness generated by a party, Alice, that is secret from an eavesdropper during any round in a protocol comprised of n measurement rounds.

Formally, let $\mathcal{M} \in \mathrm{CPTP}(RE, SCRE)$ be a quantum instrument which updates quantum registers R and E and produces classical information S, C over alphabets $\mathcal{S}, \mathcal{C}$. Let $\mathcal{P}(\mathcal{C})$ denote the set of probability distributions over alphabet $\mathcal{C}$ and let $F \cong RE$.

Definition 11 (Min-tradeoff function)**.** *A function $f : \mathcal{P}(\mathcal{C}) \to \mathbb{R}$ is a min-tradeoff function for the channel $\mathcal{M} \in \mathrm{CPTP}(RE, SCRE)$ if for any $q \in \mathcal{P}(\mathcal{C})$*

$$f(q) \leq \min_{\omega_{REF}} H(S|EF)_{\mathcal{M}(\omega_{REF})}, \tag{49}$$

where the minimum is over states $\omega_{REF} \in S(REF)$ such that $\mathrm{Tr}_{SREF}[\mathcal{M}(\omega_{REF})] = \sum_c q_c \, |c\rangle\langle c|_C$, that is over output states whose C register is distributed as $q \in \mathcal{P}(\mathcal{C})$.

Now, consider instead the sequence of channels $\{\mathcal{M}_i \in \mathrm{CPTP}(RE, S_i C_i RE)\}_{i=1}^n$ over quantum registers R, E and classical registers S_i, C_i over alphabets $\mathcal{S}, \mathcal{C}$. We say that a function $f : \mathcal{P}(\mathcal{C}) \to \mathbb{R}$ is a min-tradeoff function for the sequence $\{\mathcal{M}_i \in \mathrm{CPTP}(RE, S_i C_i RE)\}_{i=1}^n$ if f is a min-tradeoff function for each channel $\mathcal{M}_i \in \mathrm{CPTP}(RE, S_i C_i RE)$ in the sequence.

Henceforth, let f be a min-tradeoff function for a sequence of channels $\{\mathcal{M}_i \in \mathrm{CPTP}(RE, S_i C_i RE)\}$. Following the exposition from [10, Section 4], for any $q \in \mathcal{P}(\mathcal{C})$ define

$$\Sigma_i(q) := \{\mathcal{M}_i(\omega_{REF}) \mid \omega \in S(REF), \ \mathrm{Tr}_{S_i REF}[\mathcal{M}(\omega_{REF})] = \sum_{c \in \mathcal{C}} q_c \, |c\rangle\langle c|_{C_i}\} \tag{50}$$

as the set of output states of the channel $\mathcal{M}_i$ whose C_i register is distributed as q. Note that the minimisation in Definition 11 is precisely over states in $\Sigma_i(q)$. Further define $\Sigma(q) := \bigcup_i \Sigma_i(q)$. We will need the following properties of the min-tradeoff function f as defined in [9, 8, 10]:

$$\mathrm{Max}(f) := \max_{q \in \mathcal{P}(\mathcal{C})} f(q), \tag{51}$$

$$\mathrm{Min}(f) := \min_{q \in \mathcal{P}(\mathcal{C})} f(q), \tag{52}$$

$$\mathrm{Min}_\Sigma(f) := \min_{q : \Sigma(q) \neq \emptyset} f(q), \tag{53}$$

$$\mathrm{Var}(f) := \max_{q : \Sigma(q) \neq \emptyset} \sum_{x \in \mathcal{C}} q(x) f(\delta_x)^2 - \left(\sum_{x \in \mathcal{C}} q(x) f(\delta_x) \right)^2, \tag{54}$$

where δ_x is the distribution over $\mathcal{C}$ with $\Pr[C = x] = 1$.

Lastly, we will require the following result from [9, Lemma V.5].

Lemma 1. *Suppose that for each i, the channels $\mathcal{M}_i \in \mathrm{CPTP}(RE, S_i C_i RE)$ for $S_i \in \{0, 1\}$ and $C_i \in \{0, 1, \perp\}$ are of the form*

$$\mathcal{M}_i = \gamma \mathcal{M}_i^{\mathrm{test}} + (1 - \gamma) \mathcal{M}_i^{\mathrm{gen}}, \tag{55}$$

where $\gamma \in (0, 1)$ and $\mathcal{M}_i^{\mathrm{gen}}$ sets $C_i = \perp$. Further suppose that the function $g : \mathcal{P}(\{0, 1\}) \to \mathbb{R}$ is an affine function which for all $i \in \{1, ..., n\}$ and for all $[q_0, q_1] \in \mathcal{P}(\{0, 1\})$ satisfies

$$g(q) \leq \min_{\omega_{REF}} \left\{ H(S_i|EF)_{\mathcal{M}_i(\omega_{REF})} \ : \ \mathrm{Tr}_{SREF}[\mathcal{M}_i^{\mathrm{test}}(\omega_{REF})] = q_0 \, |0\rangle\langle 0|_{C_i} + q_1 \, |1\rangle\langle 1|_{C_i} \right\}. \tag{56}$$

Then the affine function defined by

$$f(\delta_0) = g(\delta_1) + \frac{1}{\gamma}(g(\delta_0) - g(\delta_1)), \qquad f(\delta_1) = f(\delta_\perp) = g(\delta_1) \tag{57}$$

is a min-tradeoff function for the sequence $\{\mathcal{M}_i \in \mathrm{CPTP}(RE, S_i C_i RE)\}_{i=1}^n$ which additionally satisfies

$$\mathrm{Max}(f) = \mathrm{Max}(g), \tag{58}$$

$$\mathrm{Min}(f) = \left(1 - \frac{1}{\gamma}\right) \mathrm{Max}(g) + \frac{1}{\gamma} \mathrm{Min}(g), \tag{59}$$

$$\mathrm{Min}_\Sigma(f) \geq \mathrm{Min}(g), \tag{60}$$

$$\mathrm{Var}(f) \leq \frac{1}{\gamma} \big(\mathrm{Max}(g) - \mathrm{Min}(g)\big)^2. \tag{61}$$

Channels of the form as in this lemma are known as *infrequent sampling channels*.

4.2 Completeness

In this section, we prove that for any $(\mathcal{D}_A^{\text{hon}}, \mathcal{D}_B^{\text{hon}}, \omega_{R_A R_B}^{\text{hon}})$ which plays the game $\mathcal{G}$ independently in every round and wins with probability ω_{exp}, the protocol $\mathcal{P}_{(\mathcal{D}_A^{\text{hon}}, \mathcal{D}_B^{\text{hon}}), (n, \mathbf{pe}, \mathbf{ec}, \mathbf{pa})}$ with parameters $\mathbf{ec} = (\text{Synd}, \text{Corr}, \mathcal{H}_{\text{EC}}, l_{\text{EC}})$ and $\mathbf{pe} = (\gamma, \omega_{\text{exp}}, \delta_{\text{tol}})$ is $\left(\epsilon_{\text{com}}^{\text{PE}} + \epsilon_{\text{com}}^{\text{EC}}\right)$-complete if

$$\Pr\left[S_A \neq \hat{S}_B\right]_{\rho^{\text{hon}}} \leq \varepsilon_{\text{com}}^{\text{EC}}, \qquad \text{where} \qquad \rho^{\text{hon}} = \mathcal{P}_{(\mathcal{D}_A^{\text{hon}}, \mathcal{D}_B^{\text{hon}}), (n, \mathbf{pe}, \mathbf{ec}, \mathbf{pa})}(\omega_{R_A R_B}^{\text{hon}}) \tag{62}$$

and if

$$\gamma \geq \frac{2(1-\omega_{\text{exp}}) + \delta_{\text{tol}}}{{\delta_{\text{tol}}}^2 n} \ln \frac{1}{\varepsilon_{\text{com}}^{\text{PE}}}. \tag{63}$$

To this end, let Ω denote the event that the protocol does not abort. We have $\Omega = \Omega_{\text{PE}} \wedge \Omega_{\text{EC}}$ where Ω_{PE} is the event $F_{\text{PE}} = \checkmark$ and Ω_{EC} is the event $F_{\text{EC}} = \checkmark$. Define the additional event

$$\Omega_{\text{g}} := \left\{S_A = \hat{S}_B\right\}, \tag{64}$$

and note $\Omega \wedge \Omega_{\text{g}} = \Omega_{\text{PE}} \wedge \Omega_{\text{EC}} \wedge \Omega_{\text{g}} = \Omega_{\text{PE}} \wedge \Omega_{\text{g}}$. The probability of abort is given by event $\Omega^c = \Omega_{\text{EC}}^c \vee \Omega_{\text{PE}}^c$, wherefore

$$\Pr[\Omega_{\text{EC}}^c \vee \Omega_{\text{PE}}^c]_{\rho^{\text{hon}}} \leq \Pr[\Omega_{\text{EC}}^c]_{\rho^{\text{hon}}} + \Pr[\Omega_{\text{PE}}^c]_{\rho^{\text{hon}}} \leq \Pr\left[\Omega_{\text{g}}^c\right]_{\rho^{\text{hon}}} + \Pr[\Omega_{\text{PE}}^c]_{\rho^{\text{hon}}}. \tag{65}$$

The first inequality follows from the union bound and the second as event Ω_{g} implies event Ω_{EC}. Informally, the term $\Pr\left[\Omega_{\text{g}}^c\right]_{\rho^{\text{hon}}}$ is the probability that the error correction in the protocol fails (not to be confused with the error correction *check* which uses hash functions and whose failure is given by event Ω_{EC}^c), and the term $\Pr[\Omega_{\text{PE}}^c]_{\rho^{\text{hon}}}$ is the probability that the parameter estimation fails. We tackle each term in Eq. (65) separately.

To bound the term $\Pr\left[\Omega_{\text{g}}^c\right]_{\rho^{\text{hon}}}$ we note that the error correction scheme aims to correct all instances $S_{A,i} \neq S_{B,i}$. In an honest implementation of the protocol, the expected number of such occurrences is $n(1-\omega_{\text{exp}})$. For n large enough [53, Theorem 1] shows that for any parameter $\varepsilon_{\text{com}}^{\text{EC}} \in (0, 1]$ independent of n, there exists an error correction scheme given by functions

$$\text{Synd} : \{0,1\}^n \to \{0,1\}^{\lambda_{\text{EC}}}, \qquad \text{Corr} : \{0,1\}^n \times \{0,1\}^{\lambda_{\text{EC}}} \to \{0,1\}^n \tag{66}$$

satisfying $\Pr[\Omega_g]_{\rho^{\text{hon}}} = \Pr[S_A = \hat{S}_B]_{\rho^{\text{hon}}} \geq 1 - \varepsilon_{\text{com}}^{\text{EC}}$ and $\frac{\lambda_{\text{EC}}}{n} = h(Q) + \Theta\left(\frac{\log n}{n}\right)$, where h is the binary entropy and $Q = 1 - \omega_{\text{exp}}$ is the quantum bit error rate.

For the remaining term $\Pr[\Omega_{\text{PE}}^c]_{\rho}$ we note that in the honest behaviour, C_i is a sequence of i.i.d variables with

$$\Pr[C_i = 0] = \gamma(1-\omega_{\text{exp}}), \qquad \Pr[C_i = 1] = \gamma\omega_{\text{exp}}, \qquad \Pr[C_i = \perp] = 1 - \gamma, \tag{67}$$

where the probabilities are over the distribution generated when the honest devices are interacted with for the i-th time. Then,

$$\Pr\left[\Omega_{\text{PE}}^c\right]_{\rho^{\text{hon}}} = \Pr\left[|\{i \ : \ C_i = 0\}| > (1 - \omega_{\text{exp}} + \delta_{\text{tol}})\gamma n\right]_{\rho^{\text{hon}}} \tag{68}$$

$$= \Pr\left[|\{i \ : \ C_i = 0\}| > \left(1 + \frac{\delta_{\text{tol}}}{1-\omega_{\text{exp}}}\right)\mathbb{E}\left[|\{i \ : \ C_i = 0\}|\right]\right]_{\rho^{\text{hon}}} \tag{69}$$

$$\leq \exp\left\{-\frac{\delta_{\text{tol}}^2}{2(1-\omega_{\text{exp}}) + \delta_{\text{tol}}}\gamma n\right\}, \tag{70}$$

where in the last inequality we used the multiplicative Chernoff bound in [58, Theorem 4.4]. Setting γ as in the statement of the theorem (Eq. (63)), we directly obtain

$$\Pr\left[\Omega_{\text{PE}}^c\right]_{\rho^{\text{hon}}} \leq \varepsilon_{\text{com}}^{\text{PE}}, \tag{71}$$

as is required to complete the proof.

4.3 Correctness

In this section we tackle the correctness as per Theorem 2, which states that for any triple $(\mathcal{D}_A, \mathcal{D}_B, \omega^0_{R_A R_B E})$, the state $\rho = \mathcal{P}_{(\mathcal{D}_A,\mathcal{D}_B),(n,\mathbf{pe},\mathbf{ec},\mathbf{pa})}(\omega^0_{R_A R_B E})$ with error correction tuple $\mathbf{ec} = (\mathrm{Synd}, \mathrm{Corr}, \mathcal{H}_{\mathrm{EC}}, l_{\mathrm{EC}})$ is such that $\Pr[K_A \neq K_B \wedge \Omega_{\mathrm{PE}} \wedge \Omega_{\mathrm{EC}}]_\rho \leq \varepsilon_{\mathrm{corr}}$ if $l_{\mathrm{EC}} \geq \log \frac{1}{\varepsilon_{\mathrm{corr}}}$, for some $\varepsilon_{\mathrm{corr}} \in (0, 1]$.

The proof is analogous to that of [6], but we present it here for completeness. As with before, let $\Omega = \Omega_{\mathrm{PE}} \wedge \Omega_{\mathrm{EC}}$ denote the event that the protocol does not abort. Indeed:

$$\begin{aligned}
\Pr\left[K_A \neq K_B \wedge \Omega_{\mathrm{PE}} \wedge \Omega_{\mathrm{EC}}\right]_\rho &\leq \Pr\left[K_A \neq K_B \wedge \Omega_{\mathrm{EC}}\right]_\rho && (72)\\
&= \Pr\left[H_{\mathrm{PA}}(S_A) \neq H_{\mathrm{PA}}(\hat{S}_B) \wedge H_{\mathrm{EC}}(S_A) = H_{\mathrm{EC}}(\hat{S}_B)\right]_\rho && (73)\\
&\leq \Pr\left[S_A \neq \hat{S}_B \wedge H_{\mathrm{EC}}(S_A) = H_{\mathrm{EC}}(\hat{S}_B)\right]_\sigma && (74)\\
&= \Pr\left[S_A \neq \hat{S}_B\right]_\sigma \cdot \Pr\left[H_{\mathrm{EC}}(S_A) = H_{\mathrm{EC}}(\hat{S}_B) \mid S_A \neq \hat{S}_B\right]_\sigma && (75)\\
&\leq \Pr\left[H_{\mathrm{EC}}(S_A) = H_{\mathrm{EC}}(\hat{S}_B) \mid S_A \neq \hat{S}_B\right]_\sigma && (76)\\
&\leq \frac{1}{2^{l_{\mathrm{EC}}}}. && (77)
\end{aligned}$$

In the above, the first inequality follows from the union bound, the second inequality follows from the fact that $H_{\mathrm{PA}}(S_A) \neq H_{\mathrm{PA}}(\hat{S}_B)$ implies $S_A \neq \hat{S}_B$ and the last inequality is the defining property of 2-universal hashing. Choosing $l_{\mathrm{EC}} \geq \log \frac{1}{\varepsilon_{\mathrm{corr}}}$ completes the proof.

4.4 Secrecy

Finally, we prove Theorem 3 through the use of the Leftover Hashing Lemma and the generalised entropy accumulation theorem. Given $n \in \mathbb{N}$ and $\varepsilon_{\mathrm{sec}} \in (0, 1]$, we want to show that for any triple $(\mathcal{D}_A, \mathcal{D}_B, \omega^0_{R_A R_B Q_E})$, protocol $\mathcal{P}_{(\mathcal{D}_A,\mathcal{D}_B),(n,\mathbf{pe},\mathbf{ec},\mathbf{pa})}$ with $\mathbf{pe} = (\gamma, \omega_{\mathrm{exp}}, \delta_{\mathrm{tol}})$, $\mathbf{ec} = (\mathrm{Synd}, \mathrm{Corr}, \mathcal{H}_{\mathrm{EC}}, l_{\mathrm{EC}})$ and $\mathbf{pa} = (\mathcal{H}_{\mathrm{PA}}, l_{\mathrm{key}})$ is $\varepsilon_{\mathrm{sec}}$-secret if

$$\begin{aligned}
l_{\mathrm{key}} \leq\ & n g(\omega_{\mathrm{exp}} - \delta_{\mathrm{tol}}) - d_1\sqrt{n} - d_0 - (2 - \omega_{\mathrm{exp}} + \delta_{\mathrm{tol}}) n(\gamma + \kappa) - 2\vartheta\left(\frac{\varepsilon_s}{4}\right) && (78)\\
& - l_{\mathrm{EC}} - \lambda_{\mathrm{EC}} - 2\log\frac{1}{\varepsilon_{\mathrm{sec}} - 2\varepsilon_s}, && (79)
\end{aligned}$$

where $\varepsilon_s \in \left(0, \frac{1}{2}\varepsilon_{\mathrm{sec}}\right)$ is a variable to be optimised, $\kappa \geq \frac{1}{\sqrt{n}}\sqrt{\ln 8 - \ln \varepsilon_s}$, $g : [0, 1] \to \mathbb{R}$ is the affine function defined by

$$g(p) := \frac{p - \beta}{\ln 2 \cdot (1 - \beta + \omega_3)} - \log\left(1 - \beta + \omega_3\right), \tag{80}$$

for $\beta \in [\omega_3, \omega_2]$ to be optimised. Further, the coefficients d_1, d_0 depend only on $\varepsilon_{\mathrm{sec}}$, ε_s and β and are respectively as in Eqs. (161) and (162). Lastly, $\vartheta(\delta) = -\log\left(1 - \sqrt{1 - \delta^2}\right)$.

To prove this, we fix parameters $\mathbf{pe}, \mathbf{ec}, \mathbf{pa}$ and consider a different protocol $\widetilde{\mathcal{P}}$ initialised with devices $\widetilde{\mathcal{D}}_A, \widetilde{\mathcal{D}}_B$ and state $\widetilde{\omega}^0_{R_A R_B Q_E} \in S(R_A R_B Q_E)$. Protocol $\widetilde{\mathcal{P}}$ is presented in algorithm 2 and differs from the original protocol $\mathcal{P}$ in algorithm 1 only in the measurement stage and in the parameter estimation stage (error correction and privacy amplification proceed identically in either protocol). Additionally, protocol $\widetilde{\mathcal{P}}$ maintains the register $\bar{S}_B$, which is only used later in the proof to bound a smooth max-entropy term. Crucially, we remark that Eve never has access to $\bar{S}_B$.

It is straightforward to see that

$$\mathcal{P}_{(\mathcal{D}_A,\mathcal{D}_B),(n,\mathbf{pe},\mathbf{ec},\mathbf{pa})}(\omega^0_{R_A R_B Q_E}) = \mathrm{Tr}_{\bar{S}_B} \circ \widetilde{\mathcal{P}}_{(\widetilde{\mathcal{D}}_A,\widetilde{\mathcal{D}}_B),(n,\mathbf{pe},\mathbf{ec},\mathbf{pa})}(\widetilde{\omega}^0_{R_A R_B Q_E}) \tag{81}$$

whenever $\widetilde{\omega}^0_{R_A R_B Q_E} = \omega^0_{R_A R_B Q_E}$ and the device's quantum instruments through an instance of $\mathcal{P}$ and $\widetilde{\mathcal{P}}$ are identical. Further, since in protocol $\widetilde{\mathcal{P}}$ the eavesdropper has access to the additional information in registers $X_1^i Y_1^i T_1^i$ prior to the i-th interaction with the devices, secrecy of protocol $\widetilde{\mathcal{P}}_{(\mathcal{D}_A,\mathcal{D}_B),(n,\mathbf{pe},\mathbf{ec},\mathbf{pa})}$ with parameters $(\mathbf{pe}, \mathbf{ec}, \mathbf{pa})$ implies secrecy of $\mathcal{P}_{(\mathcal{D}_A,\mathcal{D}_B),(n,\mathbf{pe},\mathbf{ec},\mathbf{pa})}$ with identical parameters. Therefore, without loss of generality we prove secrecy of protocol $\widetilde{\mathcal{P}}$ instantiated with $(\mathcal{D}_A, \mathcal{D}_B, \omega^0_{R_A R_B Q_E})$.

Algorithm 2: A virtual protocol for DIQKD from non-local games: $\widetilde{\mathcal{P}}$

Input : Devices $\mathcal{D}_A, \mathcal{D}_B$
Parameters : Number of rounds n
PE parameters, $\mathbf{pe} = (\gamma, \omega_{\text{exp}}, \delta_{\text{tol}})$
EC parameters, $\mathbf{ec} = (\text{Synd}, \text{Corr}, \mathcal{H}_{\text{EC}}, l_{\text{EC}})$
PA parameters, $\mathbf{pa} = (\mathcal{H}_{\text{PA}}, l_{\text{key}})$

1. Measurement;
for $i = 1$ *to* n **do**
  Bob chooses and announces $T_i \in \{0, 1\}$ with $\Pr[T_i = 1] = \gamma$;
  Alice chooses and announces $X_i \in \mathcal{X}$ and inputs it to $\mathcal{D}_A$ to receive $A_i \in \mathcal{A}$;
  Bob chooses and announces $Y_i \in \mathcal{Y}$ and inputs it to $\mathcal{D}_B$ to receive $B_i \in \mathcal{B}$;
  Alice sets $S_{A,i} = SK_A(X_i, Y_i, A_i)$;
  Bob sets $S_{B,i} = SK_B(X_i, Y_i, A_i)$;
end
if $T_i = 0$ **then**
  Bob sets $C_i = \perp$ and $\bar{S}_{B,i} = 0$;
else
  Alice announces A_i;
  Bob sets $C_i = V(X_i, Y_i, A_i, X_i)$ and $\bar{S}_{B,i} = S_{B,i}$;
end
2. Parameter Estimation;
if $|\{i \,:\, C_i = 0\}| \leq (1 - \omega_{\text{exp}} + \delta_{\text{tol}}) \cdot \gamma n$ **then**
  Bob announces $F_{\text{PE}} = \checkmark$;
else
  Bob announces $F_{\text{PE}} = \times$, both parties output $K_A = K_B = |\perp\rangle\langle\perp|$;
end
3. Error Correction;
4. Privacy Amplification;

We begin by recollecting some notation:

$$\Omega_{\mathrm{PE}} := \{|\{i \,:\, C_i = 0\}| \leq (1 - \omega_{\mathrm{exp}} + \delta_{\mathrm{tol}}) \cdot \gamma n\}, \tag{82}$$

$$\Omega_{\mathrm{EC}} := \{H_{\mathrm{EC}}(S_A) = H_{\mathrm{EC}}(\hat{S}_B)\}, \tag{83}$$

are the events that the parameter estimation test passes and that the error correction test passes, such that $\Omega = \Omega_{\mathrm{PE}} \wedge \Omega_{\mathrm{EC}}$ is the event that the protocol does not abort. Let

$$\widetilde{\mathcal{P}}_{(\mathcal{D}_A,\mathcal{D}_B),(n,\mathbf{pe},\mathbf{ec},\mathbf{pa})}(\omega^0_{R_A R_B Q_E}) = \rho_{A_1^n B_1^n K_A K_B S_A S_B \hat{S}_B \bar{S}_B C_1^n E} \tag{84}$$

be the state output by the protocol, where Eve's total side information is

$$E = X_1^n Y_1^n T_1^n S_{A,T_{\mathrm{test}}} H_A Z F_{\mathrm{PE}} F_{\mathrm{EC}} Q_E. \tag{85}$$

Lastly, let $\sigma_{A_1^n B_1^n S_A S_B \hat{S}_B \bar{S}_B C_1^n E}$ be the state prior to the privacy amplification phase.

We start the proof by noting that if $\Pr[\Omega_{\mathrm{EC}}|\Omega_{\mathrm{PE}}] < \varepsilon_s^2$ or if $\Pr[\Omega_{\mathrm{PE}}] < \varepsilon_a$ for some $\varepsilon_a \in \left(0, \frac{1}{2}\varepsilon_{\mathrm{sec}}\right]$, $\varepsilon_s \in (0, \frac{1}{2}\varepsilon_{\mathrm{sec}})$, we have that

$$\Pr[\Omega_{\mathrm{PE}} \wedge \Omega_{\mathrm{EC}}]_\rho \leq \min\left\{ \Pr[\Omega_{\mathrm{EC}}|\Omega_{\mathrm{PE}}]_\rho, \Pr[\Omega_{\mathrm{PE}}]_\rho \right\} \leq \max\left\{\varepsilon_s^2, \varepsilon_a\right\} \tag{86}$$

which implies

$$\begin{aligned} \|\rho_{K_A E \wedge \Omega_{\mathrm{PE}} \wedge \Omega_{\mathrm{EC}}} - \tau_{K_A} \otimes \rho_{E \wedge \Omega_{\mathrm{PE}} \wedge \Omega_{\mathrm{EC}}}\|_{\mathrm{Tr}} &\leq \|\rho_{K_A E \wedge \Omega_{\mathrm{PE}} \wedge \Omega_{\mathrm{EC}}}\|_{\mathrm{Tr}} + \|\tau_{K_A} \otimes \rho_{E \wedge \Omega_{\mathrm{PE}} \wedge \Omega_{\mathrm{EC}}}\|_{\mathrm{Tr}} && (87) \\ &= 2 \Pr[\Omega_{\mathrm{PE}} \wedge \Omega_{\mathrm{EC}}]_\rho && (88) \end{aligned}$$

and so secrecy is given directly by $2\max\{\varepsilon_s^2, \varepsilon_a\} \leq 2\max\{\varepsilon_s, \varepsilon_a\} \leq \varepsilon_{\mathrm{sec}}$.

Therefore, from now on we assume $\Pr[\Omega_{\mathrm{EC}}|\Omega_{\mathrm{PE}}]_\rho \geq \varepsilon_s^2$ and $\Pr[\Omega_{\mathrm{PE}}]_\rho \geq \varepsilon_a$ such that

$$\|\rho_{K_A E \wedge \Omega_{\mathrm{PE}} \wedge \Omega_{\mathrm{EC}}} - \tau_{K_A} \otimes \rho_{E \wedge \Omega_{\mathrm{PE}} \wedge \Omega_{\mathrm{EC}}}\|_{\mathrm{Tr}} = \Pr[\Omega_{\mathrm{PE}}]_\rho \left\|\rho_{K_A E|\Omega_{\mathrm{PE}} \wedge \Omega_{\mathrm{EC}}} - \tau_{K_A} \otimes \rho_{E|\Omega_{\mathrm{PE}} \wedge \Omega_{\mathrm{EC}}}\right\|_{\mathrm{Tr}}. \tag{89}$$

To bound the trace distance on the right, we use the following result from [6, Proposition 9]:

Lemma 2 (Leftover Hashing)**.** *Let $\sigma \in S_{\leq}(S_1^n E)$ be classical-quantum and let $\mathcal{H} := \left\{H : \{0,1\}^n \to \{0,1\}^l\right\}$ be a family of 2-universal functions. Further let*

$$\rho_{K_1^l S_1^n E} := \mathcal{E}_{\mathcal{H}}(\sigma_{S_1^n E} \otimes \tau_H), \tag{90}$$

where τ_H is the maximally mixed state of dimension $|\mathcal{H}|$. The CPTP map $\mathcal{E}_{\mathcal{H}}$ chooses a hash function from register H, applies it to the classical string in registers S_1^n and stores the hash in registers K_1^l.

Then, for any $\varepsilon \in \left[0, \sqrt{\mathrm{Tr}\left[\sigma_{S_1^n E}\right]}\right]$:

$$\left\|\rho_{K_1^l E H} - \tau_{K_1^l} \otimes \rho_{EH}\right\|_{\mathrm{Tr}} \leq \frac{1}{2} 2^{-\frac{1}{2}(H_{\min}^{\varepsilon}(S_1^n|E)_\sigma - l)} + 2\varepsilon, \tag{91}$$

where $\tau_{K_1^l}$ is the maximally mixed state of dimension 2^l.

Intuitively, the Leftover Hashing Lemma guarantees that the key K_A output by Alice in protocol $\mathcal{P}$ (algorithm 1) is close to a perfect key provided the smooth min-entropy of the sifted key S_A conditioned on Eve's side information E is large enough. Continuing from Eq. (89), the Leftover Hashing Lemma implies

$$\left\|\rho_{K_A E|\Omega_{\mathrm{PE}} \wedge \Omega_{\mathrm{EC}}} - \tau_{K_A} \otimes \rho_{E|\Omega_{\mathrm{PE}} \wedge \Omega_{\mathrm{EC}}}\right\|_{\mathrm{Tr}} \leq \frac{1}{2} \cdot 2^{-\frac{1}{2}\left(H_{\min}^{\varepsilon_s}(S_A|E)_{\sigma_{|\Omega_{\mathrm{PE}} \wedge \Omega_{\mathrm{EC}}}} - l_{\mathrm{key}}\right)} + 2\varepsilon_s. \tag{92}$$

The smooth min-entropy term in the exponent is further bounded by

$$\begin{aligned} H_{\min}^{\varepsilon_s}(S_A|E)_{\sigma_{|\Omega_{\mathrm{PE}} \wedge \Omega_{\mathrm{EC}}}} &\geq H_{\min}^{\varepsilon_s}(S_A|E)_{\sigma_{|\Omega_{\mathrm{PE}}}} && (93) \\ &\geq H_{\min}^{\varepsilon_s}(S_A|X_1^n Y_1^n T_1^n S_{A,T_{\mathrm{test}}} Q_E)_{\sigma_{|\Omega_{\mathrm{PE}}}} - l_{\mathrm{EC}} - \lambda_{\mathrm{EC}} - 2. && (94) \end{aligned}$$

The first inequality follows from [6, Lemma 10] and for the second inequality we used the chain rule in [57, Lemma 6.8] to remove the error correction and flag registers $H_A Z F_{\mathrm{PE}} F_{\mathrm{EC}}$ from Eve's side information.

All that remains is to bound $H_{\min}^{\varepsilon_s}(S_A|X_1^n Y_1^n T_1^n S_{A,T_{\mathrm{test}}} Q_E)_{\sigma_{|\Omega_{\mathrm{PE}}}}$. However, there are two last technical hurdles we need to address. Firstly, the conditioning event $|\Omega_{\mathrm{PE}}$ imposes a condition on the registers C_i which are themselves computed from the registers $S_{A,i}S_{B,i}T_i$. We need to ensure that all these registers are included in the smooth-min entropy term to bound. The conditioning side already includes $X_1^n Y_1^n T_1^n S_{A,T_{\mathrm{test}}}$ so it remains to add the classical registers $S_{B,T_{\mathrm{test}}} = \{S_{B,i} : i \in T_{\mathrm{test}}\}$ for $T_{\mathrm{test}} = \{i : T_i = 1\}$ which are not publicly announced in $\widetilde{\mathcal{P}}$. Secondly, the classical register $S_{A,T_{\mathrm{test}}}$ which is available to the eavesdropper needs to be removed from the conditioning side of the smooth min-entropy. This is to ensure Alice's outcome A_i on round i does not depend on her previous announced outcomes, which would violate the no-signalling assumption of our protocol.

With this in mind, let $\bar{S}_B$ be such that $\bar{S}_{B,T_{\mathrm{test}}} = S_{B,T_{\mathrm{test}}}$ and all other elements are set deterministically to 0. Letting $\bar{E}_n = X_1^n Y_1^n T_1^n Q_E$, we have that for $\varepsilon_s' \in \left[0, \frac{1}{2}\varepsilon_{\mathrm{sec}}\right)$ and $\varepsilon_s'' \in \left[0, \frac{1}{4}\varepsilon_{\mathrm{sec}}\right)$ such that $\delta = \varepsilon_s - \varepsilon_s' - 2\varepsilon_s'' > 0$:

$$
\begin{aligned}
H_{\min}^{\varepsilon_s}(S_A|S_{A,T_{\mathrm{test}}}\bar{E}_n)_{\sigma_{|\Omega_{\mathrm{PE}}}} &\geq H_{\min}^{\varepsilon_s}(S_A|S_{A,T_{\mathrm{test}}}\bar{S}_B\bar{E}_n)_{\sigma_{|\Omega_{\mathrm{PE}}}} && (95)\\
&\geq H_{\min}^{\varepsilon_s'}(S_A\bar{S}_B|\bar{E}_n)_{\sigma_{|\Omega_{\mathrm{PE}}}} - H_{\max}^{\varepsilon_s''}(S_{A,T_{\mathrm{test}}}\bar{S}_B|\bar{E}_n)_{\sigma_{|\Omega_{\mathrm{PE}}}} - 2\vartheta(\delta) && (96)\\
&\geq H_{\min}^{\varepsilon_s'}(S_A\bar{S}_B|\bar{E}_n)_{\sigma_{|\Omega_{\mathrm{PE}}}} - H_{\max}^{\varepsilon_s''}(S_{A,T_{\mathrm{test}}}\bar{S}_B|T_1^n)_{\sigma_{|\Omega_{\mathrm{PE}}}} - 2\vartheta(\delta), && (97)
\end{aligned}
$$

where the first and last inequalities follow from the data processing inequality of the smooth min/max-entropy, and in the second inequality we used Eq. (6.60) in [57, Lemma 6.16] as well as the fact that $H_{\min}(AB) \geq H_{\min}(A)$ when A and B are classical to remove the additional $S_{A,T_{\mathrm{test}}}$ on the left of the min-entropy term. The function $\vartheta(\delta) = -\log\left(1 - \sqrt{1-\delta^2}\right)$.

We now want to bound the smooth max-entropy term in the right hand side of Eq. (97). In general, the max-entropy $H_{\max}(X|B)_\rho$ of a classical-quantum state $\rho \in S(XB)$ is upper bounded by the logarithm of the support of ρ_X. However, in our case it is not clear what the support of $S_{A,T_{\mathrm{test}}}\bar{S}_B$ on $\sigma_{|\Omega_{\mathrm{PE}}}$ is, since it depends on the values of the Bernoulli variables T_i. Indeed, when conditioned on Ω_{PE}, we expect $S_{A,T_{\mathrm{test}}}$ and $\bar{S}_{B,T_{\mathrm{test}}}$ to equal in all places except with probability $(1 - \omega_{\mathrm{exp}} + \delta_{\mathrm{tol}})$. This implies that the expected size (over the random variable T_i with $\Pr[T_i = 1] = \gamma$) of $\log \mathrm{supp}\left(\sigma_{S_{A,T_{\mathrm{test}}}\bar{S}_B|\Omega_{\mathrm{PE}}}\right)$ is $(2 - \omega_{\mathrm{exp}} + \delta_{\mathrm{tol}})n\gamma$. Thus, for a small parameter κ, we want to replace the state $\sigma_{|\Omega_{\mathrm{PE}}} \in S_{\leq}(S_{A,T_{\mathrm{test}}}\bar{S}_B T_1^n)$ in which $\log \mathrm{supp}\left(\sigma_{S_{A,T_{\mathrm{test}}}\bar{S}_B|\Omega_{\mathrm{PE}}}\right)$ does not exceed $(2 - \omega_{\mathrm{exp}} + \delta_{\mathrm{tol}})n(\gamma + \kappa)$ except with small probability (certified by some tail bound), with a state $\tilde{\sigma} \in S_{\leq}(S_{A,T_{\mathrm{test}}}\bar{S}_B T_1^n)$ in which $\log \mathrm{supp}\left(\tilde{\sigma}_{S_{A,T_{\mathrm{test}}}\bar{S}_B}\right)$ never exceeds $(2 - \omega_{\mathrm{exp}} + \delta_{\mathrm{tol}})n(\gamma + \kappa)$. This will subsequently allow us to bound the smooth max-entropy term with the logarithm of the support of $\tilde{\sigma}_{S_A\bar{S}_B}$. Formally:

Lemma 3. *Let $n, T_1^n, S_{A,T_{\mathrm{test}}}, \bar{S}_B, \Omega_{\mathrm{PE}}$ and $\sigma_{|\Omega_{\mathrm{PE}}} \in S(T_1^n S_{A,T_{\mathrm{test}}}\bar{S}_B)$ be as above. Further let $\varepsilon_s'' \in (0, 1]$. Then, for any $\kappa \geq \frac{1}{\sqrt{n}}\sqrt{-\ln \varepsilon_s''}$ it holds that*

$$
H_{\max}^{\varepsilon_s''}(S_{A,T_{\mathrm{test}}}\bar{S}_B|T_1^n)_{\sigma_{|\Omega_{\mathrm{PE}}}} \leq (2 - \omega_{\mathrm{exp}} + \delta_{\mathrm{tol}})n(\gamma + \kappa). \tag{98}
$$

Proof. For κ as in the statement of the lemma, define the event

$$
\Omega_{T,\kappa} := \left\{|\{i \ : \ T_i = 1\}| \geq n(\gamma + \kappa)\right\}. \tag{99}
$$

Hoeffding's inequality implies

$$
\varepsilon := \Pr\left[\Omega_{T,\kappa}^c\right]_{\sigma_{|\Omega_{\mathrm{PE}}}} \leq \mathrm{e}^{-2n\kappa^2}. \tag{100}
$$

Since $\kappa \geq \frac{1}{\sqrt{n}}\sqrt{-\ln \varepsilon_s''}$ and $\mathrm{Tr}\left[\sigma_{|\Omega_{\mathrm{PE}}}\right] = 1$ we have that

$$
\mathrm{e}^{-2n\kappa^2} \leq (\varepsilon_s'')^2 \leq \mathrm{Tr}\left[\sigma_{|\Omega_{\mathrm{PE}}}\right]. \tag{101}
$$

Hence, Lemma 7 in [6] implies that the state $\tilde{\sigma} \in S_{\leq}(S_{A,T_{\mathrm{test}}}\bar{S}_B T_1^n)$ defined by

$$
\tilde{\sigma} := \frac{\sin^2 \phi}{1 - \varepsilon}\sigma_{|\Omega_{\mathrm{PE}} \wedge \Omega_{T,\kappa}^c} \tag{102}
$$

for some normalization factor $\phi \in [0, \frac{\pi}{2}]$, satisfies

$$\Pr\left[\Omega_{T,\kappa}\right]_{\tilde{\sigma}} = 0 \qquad \text{and} \qquad P(\sigma_{|\Omega_{\mathrm{PE}}}, \tilde{\sigma}) \leq \sqrt{\varepsilon} \leq \mathrm{e}^{-n\kappa^2}. \tag{103}$$

Using the definition of the smooth max-entropy together with the fact that $P(\sigma_{|\Omega_{\mathrm{PE}}}, \tilde{\sigma}) \leq \mathrm{e}^{-n\kappa^2} \leq \varepsilon_s''$ we have that

$$H_{\max}^{\varepsilon_s''}(S_{A,T_{\mathrm{test}}}\bar{S}_B|T_1^n)_{\sigma_{|\Omega_{\mathrm{PE}}}} \leq H_{\max}(S_{A,T_{\mathrm{test}}}\bar{S}_B|T_1^n)_{\tilde{\sigma}}. \tag{104}$$

Finally, re-writing $\tilde{\sigma} = \sum_{t_1^n \in \Omega^c_{T,\kappa}} \Pr[T_1^n = t_1^n]\, |t_1^n\rangle\langle t_1^n| \otimes \tilde{\sigma}_{|t_1^n}$ and using the expression for the max-entropy conditioned on a classical variable given in [57, Eq. (6.26)], the following holds

$$H_{\max}(S_{A,T_{\mathrm{test}}}\bar{S}_B|T_1^n)_{\tilde{\sigma}} = \log\left[\sum_{t_1^n \in \Omega^c_{T,\kappa}} \Pr[T_1^n = t_1^n] \cdot 2^{H_{\max}(S_{A,T_{\mathrm{test}}}\bar{S}_B)_{\tilde{\sigma}_{|t_1^n}}}\right] \tag{105}$$

$$\leq (2 - \omega_{\exp} + \delta_{\mathrm{tol}})n(\gamma + \kappa), \tag{106}$$

where in the last inequality we bounded the max entropy with an upper bound on $\log \mathrm{supp}(\tilde{\sigma}_{S_{A,T_{\mathrm{test}}}\bar{S}_B|t_1^n})$, noting that $\log \mathrm{supp}(\tilde{\sigma}_{S_{A,T_{\mathrm{test}}}|t_1^n}) \leq n(\gamma+\kappa)$ and that Ω_{PE} implies that $S_{A,T_{\mathrm{test}}}$ does not match $\bar{S}_{B,T_{\mathrm{test}}}$ in at most $(1 - \omega_{\exp} + \delta_{\mathrm{tol}})n\gamma \leq (1 - \omega_{\exp} + \delta_{\mathrm{tol}})n(\gamma+\kappa)$ places. □

Applying the bound from Lemma 3 to Eq. (97) gives

$$H_{\min}^{\varepsilon_s}(S_A|S_{A,T_{\mathrm{test}}}\bar{E})_{\sigma_{|\Omega_{\mathrm{PE}}}} \geq H_{\min}^{\varepsilon_s'}(S_A\bar{S}_B|\bar{E})_{\sigma_{|\Omega_{\mathrm{PE}}}} - (2 - \omega_{\exp} + \delta_{\mathrm{tol}})n(\gamma+\kappa) - 2\vartheta(\delta), \tag{107}$$

where $\delta = \varepsilon_s - \varepsilon_s' - 2\varepsilon_s'' > 0$.

All that remains is to bound the smooth min-entropy $H_{\min}^{\varepsilon_s'}(S_A\bar{S}_B|\bar{E}_n)_{\sigma_{|\Omega_{\mathrm{PE}}}}$, where $\bar{E}_n = X_1^n Y_1^n T_1^n Q_E$ contains only Eve's quantum information and the classical registers contained in the state at termination of protocol $\widetilde{\mathcal{P}}$. This is done via the Generalised Entropy Accumulation Theorem (GEAT) [10, 23], which roughly speaking bounds the smooth min-entropy with a sum over the von Neumann entropies of each round of the virtual protocol $\widetilde{\mathcal{P}}$, which are themselves bounded using the min-tradeoff functions introduced in Section 4.4.2.

We split the application of the GEAT over the remaining subsections

4.4.1 GEAT channels

Consider the sequence of CPTP maps $\{\mathcal{N}_i : R\bar{E}_{i-1} \to S_{A,i}\bar{S}_{B,i}C_iR\bar{E}_i\}_{i=1}^n$ where $S_{A,i}$ is Alice's sifted key bit in the i-th round, $R = R_AR_B$ denotes the internal register of Alice's and Bob's devices and $\bar{E}_i = X_1^iY_1^iT_1^iQ_E$ is Eve's side information in round i. The maps $\mathcal{N}_i$ receives as input the state $\omega_{R\bar{E}_{i-1}}^{i-1}$ and proceed as follows:

1. Generate X_i, Y_i, T_i as in protocol $\widetilde{\mathcal{P}}$. The resultant state is $\omega_{RX_iY_iT_i\bar{E}_{i-1}}^{i-1}$.

2. Apply map

$$\omega_{RX_iY_i}^{i-1} \mapsto \widetilde{\omega}_{RX_iY_iA_iB_i}^{i} := \sum_{x\in\mathcal{X}}\sum_{y\in\mathcal{Y}} (P_i^{xy} \otimes \mathcal{M}_A^x \otimes \mathcal{M}_B^y)(\omega_{RX_iY_i}^{i-1}), \tag{108}$$

where

$$P_i^{xy}(\cdot) = |xy\rangle\langle xy|_{X_iY_i}(\cdot)|xy\rangle\langle xy|_{X_iY_i}, \tag{109}$$

$$\mathcal{M}_A^x(\cdot) = \sum_{a\in\mathcal{A}} |a\rangle\langle a|_{A_i} \otimes \mathcal{M}_A^{a|x}(\cdot), \tag{110}$$

$$\mathcal{M}_B^y(\cdot) = \sum_{b\in\mathcal{B}} |b\rangle\langle b|_{B_i} \otimes \mathcal{M}_B^{b|y}(\cdot), \tag{111}$$

for $\mathcal{M}_A^{a|x} \in \mathrm{CP}(R_A, R_AA_i)$ and $\mathcal{M}_B^{b|y} \in \mathrm{CP}(R_B, R_BB_i)$ trace non increasing maps satisfying $\sum_a \mathrm{Tr}\left[\mathcal{M}_A^{a|x}(\omega_{R_A})\right] = 1$ and $\sum_b \mathrm{Tr}\left[\mathcal{M}_B^{b|y}(\omega_{R_B})\right] = 1$ for all $\omega_{R_A} \in S(R_A)$, $\omega_{R_B} \in S(R_B)$ and for all $x \in \mathcal{X}$, $y \in \mathcal{Y}$.

3. Apply map

$$\widetilde{\omega}^i_{X_iY_iT_iA_iB_i} \mapsto \sum_{x,y,a,b} \Big(Q_i^{xyab} \otimes [SK_A(x,y,a)]_{S_{A,i}} \otimes \big(P_i^{t=0} \otimes [0]_{\bar{S}_{B,i}} \otimes [\perp]_{C_i} + \tag{112}$$

$$P_i^{t=1} \otimes [SK_B(x,y,b)]_{\bar{S}_{B,i}} \otimes [V(x,y,a,b)]_{C_i} \big) \Big) (\widetilde{\omega}^i_{X_iY_iT_iA_iB_i}), \tag{113}$$

whose output we label $\omega^i_{X_iY_iS_{A,i}\bar{S}_{B,i}C_i}$. In the above, we use $[\cdot]$ as shorthand for $|\cdot\rangle\langle\cdot|$, recall $V(x,y,a,b)$ is the predicate of the game $\mathcal{G}$, and

$$Q_i^{xyab}(\cdot) = |xy\rangle\langle xy|_{X_iY_i} \otimes \mathrm{Tr}\big[|xyab\rangle\langle xyab|_{X_iY_iA_iB_i}(\cdot)\big], \tag{114}$$

$$P_i^t(\cdot) = |t\rangle\langle t|_{T_i}(\cdot)\,|t\rangle\langle t|_{T_i}. \tag{115}$$

4. Apply eavesdropper's attack

$$\mathcal{E} : \omega^i_{X_iY_iT_i\bar{E}_{i-1}} \mapsto \omega^i_{\bar{E}_i}. \tag{116}$$

Without loss of generality, this attack simply passes all of Eve's available information onto the next round of the protocol. Otherwise, the data processing inequality for the smooth min-entropy guarantees that Eve's available information decreases.

We notice that the sum over operations P_i^t for $t \in \{0,1\}$ on the right hand side of Eq. (112) induces the following *infrequent sampling channel* form on each $\mathcal{N}_i$

$$\mathcal{N}_i = \gamma\mathcal{N}_i^{\text{test}} + (1-\gamma)\mathcal{N}_i^{\text{gen}}. \tag{117}$$

The channel $\mathcal{N}_i^{\text{gen}} \in \text{CPTP}(R\bar{E}_{i-1}, S_{A,i}\bar{S}_{B,i}C_iR\bar{E}_i)$ sets register C_i to $\perp$ and register $\bar{S}_{B,i}$ to 0, whereas the channel $\mathcal{N}_i^{\text{test}} \in \text{CPTP}(R\bar{E}_{i-1}, S_{A,i}\bar{S}_{B,i}C_iR\bar{E}_i)$ sets $\bar{S}_{B,i}$ to Bob's sifted key bit and C_i to the predicate of the game $\mathcal{G}$.

The sequence of channels $\{\mathcal{N}_i \in \text{CPTP}(R\bar{E}_{i-1}, S_{A,i}\bar{S}_{B,i}C_iR\bar{E}_i)\}_{i=1}^n$ is no-signalling in the sense that Eve's operations are unable to act on the registers R_AR_B in the devices of Alice and Bob. Formally, the channel $\mathcal{R}_i \in \text{CPTP}(\bar{E}_{i-1}, \bar{E}_i)$ which samples X_i, Y_i and T_i and subsequently updates $\bar{E}_{i-1}$ as in steps 1 and 4 of the map $\mathcal{N}_i$ above, trivially satisfies

$$\mathrm{Tr}_{S_{A,i}\bar{S}_{B,I}C_iR} \circ \mathcal{N}_i = \mathcal{R}_i \circ \mathrm{Tr}_R. \tag{118}$$

4.4.2 Min-tradeoff function and GEAT

Now, let $g : \mathcal{P}(\{0,1\}) \to \mathbb{R}$ be an arbitrary affine function satisfying

$$g(q) \leq \min_{\omega_{R\bar{E}_{i-1}F}} \big\{ H(S_{A,i}|\bar{E}_{i-1}F)_{\mathcal{N}_i(\omega_{R\bar{E}_{i-1}F})} \,:\, \mathrm{Tr}_{S_{A,i}R\bar{E}_iF}[\mathcal{N}_i^{\text{test}}(\omega_{R\bar{E}_{i-1}F})] = q_0\,|0\rangle\langle 0| + q_1\,|1\rangle\langle 1| \big\}, \tag{119}$$

for all $i \in \{1,...,n\}$ and all $[q_0,q_1] \in \mathcal{P}(\{0,1\})$, as well as $\text{Max}(g) = g(\delta_1)$[8]. Proceeding as in [9, 10, 23], Lemma 1 implies that the function $f : \mathcal{P}(\{0,1,\perp\}) \to \mathbb{R}$ defined by

$$f(\delta_0) = g(\delta_1) + \frac{1}{\gamma}(g(\delta_0) - g(\delta_1)), \qquad f(\delta_1) = f(\delta_\perp) = g(\delta_1) \tag{120}$$

is an affine min-tradeoff function for the infrequent sampling channels[9] $\{\mathcal{N}_i = \gamma\mathcal{N}_i^{\text{test}} + (1-\gamma)\mathcal{N}_i^{\text{gen}}\}_i$. Using the affinity of f, for any $c_1^n \in \Omega_{\text{PE}}$:

$$f(\text{Freq}_{c_1^n}(\cdot)) = \text{Freq}_{c_1^n}(0)f(\delta_0) + (1 - \text{Freq}_{c_1^n}(0))f(\delta_1) \tag{121}$$

$$= \frac{\text{Freq}_{c_1^n}(0)}{\gamma} g(\delta_0) + \left(1 - \frac{\text{Freq}_{c_1^n}(0)}{\gamma}\right) g(\delta_1), \tag{122}$$

[8] We remark that the following proof is independent of the choice of min-tradeoff function, which in particular may be optimized when considering specific non-local game primitives. To retrieve the statement in Theorem 3 we use the affine function in Eq. (136) which works for arbitrary non-local games for which $\omega_3 < \omega_2$, but to obtain tighter key rates for the MSG in Section 3.2 we use the affine functions constructed in Sections 5.2 and 5.3.

[9] This follows directly from the observation that if $S_{A,i}$ and $\bar{S}_{B,i}$ are classical, then $H(S_{A,i}\bar{S}_{B,i}|\bar{E}_i) \geq H(S_{A,i}|\bar{E}_i)$.

where in the last equality we use the definition of f in Eq. (57). By definition of Ω_{PE}, we must have $\mathrm{Freq}_{c_1^n}(0) \leq (1-\omega_{\exp}+\delta_{\mathrm{tol}})\cdot\gamma$ which implies $1-\frac{1}{\gamma}\cdot\mathrm{Freq}_{c_1^n}(0) \geq \omega_{\exp}-\delta_{\mathrm{tol}}$. The affinity of f then gives

$$f(\mathrm{Freq}_{c_1^n}(\cdot)) \geq \frac{\mathrm{Freq}_{c_1^n}(0)}{\gamma} g(\delta_0) + (\omega_{\exp}-\delta_{\mathrm{tol}})g(\delta_1) \tag{123}$$

$$= g\left(\frac{\mathrm{Freq}_{c_1^n}(0)}{\gamma}\cdot\delta_0 + (\omega_{\exp}-\delta_{\mathrm{tol}})\cdot\delta_1\right) \tag{124}$$

$$= g(\omega_{\exp}-\delta_{\mathrm{tol}}), \tag{125}$$

where in the last equality we slightly abuse notation to turn the argument to g from a distribution $[q_0,q_1]\in\mathcal{P}(\{0,1\})$ into the winning probability p, which equals one when $[q_0,q_1]=\delta_1$ and zero when $[q_0,q_1]=\delta_0$.

The generalised entropy accumulation theorem [10, Corollary 4.6] then implies:

Lemma 4. *Let $\omega^0_{RQ_E}\in S(RQ_E)$ be the input state to the sequence of channels*

$$\{\mathcal{N}_i\in\mathrm{CPTP}(R\bar{E}_{i-1}, S_{A,i}\bar{S}_{B,i}C_iR\bar{E}_i)\}_{i=1}^n \tag{126}$$

defined in Section 4.4.1. Define the event $\Omega_{\mathrm{PE}}=\{|\{i:C_i=0\}|\leq(1-\omega_{\exp}+\delta_{\mathrm{tol}})\cdot\gamma n\}$ and let $f:\mathcal{P}(\{0,1,\perp\})\to\mathbb{R}$ and $g:\mathcal{P}(\{0,1\})\to\mathbb{R}$ be the functions respectively defined in Eq. (120) and Eq. (119).

Then for any $\varepsilon_s'\in\left[0,\frac{1}{2}\varepsilon_{\mathrm{sec}}\right)$:

$$H_{\min}^{\varepsilon_s'}(S_A\bar{S}_B|\bar{E}_n)_\sigma \geq ng(\omega_{\exp}-\delta_{\mathrm{tol}}) - d_1\sqrt{n} - d_0, \tag{127}$$

where $\sigma_{S_A\bar{S}_BC_1^nR\bar{E}_n}=\mathcal{N}_n\circ\cdots\circ\mathcal{N}_1(\omega^0_{RQ_E})$ and the constants d_1 and d_0 are

$$d_1 := \sqrt{\frac{2\ln(2)V^2}{\eta}\left(\vartheta(\varepsilon_s')+(2-\eta)\log\left(\frac{1}{\Pr[\Omega_{\mathrm{PE}}]_\sigma}\right)\right)}, \tag{128}$$

$$d_0 := \frac{(2-\eta)\eta^2\log\left(\frac{1}{\Pr[\Omega_{\mathrm{PE}}]_\sigma}\right)+\eta^2\vartheta(\varepsilon_s')}{3(\ln 2)^2V^2(2\eta-1)^3}2^{\frac{1-\eta}{\eta}(2+\mathrm{Max}(f)-\mathrm{Min}_\Sigma(f))}\ln^3\left(2^{2+\mathrm{Max}(f)-\mathrm{Min}_\Sigma(f)}+e^2\right) \tag{129}$$

with

$$\eta=\frac{2\ln 2}{1+2\ln 2},\qquad \vartheta(\varepsilon_s')=-\log\left(1-\sqrt{1-(\varepsilon_s')^2}\right),\qquad V=\log(17)+\sqrt{2+\mathrm{Var}(f)}, \tag{130}$$

and where we recall $\Pr[\Omega_{\mathrm{PE}}]_\sigma\geq\varepsilon_a\in\left(0,\frac{1}{2}\varepsilon_{\mathrm{sec}}\right]$.

4.4.3 Guessing probability per testing round

In this section, we construct a simple affine function that bounds the amount of min-entropy generated during each measurement round with a sufficiently high winning probability and serves as the function $g:\mathcal{P}(\{0,1\})\to\mathbb{R}$ in Lemma 4. The method presented here applies to all suitable non-local games as in the framework of Section 2.2 that satisfy the monogamy-of-entanglement property $\omega_3<\omega_2$, where ω_2 is the quantum value of $\mathcal{G}_2$ and ω_3 is the quantum value of the tripartite extension.

Fix a strategy for the 2-player non-local game

$$\mathcal{S}_2=\left\{\nu_{Q_AQ_B},\left\{\{P_a^x\}_{a\in\mathcal{A}}\right\}_x,\left\{\{Q_b^y\}_{b\in\mathcal{B}}\right\}_y\right\} \tag{131}$$

which allows Alice and Bob to win with probability at least $\omega_{\exp}$. That is, letting W_{AB} be the event that Alice and Bob win an instance of the non-local game, we have $\Pr[W_{\mathrm{AB}}]_{\mathcal{S}_2}\geq\omega_{\exp}$ for some $\omega_{\exp}\in[\omega_3,\omega_2]$, where the subscript $\mathcal{S}_2$ denotes that the probability is over the output distribution using strategy $\mathcal{S}_2$.

Add the third player Eve and fix a strategy

$$\mathcal{S}_3=\left\{\nu_{Q_AQ_BE},\left\{\{F_c^{xy}\}_{c\in\mathcal{C}}\right\}_{(x,y)},\left\{\{P_a^x\}_{a\in\mathcal{A}}\right\}_x,\left\{\{Q_b^y\}_{b\in\mathcal{B}}\right\}_y\right\}, \tag{132}$$

which extends $\mathcal{S}_2$. Namely, Alice and Bob's measurements are the same in $\mathcal{S}_2$ and $\mathcal{S}_3$, and $\nu_{Q_A Q_B E} \in \mathcal{S}_3$ is a quantum extension of $\nu_{Q_A Q_B} \in \mathcal{S}_2$. Let G_{E} be the event that Eve guesses the bit S_A sifted by Alice from her output and both inputs to Alice and Bob in one instance of the non-local game. Since strategies of the form $\mathcal{S}_3$ are a subset of all possible tripartite strategies, we have that $\Pr[W_{\mathrm{AB}} \wedge G_{\mathrm{E}}]_{\mathcal{S}_3} \leq \omega_3$. As before, the subscript $\mathcal{S}_3$ indicates that the probability is over the output distribution using strategy $\mathcal{S}_3$.

Now, consider the probability of event G_{E}^c conditioned on W_{AB}:

$$\Pr[G_{\mathrm{E}}^c | W_{\mathrm{AB}}]_{\mathcal{S}_3} = \frac{\Pr[G_{\mathrm{E}}^c \wedge W_{\mathrm{AB}}]_{\mathcal{S}_3}}{\Pr[W_{\mathrm{AB}}]_{\mathcal{S}_2}} \leq \frac{\Pr[G_{\mathrm{E}}^c]_{\mathcal{S}_3}}{\omega_{\mathrm{exp}}}, \tag{133}$$

where we have noted that $\Pr[W_{\mathrm{AB}}]_{\mathcal{S}_3} = \Pr[W_{\mathrm{AB}}]_{\mathcal{S}_2}$. It follows that

$$\omega_{\mathrm{exp}}(1 - \Pr[G_{\mathrm{E}} | W_{\mathrm{AB}}]_{\mathcal{S}_3}) \leq 1 - \Pr[G_{\mathrm{E}}]_{\mathcal{S}_3}, \tag{134}$$

and after rearranging we get

$$\Pr[G_{\mathrm{E}}]_{\mathcal{S}_3} \leq 1 - \omega_{\mathrm{exp}} + \Pr[G_{\mathrm{E}} \wedge W_{\mathrm{AB}}]_{\mathcal{S}_3} \leq 1 - \omega_{\mathrm{exp}} + \omega_3, \tag{135}$$

which readily implies $-\log \Pr[G_{\mathrm{E}}]_{\mathcal{S}_3} \geq -\log(1 - \omega_{\mathrm{exp}} + \omega_3)$.

We wish to find an affine lower bound to $-\log(1 - \omega_{\mathrm{exp}} + \omega_3)$. Since this is convex, a tangent line at any point $\beta \in [\omega_3, \omega_2]$ suffices. This yields the following affine lower bound $g : [\omega_3, \omega_2] \to \mathbb{R}$ to $-\log \Pr[G_{\mathrm{E}}]_{\mathcal{S}_3}$:

$$g(\omega_{\mathrm{exp}}) := \frac{\omega_{\mathrm{exp}} - \beta}{\ln 2 \cdot (1 - \beta + \omega_3)} - \log\big(1 - \beta + \omega_3\big). \tag{136}$$

Then, the function $g(p)$ linearly extended to the domain $p \in [0, 1]$ is such that $-\log \Pr[G_{\mathrm{E}}]_{\mathcal{S}_3} \geq g(p)$, and further g achieves its maximum when $p = 1$. In particular, note that Lemma 1 implies that the function $f : \mathcal{P}(\{0, 1, \perp\}) \to \mathbb{R}$ defined in Eq. (57) satisfies

$$\mathrm{Max}(f) = g(1), \tag{137}$$

$$\mathrm{Min}(f) = \Big(1 - \frac{1}{\gamma}\Big) g(1) + \frac{1}{\gamma} g(0), \tag{138}$$

$$\mathrm{Min}_{\Sigma}(f) \geq g(0), \tag{139}$$

$$\mathrm{Var}(f) \leq \frac{1}{\gamma} \big(g(1) - g(0)\big)^2. \tag{140}$$

Substituting these values in the constants d_1, d_0 of Lemma 4 gives

$$d_1 \leq \sqrt{\frac{2 \ln(2) V^2}{\eta} \left(\vartheta(\varepsilon_s') + (2 - \eta) \log\left(\frac{1}{\varepsilon_a}\right)\right)}, \tag{141}$$

$$d_0 \leq \frac{(2 - \eta)\eta^2 \log\left(\frac{1}{\varepsilon_a}\right) + \eta^2 \vartheta(\varepsilon_s')}{3(\ln 2)^2 V^2 (2\eta - 1)^3} 2^{\frac{1-\eta}{\eta}(2 + g(1) - g(0))} \ln^3\left(2^{2 + g(1) - g(0)} + \mathrm{e}^2\right), \tag{142}$$

where we recall $\varepsilon_a \in \big(0, \frac{1}{2}\varepsilon_{\mathrm{sec}}\big]$ is such that $\Pr[\Omega_{\mathrm{PE}}]_{\sigma} \geq \varepsilon_a$. Further,

$$\eta = \frac{2 \ln 2}{1 + 2 \ln 2}, \qquad \vartheta(\varepsilon_s') = -\log\Big(1 - \sqrt{1 - (\varepsilon_s')^2}\Big), \qquad V \leq \log(17) + \sqrt{2 + \frac{1}{\gamma}\big(g(1) - g(0)\big)^2}, \tag{143}$$

and from g as defined in Eq. (136) we have:

$$g(1) = \frac{1 - \beta}{\ln 2 \cdot (1 - \beta + \omega_3)} - \log\big(1 - \beta + \omega_3\big), \tag{144}$$

$$g(0) = \frac{-\beta}{\ln 2 \cdot (1 - \beta + \omega_3)} - \log\big(1 - \beta + \omega_3\big), \tag{145}$$

for a variable $\beta \in [\omega_3, \omega_2]$ to be optimised.

The assumption $\Pr[W_{\mathrm{AB}} \wedge G_{\mathrm{E}}]_{\mathcal{S}_3} \leq \omega_3$ marks a point where this analysis may be improved. Specifically, when dealing with non-local games that exhibit monogamy of entanglement it is expected that the probability of Alice, Bob and Eve winning an instance of $\mathcal{G}_3$ decreases monotonically if we increase the expected bipartite winning probability $\omega_{\mathrm{exp}} \in [\omega_3, \omega_2]$. Further, if the optimal strategy for Alice and Bob in an instance of $\mathcal{G}_2$ self-tests maximally entangled states, then in the extreme $\Pr[W_{\mathrm{AB}}]_{\mathcal{S}_2} \geq \omega_2$ we expect $\Pr[W_{\mathrm{AB}} \wedge G_{\mathrm{E}}]_{\mathcal{S}_3} \leq \frac{\omega_2}{2}$, as Eve's best strategy is to produce a uniform guess.

Explicitly, suppose instead that whenever $\Pr[W_{\mathrm{AB}}]_{\mathcal{S}_2} \geq \omega_{\mathrm{exp}}$ for $\omega_{\mathrm{exp}} \in [\omega_3, \omega_2]$ we have that $\Pr[W_{\mathrm{AB}} \wedge G_{\mathrm{E}}]_{\mathcal{S}_3} \leq h(\omega_{\mathrm{exp}})$ for a monotonically decreasing, piece-wise differentiable function h. The same analysis as in Eq. (133) shows

$$\Pr[G_{\mathrm{E}}]_{\mathcal{S}_3} \leq 1 - \omega_{\mathrm{exp}} + h(\omega_{\mathrm{exp}}), \tag{146}$$

so a suitable affine lower bound to $-\log \Pr[G_{\mathrm{E}}]$ is given by a tangent at some $\beta \in [\omega_3, \omega_2]$

$$g_{\mathrm{cons}}(\omega_{\mathrm{exp}}) := \frac{(1 - h'(\beta)) \cdot (\omega_{\mathrm{exp}} - \beta)}{\ln 2 \cdot (1 - \beta + h(\beta))} - \log\big(1 - \beta + h(\beta)\big), \tag{147}$$

where the subscript 'cons' emphasizes that $\mathcal{G}_3$ was constrained by Alice and Bob's winning probability in an instance of $\mathcal{G}_2$. In practice, the function h bounding the winning probability of Alice, Bob and Eve in an instance of $\mathcal{G}_3$ constrained on Alice and Bob's winning probability in $\mathcal{G}_2$ may be computed numerically with the NPA hierarchy [42, 43, 44] —see Section 5.2.

Now, we conclude that the functions g and g_{cons} satisfy the definition of Eq. (56). Indeed, letting $S_A = SK_A(A, X, Y)$ be the bit Alice generates from her output A and inputs X, Y in one instance of the non-local game primitive, we have that for any probability distribution $q = [1 - \omega_{\mathrm{exp}}, \omega_{\mathrm{exp}}]$:

$$\min_{\omega_{RE}} \left\{ H(S_A|E)_{\mathcal{N}_i(\omega_{RE})} : \mathrm{Tr}_{S_A RE}[\mathcal{N}_i^{\mathrm{test}}(\omega_{RE})] = (1 - \omega_{\mathrm{exp}}) \left|0\right\rangle\!\left\langle 0\right|_{C_i} + \omega_{\mathrm{exp}} \left|1\right\rangle\!\left\langle 1\right|_{C_i} \right\} \tag{148}$$

$$\geq \min_{\omega_{RE}} \left\{ H_{\min}(S_A|E)_{\mathcal{N}_i(\omega_{RE})} : \mathrm{Tr}_{S_A RE}[\mathcal{N}_i^{\mathrm{test}}(\omega_{RE})] = (1 - \omega_{\mathrm{exp}}) \left|0\right\rangle\!\left\langle 0\right|_{C_i} + \omega_{\mathrm{exp}} \left|1\right\rangle\!\left\langle 1\right|_{C_i} \right\} \tag{149}$$

$$\geq g_{\mathrm{cons}}(\omega_{\mathrm{exp}}) \geq g(\omega_{\mathrm{exp}}), \tag{150}$$

where we have identified register $R = R_A R_B$ with the registers $Q_A Q_B$ shared amongst Alice and Bob in strategy $\mathcal{S}_2$ and noted that since the strategy $\mathcal{S}_3$ is over arbitrary extensions $\nu_{Q_A Q_B E}$ of $\nu_{Q_A Q_B}$ so in particular includes the case where $E = E'F$ for a purifying register F that gets acted on trivially by Eve's instruments, as per the definition in Eq. (56). Further, the channel $\mathcal{N}_i$ used above is as in Eq. (117) such that the strategy $\mathcal{S}_2$ corresponds to the quantum instruments performed by the devices of Alice and Bob in an application of $\mathcal{N}_i$. Lastly, on the last inequality above we shift the argument of g from a probability distribution on $\mathcal{P}(\{0,1\})$ to the winning probability.

4.4.4 Final secrecy bound

Finally, we are ready to lower bound the smooth min-entropy $H_{\min}^{\varepsilon_s'}(S_A \bar{S}_B|\bar{E})_{\sigma_{|\Omega_{\mathrm{PE}}}}$ in the right hand side of Eq. (107) and conclude the secrecy proof.

Lemma 4 with g as in the previous section gives

$$H_{\min}^{\varepsilon_s'}(S_A \bar{S}_B|\bar{E})_{\sigma_{|\Omega_{\mathrm{PE}}}} \geq n g(\omega_{\mathrm{exp}} - \delta_{\mathrm{tol}}) - d_1 \sqrt{n} - d_0, \tag{151}$$

for the constants d_1, d_0 as in Eqs. (141) and (142) respectively. Together with Eqs. (94) and (107) we have

$$H_{\min}^{\varepsilon_s}(S_A|E_n)_{\sigma_{|\Omega_{\mathrm{PE}} \wedge \Omega_{\mathrm{EC}}}} \geq n g(\omega_{\mathrm{exp}} - \delta_{\mathrm{tol}}) - d_1 \sqrt{n} - d_0 - (2 - \omega_{\mathrm{exp}} + \delta_{\mathrm{tol}}) n(\gamma + \kappa) \tag{152}$$

$$- 2\vartheta(\delta) - l_{\mathrm{EC}} - \lambda_{\mathrm{EC}} - 2, \tag{153}$$

where we recall $\varepsilon_s \in \big(0, \frac{1}{2}\varepsilon_{\mathrm{sec}}\big)$, $\varepsilon_s' \in \big[0, \frac{1}{2}\varepsilon_{\mathrm{sec}}\big)$ and $\varepsilon_s'' \in \big[0, \frac{1}{4}\varepsilon_{\mathrm{sec}}\big)$ are such that $\delta = \varepsilon_s - \varepsilon_s' - 2\varepsilon_s'' > 0$, and $\kappa \geq \frac{1}{\sqrt{n}} \sqrt{-\ln \varepsilon_s''}$. Then, the Leftover Hashing Lemma (Lemma 2) implies

$$\left\| \rho_{K_A E|\Omega_{\mathrm{PE}} \wedge \Omega_{\mathrm{EC}}} - \tau_{K_A} \otimes \rho_{E|\Omega_{\mathrm{PE}} \wedge \Omega_{\mathrm{EC}}} \right\|_{\mathrm{Tr}} \tag{154}$$

$$\leq \frac{1}{2} \cdot 2^{-\frac{1}{2}\left(n g(\omega_{\mathrm{exp}} - \delta_{\mathrm{tol}}) - d_1 \sqrt{n} - d_0 - (2 - \omega_{\mathrm{exp}} + \delta_{\mathrm{tol}}) n(\gamma + \kappa) - 2\vartheta(\delta) - l_{\mathrm{EC}} - \lambda_{\mathrm{EC}} - 2 - l_{\mathrm{key}}\right)} + 2\varepsilon_s. \tag{155}$$

Finally, merging with Eq. (88) and the conditions $\Pr[\Omega_{\rm g}|\Omega_{\rm PE}] \geq \varepsilon_s^2$ and $\Pr[\Omega_{\rm PE}] \geq \varepsilon_a \in \left(0, \frac{1}{2}\varepsilon_{\rm sec}\right]$, we have secrecy with parameter $\max\left\{2\varepsilon_a, 2\varepsilon_s^2, \varepsilon_{\rm sec}\right\} = \varepsilon_{\rm sec}$ provided

$$2^{-\frac{1}{2}\left(ng(\omega_{\rm exp}-\delta_{\rm tol})-d_1\sqrt{n}-d_0-(2-\omega_{\rm exp}+\delta_{\rm tol})n(\gamma+\kappa)-2\vartheta(\varepsilon_s-\varepsilon'_s-2\varepsilon''_s)-l_{\rm EC}-\lambda_{\rm EC}-l_{\rm key}\right)} + 2\varepsilon_s \leq \varepsilon_{\rm sec}, \tag{156}$$

which implies

$$l_{\rm key} \leq ng(\omega_{\rm exp}-\delta_{\rm tol}) - d_1\sqrt{n} - d_0 - (2-\omega_{\rm exp}+\delta_{\rm tol})n(\gamma+\kappa) - 2\vartheta(\varepsilon_s-\varepsilon'_s-2\varepsilon''_s) \tag{157}$$

$$- l_{\rm EC} - \lambda_{\rm EC} - 2\log\frac{1}{\varepsilon_{\rm sec}-2\varepsilon_s}. \tag{158}$$

In order to maximize the finite key rates given by $\frac{1}{n}l_{\rm key}$, we wish to minimize all the terms in the right hand side which depend on the free variables $\varepsilon_a, \varepsilon_s, \varepsilon'_s, \varepsilon''_s$.

First, we tackle the coefficients d_1, d_0 respectively as in Eqs. (141), and (142). Note that d_1 asymptotically scales as $O(n^{-1/2})$ in the expression for the key rate, whereas d_0 scales as $O(n^{-1})$. Without loss of generality we can fix $\varepsilon_a = \frac{1}{2}\varepsilon_{\rm sec}$ since $\arg\min_{\varepsilon_a}(d_0) = \arg\min_{\varepsilon_a}(d_1) = \frac{1}{2}\varepsilon_{\rm sec}$, as ε_a does not appear elsewhere in Eq. (157). To further minimize d_1, d_0, we need $\vartheta(\varepsilon'_s) \in \mathbb{R}^+ \cup \{0\}$ to be small, which requires $\varepsilon'_s \in \left[0, \frac{1}{2}\varepsilon_{\rm sec}\right)$ to be large. Moreover, the term κ which also scales as $O(n^{-1/2})$ in the key rate is minimized when $\varepsilon''_s \in \left[0, \frac{1}{4}\varepsilon_{\rm sec}\right)$ is large. Further, $\vartheta(\varepsilon_s - \varepsilon'_s - 2\varepsilon''_s)$ which scales as $O(n^{-1})$ in $\frac{1}{n}l_{\rm key}$, is smallest when $\varepsilon_s - \varepsilon'_s - 2\varepsilon''_s \in \left(0, \frac{1}{2}\varepsilon_{\rm sec}\right)$ is large. This requires both $\varepsilon_s \in \left(0, \frac{1}{2}\varepsilon_{\rm sec}\right)$ to be large and $\varepsilon'_s, 2\varepsilon''_s \in \left[0, \frac{1}{2}\varepsilon_{\rm sec}\right)$ to be small. Lastly, the $\log\frac{1}{\varepsilon_{\rm sec}-2\varepsilon_s}$ term vanishes as $O(n^{-1})$ in the key rate and is minimized when ε_s is close to 0.

These conditions impose a tradeoff between $\varepsilon_s, \varepsilon'_s, \varepsilon''_s$ in order to maximize the finite key rates. For pedagogical purposes, it suffices to set $\varepsilon_a = \frac{1}{2}\varepsilon_{\rm sec}$, $\varepsilon'_s = \frac{1}{2}\varepsilon_s$ and $\varepsilon''_s = \frac{1}{8}\varepsilon_s$, in which case we obtain the expression from the statement of Theorem 3

$$l_{\rm key} \leq ng(\omega_{\rm exp}-\delta_{\rm tol}) - d_1\sqrt{n} - d_0 - (2-\omega_{\rm exp}+\delta_{\rm tol})n(\gamma+\kappa) - 2\vartheta\left(\frac{\varepsilon_s}{4}\right) \tag{159}$$

$$- l_{\rm EC} - \lambda_{\rm EC} - 2\log\frac{1}{\varepsilon_{\rm sec}-2\varepsilon_s}, \tag{160}$$

wherein $\kappa \geq \frac{1}{\sqrt{n}}\sqrt{\ln 8 - \ln\varepsilon_s}$, and

$$d_1 \leq \sqrt{\frac{2\ln(2)V^2}{\eta}\left(\vartheta\left(\frac{\varepsilon_s}{2}\right) + (2-\eta)\log\left(\frac{2}{\varepsilon_{\rm sec}}\right)\right)}, \tag{161}$$

$$d_0 \leq \frac{(2-\eta)\eta^2\log\left(\frac{2}{\varepsilon_{\rm sec}}\right) + \eta^2\vartheta(\frac{\varepsilon_s}{2})}{3(\ln 2)^2V^2(2\eta-1)^3}2^{\frac{1-\eta}{\eta}(2+g(1)-g(0))}\ln^3\left(2^{2+g(1)-g(0)} + {\rm e}^2\right). \tag{162}$$

Further,

$$\eta = \frac{2\ln 2}{1+2\ln 2}, \qquad V \leq \log(17) + \sqrt{2 + \frac{1}{\gamma}\big(g(1)-g(0)\big)^2}, \tag{163}$$

and from g as defined in Eq. (136) we have:

$$g(1) = \frac{1-\beta}{\ln 2\cdot(1-\beta+\omega_3)} - \log\big(1-\beta+\omega_3\big), \tag{164}$$

$$g(0) = \frac{-\beta}{\ln 2\cdot(1-\beta+\omega_3)} - \log\big(1-\beta+\omega_3\big), \tag{165}$$

for a variable $\beta \in [\omega_3, \omega_2]$ to be optimised. This concludes the proof.

We remark that the finite key rates for the magic square game in Figure 3 are generated through numerical optimization of all free variables $\varepsilon_a, \varepsilon_s, \varepsilon'_s, \varepsilon''_s$, but the particular choice of variables above does not incur discernible changes in the finite key rates.

5 Numerical optimizations for the magic square game

In this section, we show that the magic square game satisfies $\omega_3 < \omega_2$, and subsequently construct bounds on the min-entropy and von Neumann entropy of Alice's generated bit conditioned on an eavesdropper's information.

5.1 Tripartite value of the magic square game

Recall the bipartite magic square game MSG_2, in which Alice and Bob respectively receive uniform inputs $x, y \in \{0, 1, 2\}$, produce bit triples a of even Hamming weight and b of odd Hamming weight, and win whenever the y-th bit of a equals the x-th bit of b —symbolically $a[y] = b[x]$.

It is known [40, 41] that the maximal winning probability using classical strategies is $\omega_{\mathrm{C}}(\mathrm{MSG}_2) = \frac{8}{9}$ and that the maximal winning probability using a quantum strategy is $\omega_{\mathrm{Q}}(\mathrm{MSG}_2) = 1$. The strategies achieving each value are outlined at the beginning of Section 3.2.

We consider a tripartite extension to the standard magic square game, which we label MSG_3, in which the third player (for now, let us blissfully call him Charlie) receives both inputs x, y and produces a single bit $c \in \{0, 1\}$ required to satisfy $c = a[y] = b[x]$.

In this section we compute bounds on the min-entropy and on the von Neumann entropy of Alice's sifted bit $a[y]$ conditioned on the third player's side information. The main numerical tools used in this section is the NPA hierarchy [42, 43, 44] which we briefly describe in the following. Consider a polynomial optimization problem with non-commuting variables of the form

$$p_{\mathrm{opt}} := \inf_{\mathcal{H}, X, |\phi\rangle} \langle\phi| \, p(X) \, |\phi\rangle \tag{166}$$

$$\text{s.t.:} \quad g_i(X) \geq 0 \quad i = 1, ..., m, \tag{167}$$

$$\|\phi\| = 1, \tag{168}$$

where p and g_i are Hermitian polynomials in the algebra generated by $2n$ non-commuting variables $(x_1, ..., x_n, x_1^\dagger, ..., x_n^\dagger)$. The optimization is over the Hilbert space $\mathcal{H}$, the state $|\phi\rangle \in \mathcal{H}$ and the variables $X = (X_1, ..., X_n)$ which are bounded operators in $\mathcal{H}$. The NPA hierarchy is a sequence of semidefinite programs (SDP) with increasing relaxations which monotonically converge to the optimal value in Eq. (166). In short, if $d \in \mathbb{N}$ is the level of the hierarchy[10] and $p_d \in \mathbb{R}$ is the optimum value of the SDP at level d of the hierarchy, then

$$p_{d'} \geq p_d \quad \forall d' \geq d \tag{169}$$

$$\lim_{d \to \infty} p_d = p_{\mathrm{opt}}. \tag{170}$$

We also reference the **ncpol2sdpa** python library [44] written by Wittek and maintained by Brown, which implements the NPA hierarchy and which we use throughout this section (see our python scripts in [55]).

We begin with an analysis on the classical, quantum and no-signalling values of the tripartite MSG_3. The classical strategy achieving $\omega_{\mathrm{C}}(\mathrm{MSG}_2) = \frac{8}{9}$ can be used to infer that $\omega_{\mathrm{C}}(\mathrm{MSG}_3) = \frac{8}{9}$. Further, we use the linear program in [56, Section 3] to show $\omega_{\mathrm{NS}}(\mathrm{MSG}_3) = 1$. Now, a general quantum strategy for MSG_3 is given by the tuple

$$\mathcal{S} = \Big\{ \nu_{Q_A Q_B Q_C}, \big\{ \{F_c^{xy}\}_{c \in \{0,1\}} \big\}_{(x,y)}, \big\{ \{P_a^x\}_{a \in \mathcal{A}} \big\}_x, \big\{ \{Q_b^y\}_{b \in \mathcal{B}} \big\}_y \Big\}, \tag{171}$$

where $\nu_{Q_A Q_B Q_C} \in S(Q_A Q_B Q_C)$ is a tripartite state, $\{\{P_a^x\}_{a \in \mathcal{A}}\}_x$, and $\{\{Q_b^y\}_{b \in \mathcal{B}}\}_y$ are POVMs in Alice and Bob's spaces indexed over respective alphabets $\mathcal{A} = \{000, 011, 101, 110\}$ and $\mathcal{B} = \{001, 010, 100, 111\}$, and $\{\{F_c^{xy}\}_{c \in \{0,1\}}\}_{(x,y)}$ are POVMs in Charlie's space.

The quantum value of MSG_3 is then

$$\omega_{\mathrm{Q}}(\mathrm{MSG}_3) = \sup_{\mathcal{S}} \sum_{x,y} \frac{1}{9} \mathrm{Tr}\Big[\nu_{Q_A Q_B Q_C} \Pi^{xy} \Big], \tag{172}$$

[10] We note that in principle it is possible to optimise SDPs that lie between the discrete levels of the hierarchy, depending on the available computational power.

where

$$\Pi^{xy} := \sum_{c\in\{0,1\}} \left[F_c^{xy} \otimes \sum_{a\in\mathcal{A}:a[y]=c} P_a^x \otimes \sum_{b\in\mathcal{B}:b[x]=c} Q_b^y \right]. \tag{173}$$

Without loss of generality we can assume that all POVMs in $\mathcal{S}$ are projective by Naimark's Theorem, and further that $\nu_{Q_AQ_BQ_C} = |\phi\rangle\langle\phi|_{Q_AQ_BQ_C}$ is pure since the dimension of $Q_AQ_BQ_C$ is arbitrary. Eq. (172) therefore becomes

$$\omega_{\mathrm{Q}}(\mathrm{MSG}_3) = \sup_{\mathcal{S}} \frac{1}{9} \sum_{x,y} \langle\phi| \Pi^{xy} |\phi\rangle , \tag{174}$$

and the optimization is over the Hilbert space $Q_AQ_BQ_C$, the state $|\phi\rangle \in Q_AQ_BQ_C$ and the PVMs on Alice, Bob and Charlie's systems.

We use the NPA hierarchy to show (see Appendix A and [55]):

Theorem 4. *For the* MSG_3 *game considered above, we have*

$$\omega_{\mathrm{Q}}(\mathrm{MSG}_3) \lesssim \frac{8.00077}{9}. \tag{175}$$

This is a numerical upper bound on the winning probability, supporting the conjecture that the value is in fact exactly $\frac{8}{9}$. The intuition behind this result is that the quantum strategy yielding $\omega_{\mathrm{Q}}(\mathrm{MSG}_2) = 1$ requires Alice and Bob to share maximally entangled states —in fact, the optimal quantum bipartite strategy self-tests a pair of maximally entangled states [31]. Monogamy of entanglement then suggests that the correlations shared by Alice, Bob and Charlie in an instance of MSG_3 are not enough to obtain a value $\omega_{\mathrm{Q}}(\mathrm{MSG}_3)$ larger than $\omega_{\mathrm{C}}(\mathrm{MSG}_3)$.

5.2 Bound on min-entropy

The goal of this section is to compute the function $h : [8/9, 1] \to \mathbb{R}$ in Eq. (147) to lower bound the min-entropy of Alice's bit $A[Y]$ conditioned on the third player's information, generated in one round of the MSG. The function h is used in the min-tradeoff function in Eq. (147) to provide the finite key length in Eq. (27) of the MSG-DIQKD protocol.

To bound the min-entropy of Alice's bit conditioned on third player (now turned Eve), we are interested in the related optimization problem given by

$$\sup \frac{1}{9} \sum_{x,y} \langle\phi| \Pi^{xy} |\phi\rangle \tag{176}$$

$$\text{s.t.: } \{P_a^x\}_a, \{Q_b^y\}_b, \{F_c^{xy}\}_c \text{ are PVMs in different labs for all } x, y, \tag{177}$$

$$\langle\phi| \frac{1}{9} \sum_{xy} \Pi_{AB}^{xy} |\phi\rangle \geq \omega_{\mathrm{exp}}, \tag{178}$$

where $\omega_{\mathrm{exp}} \in [8/9, 1]$ and

$$\Pi_{AB}^{xy} := \sum_{c\in\{0,1\}} \mathbb{I}_{Q_C} \otimes \sum_{a\in\mathcal{A}:a[y]=c} P_a^x \otimes \sum_{b\in\mathcal{B}:b[x]=c} Q_b^y \tag{179}$$

is the projection yielding a winning outcome for Alice and Bob. This is precisely the optimization problem resulting from fixing a bipartite strategy

$$\mathcal{S}_2 = \left\{ \nu_{Q_AQ_B}, \left\{ \{P_a^x\}_{a\in\mathcal{A}} \right\}_x, \left\{ \{Q_b^y\}_{b\in\mathcal{B}} \right\}_y \right\} \tag{180}$$

which allows Alice and Bob to win with probability at least ω_{exp} and subsequently considering a tripartite strategy

$$\mathcal{S}_3 = \left\{ \nu_{Q_AQ_BE}, \left\{ \{F_c^{xy}\}_{c\in\mathcal{C}} \right\}_{(x,y)}, \left\{ \{P_a^x\}_{a\in\mathcal{A}} \right\}_x, \left\{ \{Q_b^y\}_{b\in\mathcal{B}} \right\}_y \right\}, \tag{181}$$

which extends $\mathcal{S}_2$ —that is $\mathcal{S}_3 = \mathcal{S}_2 \cup \left\{\{\{F_c^{xy}\}_c\}_{(x,y)}\right\}$ and $\mathrm{Tr}_{Q_C}[\nu_{Q_A Q_B E}] = \nu_{Q_A Q_B}$. We use the NPA hierarchy to bound these probabilities constrained on a range of values of $\omega_{\text{exp}} \in [8/9, 1]$ and display the results in Figure 6[11].

We remark that the optimums in the optimization problem in Eq. (176) form a monotonically decreasing and concave curve. Monotonically decreasing because increasing $\omega_{\text{exp}} \in [8/9, 1]$ decreases the size of the feasible set of the optimization problem, and concave because the straight line connecting the optimums given by any pair of constraints $\omega_{\text{exp}}^1 < \omega_{\text{exp}}^2$ on Alice and Bob's winning probability is a lower bound on the optimal value for any $\omega_{\text{exp}} \in (\omega_{\text{exp}}^1, \omega_{\text{exp}}^2)$[12].

The monotonicity is a direct consequence of the monogamy-of-entanglement property. Indeed, the magic square game self-tests a pair of maximally entangled states [31], so it is expected that the value $\sup \frac{1}{9} \sum_{x,y} \langle\phi| \Pi^{xy} |\phi\rangle$ decreases from 8/9 when $\omega_{\text{exp}} = 8/9$ to 1/2 when $\omega_{\text{exp}} = 1$. Consequently, Eve's best strategy if Alice and Bob are required to win with unit probability is to make a uniform guess, which brings the tripartite winning probability to 1/2 —as can be verified by the rightmost datapoint in Figure 6.

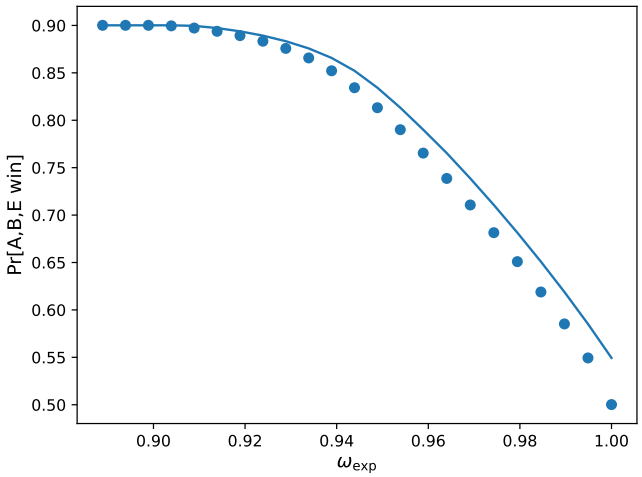


Figure 6: Upper bounds on the winning probability of Alice, Bob and Eve on non-local games constrained on the winning probability of Alice and Bob as given by the problem in Eq. (176). The solid line corresponds to the upper bound defined in Eq. (183) from the NPA points. See [55] for Python script used to generate these figures.

The upper bound $h : [8/9, 1] \to \mathbb{R}$ can be constructed from the N points computed via the NPA hierarchy as follows. Given a sequence of N constraints $[x_k]_{k=0}^{N-1}$ on ω_{exp} with corresponding upper bounds $[y_k]_{k=0}^{N-1}$ to the optimization in Eq. (176) obtained via the NPA hierarchy, let L_k be the straight line segment connecting points (x_k, y_k) to (x_{k+1}, y_{k+1}). For any $x \in [x_k, x_{k+1}]$, L_k is given by the following explicit form

$$f_k(x) = \frac{y_{k-1} - y_k}{x_{k-1} - x_k}(x - x_k) - y_k. \tag{182}$$

Hence, a continuous upper bound to the tripartite winning probability h is defined as follows

$$h(\omega_{\text{exp}}) := \begin{cases} 8/9 & \text{if } x_0 \leq \omega_{\text{exp}} \leq x_1 \\ f_k(\omega_{\text{exp}}) & \text{if } x_{k+1} \leq \omega_{\text{exp}} \leq x_{k+2} \text{ for } k = 0, ..., N-3. \end{cases} \tag{183}$$

[11] We remark that the values in the figure are obtained via relaxation of the NPA containing less extramonomials than the value in Theorem 4. For reference, each semidefinite program in Figure 6 takes roughly 12h on a desktop with 256GB of RAM using the scripts in [55], whereas the 8.00077/9 bound obtained in Theorem 4 takes about 3 days.

[12] Specifically, a convex combination of the strategies given by the pair of constraints $\omega_{\text{exp}}^1 < \omega_{\text{exp}}^2$ is a valid strategy, but not necessarily the optimal one

On a slight technicality, we remark that this upper bound is differentiable everywhere except at each point x_k. However, this is not an issue as one can simply choose the gradient of either the line segment preceding or succeeding it whilst guaranteeing that the resulting tangent is still an upper bound to the tripartite winning probability.

Intuitively, h is constructed by placing the line segment L_k connecting the pairs (x_k, y_k) and (x_{k+1}, y_{k+1}) above the pairs (x_{k+1}, y_{k+1}) to (x_{k+2}, y_{k+2}). The resultant function is clearly an upper bound by the monotonicity and concavity of the optimums of Eq. (176) for constraints $\omega_{\text{exp}} \in [8/9, 1]$ and further converges as $N \to \infty$. The function h is plotted in Figure 6.

Using h in the the bound for Eve's guessing probability in Eq. (146) directly yields a bound to the min-entropy of Alice's key bit in one instance of the magic square game $H_{\min}(S_A|E)_\nu$ for $\nu \in \mathcal{S}_2$. An affine lower bound to this min-entropy is subsequently given by Eq. (147).

5.3 Bound on von-Neumann entropy

In this section, we additionally employ the device independent bounds introduced in [45] to obtain a bound of the von Neumann entropy $H(S_A|E)_\nu$ of Alice's bit $S_A = A[Y]$ in one instance of the MSG over states ν belonging to a strategy of Alice and Bob $\mathcal{S}_2$ which achieves $\omega_{\text{exp}} \in [8/9, 1]$. This is done in order to obtain a tighter min-tradeoff function for improved key rates in our MSG-DIQKD protocol.

Firstly, note that it is not possible to use [45, Lemma 2.3] directly for the magic square game. This is because in the MSG, the key bit S_A generated each round is not interchangeable with the register A in the lemma, which is to be interpreted as the outcome of the non-local game. Indeed, Alice's measurement output A in the magic square non-local game does not correspond to Alice's key bit for that round. Nonetheless, it is possible to use [45, Theorem 2.1] to overcome this subtlety for the MSG and prove a similar bound:

Theorem 5. *Let $m \in \mathbb{N}$, and let $t_1, ..., t_m$ and $w_1, ..., w_m$ be the nodes and weights of an m-point Gauss-Radau quadrature on $[0, 1]$ with endpoint $t_m = 1$ (see [45] for relevant definitions). Let $\nu_{Q_A Q_B E}$ be the initial quantum state shared between the devices of Alice, Bob and Eve in an instance of the MSG and let $\{P_a^x\}_a$ denote the measurement operators performed by Alice's device in the MSG on input $x \in \mathcal{X}$. Further, for $i = 1, ..., m-1$ let $\alpha_i = \frac{3}{2}\max\{\frac{1}{t_i}, \frac{1}{t_{1-1}}\}$. Then $H(S_A|XYE)_\nu$ is lower bounded by*

$$c_m + \sum_{i=1}^{m-1} \frac{w_i}{t_i \ln 2} \sum_{s,x,y} \pi(x,y) \inf_{Z_{s,x,y}} \text{Tr}\left[\nu_{Q_A E}\left(\sum_{a:a[y]=s} P_a^x \otimes (Z_{s,x,y} + Z_{s,x,y}^\dagger + (1-t_i) Z_{s,x,y}^\dagger Z_{s,x,y})\right)\right] \tag{184}$$

$$+ \text{Tr}\big[\rho_{Q_A Q_E} t_i (\mathbb{I}_{S_A} \otimes Z_{s,x,y} Z_{s,x,y}^\dagger)\big], \tag{185}$$

such that $\|Z_{s,x,y}\|_\infty \leq \alpha_i$, where $c_m = \sum_{i=1}^{m-1} \frac{w_i}{t_i \ln 2}$, the infimum is over operators $Z_{s,x,y}$ in Eve's space and $\pi(x,y)$ is the probability that Alice and Bob select inputs x, y. Moreover, these bounds converge to $H(S_A|XYE)_\nu$ as $m \to \infty$.

The proof of this theorem is analogous to that of [45, Lemma 2.3] albeit more involved by necessity of notation, but requires us to first establish some notation about the magic square game.

Suppose that $\nu_{Q_A Q_B E} \in S(Q_A Q_B E)$ is the state shared by Alice, Bob and Eve at the beginning of the game chosen such that Alice and Bob win MSG_2 with probability $\omega_{\text{exp}} \in [8/9, 1]$. On input of $x \in \{0, 1, 2\}$ for Alice and $y \in \{0, 1, 2\}$ for Bob, they will perform measurements $\{P_a^x\}_a$ and $\{Q_b^y\}_b$ on their respective portions of ν. Including the input registers, the post-measurement state is $\nu_{ABXYE} = \sum_{a,b,x,y} \pi(x,y) \, |abxy\rangle\langle abxy| \otimes \nu_E^{abxy}$, where $\nu_E^{abxy} = \text{Tr}_{Q_A Q_B}[\nu_{Q_A Q_B E}(P_a^x \otimes Q_b^y \otimes \mathbb{I}_E)]$ is Eve's post-measurement subnormalised state. Now, to generate her key bit Alice applies the map

$$\mathcal{E} \in \text{CPTP}(AY, SY), \tag{186}$$

$$\mathcal{E} : |a_0 y_0\rangle\langle a_1 y_1| \mapsto |a_0[y_0] y_0\rangle\langle a_1[y_1] y_1|, \tag{187}$$

for any pairs $a_0, a_1 \in \{000, 011, 101, 110\}$ and $y_0, y_1 \in \{0, 1, 2\}$. We include the register Y in the codomain

of $\mathcal{E}$ to emphasize that Eve knows it. This results in the state

$$\nu_{S_A BXYE} = \sum_{a,b,x,y} \pi(x,y)\,|a[y]bxy\rangle\langle a[y]bxy| \otimes \nu_E^{abxy} \tag{188}$$

$$= \sum_{s,b,x,y} \pi(x,y)\,|sbxy\rangle\langle sbxy| \otimes \nu_E^{sbxy}, \tag{189}$$

where we have introduced the subnormalized state $\nu_E^{sbxy} := \sum_{a:a[y]=s} \nu_E^{abxy}$. Note that

$$\sum_{a:a[y]=s} \nu_E^{abxy} = \mathrm{Tr}_{Q_A Q_B}\left[\nu_{Q_A Q_B E}\left(\sum_{a:a[y]=s} P_a^x \otimes Q_b^y \otimes \mathbb{I}_E\right)\right], \tag{190}$$

so ν_E^{sbxy} is analogously obtained by using $P_s^{xy} = \sum_{a:a[y]=s} P_a^x$ instead.

We continue by exploring how this rewriting of P_s^{xy} affects the expression for Alice's and Bob's winning probability constraint. Recall that $\nu_{Q_A Q_B E}$ is chosen so that

$$\omega_{\text{exp}} = \sum_{x,y} \frac{1}{9}\,\mathrm{Tr}[\nu_{Q_A Q_B E}\Pi_{AB}^{xy}], \tag{191}$$

where

$$\Pi_{AB}^{xy} = \frac{1}{9}\sum_{s\in\{0,1\}}\left[\sum_{a:a[y]=s} P_a^x \otimes \sum_{b:b[x]=s} Q_b^y \otimes \mathbb{I}_E\right] \tag{192}$$

$$= \frac{1}{9}\sum_{s\in\{0,1\}}\left[P_s^{xy} \otimes \sum_{b:b[x]=s} Q_b^y \otimes \mathbb{I}_E\right]. \tag{193}$$

Replacing Alice's projections with $\{P_s^{xy}\}$ and accounting for inputs x, y in the proof of [45, Lemma 2.3] yields precisely the statement in Theorem 5.

In practice, the expression in Theorem 5 bounding the entropy $H(S_A|XYE)$ in the MSG contains too many operators to feasibly optimize using the NPA hierarchy. However, note $H(S_A|XYE)_\nu = \sum_{x,y}\pi(x,y)H(S_A|X=x,Y=y;E)_{\nu^{xy}}$ where $\nu_{S_A XYE}^{xy} = \sum_s \pi(x,y)[s]\otimes\nu_E^{sxy}$ is the final state with fixed inputs (x,y) and $\pi(x,y)$ is uniform. This implies $H(S_A|XYE)_\nu$ is lower bounded by $H(S_A|X\in\mathcal{X}', Y\in\mathcal{Y}';E)_\nu$ for any subsets $\mathcal{X}'\subset\mathcal{X}, \mathcal{Y}'\subset\mathcal{Y}$ which may be chosen to make the NPA optimization feasible. In particular, $H(S_A|X\in\mathcal{X}', Y\in\mathcal{Y}';E)_\nu$ is lower bounded by replacing the inner summation in the expression of Theorem 5 with

$$\sum_{\substack{s\\ x\in\mathcal{X}'\\ y\in\mathcal{Y}'}} \frac{1}{|\mathcal{X}'\times\mathcal{Y}'|}\inf_{Z_{s,x,y}}\ \mathrm{Tr}\left[\nu_{Q_A Q_E}\left(\sum_{a:a[y]=s} P_a^x \otimes (Z_{s,x,y} + Z_{s,x,y}^\dagger + (1-t_i)Z_{s,x,y}^\dagger Z_{s,x,y})\right)\right] \tag{194}$$

$$+\,\mathrm{Tr}\big[\nu_{Q_A Q_E} t_i(\mathbb{I}_{S_A}\otimes Z_{s,x,y}Z_{s,x,y}^\dagger)\big]. \tag{195}$$

Results from these optimizations choosing $\mathcal{X}'=\{0\}$ and $\mathcal{Y}'=\{0\}$, and $\mathcal{X}'=\{0,1,2\}$ and $\mathcal{Y}'=\{0\}$ are presented in Figures 4 (alongside the corresponding Devetak-Winter rates) and 7. In the latter, we also compare the min-entropy bound derived in the previous section: $-\log(1-\omega_{\text{exp}}+h(\omega_{\text{exp}}))$ for $\omega_{\text{exp}}\in[\frac{8}{9},1]$ and $h:[\frac{8}{9},1]\to\mathbb{R}$ the continuous upper bound defined in Eq. (183).

It is apparent in Figure 7 that as a consequence of having to restrict the set of inputs in Eq. (194) to make the numerical optimization feasible, the resultant von Neumann entropy bounds are not optimal —in particular, for $\omega_{\text{exp}}\lesssim 0.97$ the min-entropy bound gives a higher value. When reporting the finite and asymptotic statistics for the MSG-DIQKD in Section 3.2 we use whichever entropy bound yields better key rates.

Further, we remark that when Alice and Bob require a winning probability of 1, $H_{\min}(S_A|XYE) = H(S_A|XYE) = 1$ as opposed to the roughly $H_{\min}(S_A|XYE)\approx 0.85$ in Figure 7. We attribute this error to the amount of points in Figure 6 from which h is constructed —indeed the function h converges to the tripartite winning probability bound as the number of points increases.

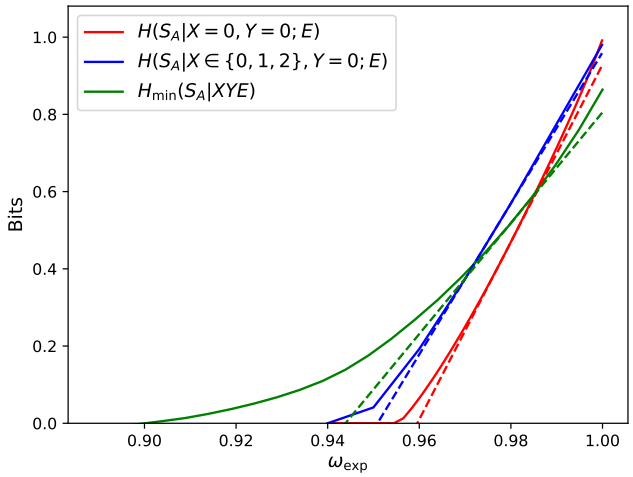


Figure 7: Comparison of bounds to the entropy of Alice's raw key conditioned on Eve's information. Solid green line corresponds to the negative logarithm of Eq. (146), whilst the solid red line and solid blue line correspond to the bounds on $H(S|X \in \mathcal{X}', Y=0; Q_E)$ for $\mathcal{X}' = \{0\}, \{0,1,2\}$ respectively, found via Theorem 5 and Eq. (194). The corresponding dashed lines are affine lower bounds to each entropy at the point 0.98, computed using Eq. (147) for the min entropy (green) and Eq. (196) for the von Neumann entropies (red, blue).

In the remainder of this section, we use the points computed using the optimization from Theorem 5 to construct an affine lower bound to the von Neumann entropy $H(S_A|XYE)$ in one instance of the magic square game. Analogous to the previous section, given a sequence of constraints $[x_k]_{k=0}^{N-1} \subset [8/9, 1]$ with corresponding optimums $[y_k]_{k=0}^{N-1} \subset [0,1]$ of the optimization problem in Theorem 5, then a lower bound to $H(S_A|XYE)$ is given by the continuous function $h_{\text{vN}} : [8/9,1] \to \mathbb{R}$ defined by

$$h_{\text{vN}}(\omega_{\text{exp}}) := \begin{cases} 0 & \text{if } x_0 \leq \omega_{\text{exp}} \leq x_1 \\ \frac{y_{k-1}-y_k}{x_{k-1}-x_k}(\omega_{\text{exp}} - x_k) - y_k & \text{if } x_{k+1} \leq \omega_{\text{exp}} \leq x_{k+2} \text{ for } k = 0, ..., N-3. \end{cases} \tag{196}$$

Since the von Neumann entropy is convex and monotically increasing in the constraint $\omega_{\text{exp}} \in [8/9, 1]$, the function h_{vN} obtained via the lower bounds of Theorem 5 is indeed a lower bound which converges as the number of points N goes to infinity. Hence, any tangent $g_{\text{vN}} : [8/9,1] \to \mathbb{R}$ to h_{vN} is a suitable affine lower bound to the von Neumann entropy which may replace the affine function g in the finite key length of Eq. (27). This is because g_{vN} is a lower bound to

$$\min_{\omega_{REF}} \{H(S_A|E)_{\mathcal{N}_i(\omega_{REF})} : \text{Tr}_{S_A REF}[\mathcal{N}_i^{\text{test}}(\omega_{REF})] = (1-\omega_{\text{exp}})\,|0\rangle\langle 0|_{C_i} + \omega_{\text{exp}}\,|1\rangle\langle 1|_{C_i}\} \tag{197}$$

for $\mathcal{N}_i$ as in Eq. (117), following the same logic as in Eqs. (148)-(150) and the remarks thereafter.

6 Conclusions

In this work we introduce a framework for device independent quantum key distribution leveraging on any two party non-local game with a winning condition that requires Alice and Bob to produce a matching bit. The security of this protocol is derived from a monogamy-of-entanglement property which states that the winning probability of the non-local game played solely by Alice and Bob is higher than the winning probability of the same game extended to three parties, in which the third party receives all inputs and is required to guess the bit produced by Alice and Bob. Using the gap in the winning probabilities in the two and three party games we provide a very simple affine bound to the min-entropy of each round which is sufficient to bound an eavesdropper's knowledge of the sifted keys in the quantum key distribution protocol proposed in algorithm 1.

We exemplify our general framework with the magic square game, for which we provide a numerical bound on the maximal tripartite winning probability of about $\frac{8.00077}{9}$ which is close to the maximal classical bipartite winning probability of $\frac{8}{9}$. We use the NPA hierarchy to compute bounds on the min-entropy of Alice's bit using the tripartite winning probabilities (Section 5.2) of the magic square game. Further, we also use the the techniques from [45] to compute bounds on the respective von Neumann entropy (Section 5.3). Using a combination of the min- and von Neumann entropy bounds we provide a simple numerical construction for min-tradeoff functions suitable for the EAT/GEAT. We use these bounds to numerically optimize the finite and asymptotic key rates of our protocol using the magic square game as primitive, obtaining robustness up to roughly 2.88% in depolarizing noise —the highest tolerance reported for MSG based DIQKD.

Lastly, we remark that our proof of secrecy is mostly independent of our monogamy-of-entanglement framework and the subsequent choice of min-tradeoff function g. In fact, as can be inferred from Sections 4.4.2 and 4.4.4, any affine function $g : \mathcal{P}(\{0,1\}) \to \mathbb{R}$ satisfying Eq. (119) derived for a specific primitive may be substituted into Theorem 3 to yield a secrecy guarantee. In particular, the secrecy proof remains valid when considering games where the set of inputs in testing rounds differs from those in generation rounds, provided g is chosen appropriately. For example, [21, Eq. (28)] may be directly used in Eq. (27) to bound l_{key} when considering a DIQKD protocol based on the CHSH game where Alice always produces inputs in $\{0,1\}$ whereas Bob produces $\{0,1\}$ in generation rounds but $\{2,3\}$ in testing rounds.

Acknowledgements

We would like to thank Armando Bellante for early discussions on this work, as well as Mario Berta, Christian Boghiu, Peter Brown and Javier Rivera-Dean for tips on the usage of the ncpol2sdpa python library. We are additionally grateful to Ernest Y.-Z. Tan for valuable discussions and tips on entropy accumulation based proofs, and also Roberto Rubboli for useful comments on earlier versions of this manuscript. Lastly we thank Acharya Tejas and Ian George for pointing out a mistake in the original manuscript's calculation of the magic square game's QBER. E.C.M. and M.T. are funded by the National Research Foundation, Singapore and A*STAR under its CQT Bridging Grant. This research is also supported by the National Research Foundation, Singapore and A*STAR under its Quantum Engineering Programme (NRF2021-QEP2-01-P06).

References

[1] Jonathan Barrett, Lucien Hardy, and Adrian Kent. "No signaling and quantum key distribution". Phys. Rev. Lett. **95**, 010503 (2005).

[2] Antonio Acín, Serge Massar, and Stefano Pironio. "Efficient quantum key distribution secure against no-signalling eavesdroppers". New Journal of Physics **8**, 126–126 (2006).

[3] Reinhard F. Werner. "An application of bell's inequalities to a quantum state extension problem". Letters in Mathematical Physics **17**, 359–363 (1989).

[4] Andrew C. Doherty, Pablo A. Parrilo, and Federico M. Spedalieri. "Complete family of separability criteria". Phys. Rev. A **69**, 022308 (2004).

[5] Renato Renner. "Security of quantum key distribution". PhD thesis. ETH Zurich. (2006). url: arxiv.org/abs/quant-ph/0512258.

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

[7] Marco Tomamichel, Roger Colbeck, and Renato Renner. "A fully quantum asymptotic equipartition property". IEEE Transactions on Information Theory **55**, 5840–5847 (2009).

[8] Frédéric Dupuis, Omar Fawzi, and Renato Renner. "Entropy accumulation". Communications in Mathematical Physics **379**, 867–913 (2020).

[9] Frédéric Dupuis and Omar Fawzi. "Entropy accumulation with improved second-order term". IEEE Transactions on Information Theory **65**, 7596–7612 (2019).

[10] Tony Metger, Omar Fawzi, David Sutter, and Renato Renner. "Generalised entropy accumulation". 2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)Pages 844–850 (2022).

[11] Ernest Y. Z. Tan. "Prospects for device-independent quantum key distribution". PhD thesis. ETH Zurich. (2021). url: arxiv.org/abs/2111.11769.

[12] Valerio Scarani and Renato Renner. "Security bounds for quantum cryptography with finite resources". In Theory of Quantum Computation, Communication, and Cryptography. Pages 83–95. Berlin, Heidelberg (2008). Springer Berlin Heidelberg.

[13] Lana Sheridan, Thinh Phuc Le, and Valerio Scarani. "Finite-key security against coherent attacks in quantum key distribution". New Journal of Physics **12**, 123019 (2010).

[14] Marco Tomamichel, Charles C.-W. Lim, Nicolas Gisin, and Renato Renner. "Tight finite-key analysis for quantum cryptography". Nature Communications **3** (2012).

[15] Marco Tomamichel, Serge Fehr, Jędrzej Kaniewski, and Stephanie Wehner. "A monogamy-of-entanglement game with applications to device-independent quantum cryptography". New Journal of Physics **15**, 103002 (2013).

[16] Umesh Vazirani and Thomas Vidick. "Fully device-independent quantum key distribution". Physical Review Letters **113** (2014).

[17] Rotem Arnon-Friedman, Frédéric Dupuis, Omar Fawzi, Renato Renner, and Thomas Vidick. "Practical device-independent quantum cryptography via entropy accumulation". Nature Communications **9**, 459 (2018).

[18] Rotem Arnon-Friedman, Renato Renner, and Thomas Vidick. "Simple and tight device-independent security proofs". SIAM Journal on Computing **48**, 181–225 (2019).

[19] Ernest Y.-Z. Tan, René Schwonnek, Koon Tong Goh, Ignatius William Primaatmaja, and Charles C.-W. Lim. "Computing secure key rates for quantum cryptography with untrusted devices". npj Quantum Information **7** (2021).

[20] René Schwonnek, Koon Tong Goh, Ignatius W. Primaatmaja, Ernest Y.-Z. Tan, Ramona Wolf, Valerio Scarani, and Charles C.-W. Lim. "Device-independent quantum key distribution with random key basis". Nature Communications **12** (2021).

[21] Ernest Y.-Z. Tan, Pavel Sekatski, Jean-Daniel Bancal, René Schwonnek, Renato Renner, Nicolas Sangouard, and Charles C.-W. Lim. "Improved DIQKD protocols with finite-size analysis". Quantum **6**, 880 (2022).

[22] D. P. Nadlinger, P. Drmota, B. C. Nichol, G. Araneda, D. Main, R. Srinivas, D. M. Lucas, C. J. Ballance, K. Ivanov, E. Y.-Z. Tan, P. Sekatski, R. L. Urbanke, R. Renner, N. Sangouard, and J.-D. Bancal. "Experimental quantum key distribution certified by bell's theorem". Nature **607**, 682–686 (2022).

[23] Tony Metger and Renato Renner. "Security of quantum key distribution from generalised entropy accumulation". Nature Communications **14**, 5272 (2023).

[24] Stefano Pirandola, Ulrik L. Andersen, Leonardo Banchi, Mario Berta, Darius Bunandar, Roger Colbeck, Dirk Englund, Tobias Gehring, Cosmo Lupo, Carlo Ottaviani, Jason L. Pereira, Mohsen Razavi, Jesni Shamsul Shaari, Marco Tomamichel, Vladyslav C. Usenko, Giuseppe Vallone, Paolo Villoresi, and Petros Wallden. "Advances in quantum cryptography". Advances in Optics and Photonics **12**, 1012 (2020).

[25] Víctor Zapatero, Tim van Leent, Rotem Arnon-Friedman, Wen-Zhao Liu, Qiang Zhang, Harald Weinfurter, and Marcos Curty. "Advances in device-independent quantum key distribution". npj Quantum Information **9** (2023).

[26] Ignatius W. Primaatmaja, Koon Tong Goh, Ernest Y.-Z. Tan, John T.-F. Khoo, Shouvik Ghorai, and Charles C.-W. Lim. "Security of device-independent quantum key distribution protocols: a review". Quantum **7**, 932 (2023).

[27] Tim Zhang, Weiand van Leent, Kai Redeker, Robert Garthoff, René Schwonnek, Florian Fertig, Sebastian Eppelt, Wenjamin Rosenfeld, Valerio Scarani, Charles C.-W. Lim, and Harald Weinfurter. "A device-independent quantum key distribution system for distant users". Nature **607**, 687–691 (2022).

[28] Thomas Vidick. "Parallel diqkd from parallel repetition" (2017). arXiv:1703.08508.

[29] Rahul Jain, Carl A. Miller, and Yaoyun Shi. "Parallel device-independent quantum key distribution". IEEE Transactions on Information Theory **66**, 5567–5584 (2020).

[30] Rahul Jain and Srijita Kundu. "A direct product theorem for quantum communication complexity with applications to device-independent cryptography" (2023). arXiv:2106.04299.

[31] Xingyao Wu, Jean-Daniel Bancal, Matthew McKague, and Valerio Scarani. "Device-independent parallel self-testing of two singlets". Physical Review A **93** (2016).

[32] Eric Culf and Thomas Vidick. "A monogamy-of-entanglement game for subspace coset states". Quantum **6**, 791 (2022).

[33] Eric Culf, Thomas Vidick, and Victor V. Albert. "Group coset monogamy games and an application to device-independent continuous-variable qkd" (2022). arXiv:2212.03935v15.

[34] Damián Pitalúa-García and Iordanis Kerenidis. "Practical and unconditionally secure spacetime-constrained oblivious transfer". Physical Review A**98** (2018).

[35] Andrea Coladangelo, Jiahui Liu, Qipeng Liu, and Mark Zhandry. "Hidden cosets and applications to unclonable cryptography". In Advances in Cryptology – CRYPTO 2021. Pages 556–584. Springer International Publishing (2021).

[36] Srijita Kundu and Ernest Y. Z. Tan. "Device-independent uncloneable encryption" (2023). arXiv:2210.01058.

[37] Stefano Pironio, Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, and Valerio Scarani. "Device-independent quantum key distribution secure against collective attacks". New Journal of Physics **11**, 045021 (2009).

[38] Pavel Sekatski, Jean-Daniel Bancal, Xavier Valcarce, Ernest Y.-Z. Tan, Renato Renner, and Nicolas Sangouard. "Device-independent quantum key distribution from generalized CHSH inequalities". Quantum **5**, 444 (2021).

[39] Carl A. Miller and Yaoyun Shi. "Robust protocols for securely expanding randomness and distributing keys using untrusted quantum devices". J. ACM **63** (2016).

[40] N. David Mermin. "Simple unified form for the major no-hidden-variables theorems". Phys. Rev. Lett. **65**, 3373–3376 (1990).

[41] Asher Peres. "Incompatible results of quantum measurements". Physics Letters A **151**, 107–108 (1990).

[42] Miguel Navascués, Stefano Pironio, and Antonio Acín. "A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations". New Journal of Physics **10**, 073013 (2008).

[43] Stefano Pironio, Miguel Navascués, and Antonio Acín. "Convergent relaxations of polynomial optimization problems with noncommuting variables". SIAM Journal on Optimization **20**, 2157–2180 (2010).

[44] Peter Wittek. "Algorithm 950". ACM Transactions on Mathematical Software **41**, 1–12 (2015).

[45] Peter Brown, Hamza Fawzi, and Omar Fawzi. "Device-independent lower bounds on the conditional von neumann entropy". Quantum **8**, 1445 (2024).

[46] Yi-Zheng Zhen, Yingqiu Mao, Yu-Zhe Zhang, Feihu Xu, and Barry C. Sanders. "Device-independent quantum key distribution based on the mermin-peres magic square game". Phys. Rev. Lett. **131**, 080801 (2023).

[47] Carlos Palazuelos and Thomas Vidick. "Survey on nonlocal games and operator space theory". Journal of Mathematical Physics **57**, 015220 (2016).

[48] Lluís Masanes, Renato Renner, Matthias Christandl, Andreas Winter, and Jonathan Barrett. "Full security of quantum key distribution from no-signaling constraints". IEEE Transactions on Information Theory **60**, 4973–4986 (2014).

[49] Renato Renner and Stefan Wolf. "The exact price for unconditionally secure asymmetric cryptography". In Advances in Cryptology - EUROCRYPT 2004. Pages 109–125. Berlin, Heidelberg (2004). Springer Berlin Heidelberg.

[50] Dodis, Yevgeniy and Wichs, Daniel. "Non-malleable extractors and symmetric key cryptography from weak secrets". In Proceedings forty-first annual acm symposium on theory computing. Page 601–610. New York, NY, USA (2009). Association for Computing Machinery.

[51] Christopher Portmann and Renato Renner. "Cryptographic security of quantum key distribution" (2014). arXiv:1409.3525.

[52] Joseph M. Renes and Renato Renner. "One-shot classical data compression with quantum side information and the distillation of common randomness or secret keys". IEEE Transactions on Information Theory **58**, 1985–1991 (2012).

[53] Marco Tomamichel, Jesus Martinez-Mateo, Christoph Pacher, and David Elkouss. "Fundamental finite key limits for one-way information reconciliation in quantum key distribution". Quantum Information Processing **16** (2017).

[54] Igor Devetak and Andreas Winter. "Distillation of secret key and entanglement from quantum states". Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **461**, 207–235 (2005).

[55] Enrique Cervero-Martín. "Python script for obtaining tripartite winning probabilities, and finite and asymptotic keyrates". `https://github.com/EnriqueCerv/NLG_DI_QKD.git` (2023).

[56] Ben Toner. "Monogamy of non-local quantum correlations". Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences **465**, 59–69 (2008).

[57] Marco Tomamichel. "Quantum information processing with finite resources". Springer International Publishing. (2016).

[58] Michael Mitzenmacher and Eli Upfal. "Probability and computing: Randomized algorithms and probabilistic analysis". Cambridge University Press. USA (2005).

A Simplifying $\omega_{\mathrm{Q}}(\mathrm{MSG}_3)$

In this appendix we provide a simplification to the objective function in the optimization problems for the tripartite magic square game in Eq. (174) which we used to compute the numerical results in Theorem 4 and Figure 6.

Recall the optimization problem

$$\omega_{\mathrm{Q}}(\mathrm{MSG}_3) = \sup_{\mathcal{S}} \frac{1}{9} \sum_{x,y} \langle\phi| \Pi^{xy} |\phi\rangle \,, \tag{198}$$

where

$$\Pi^{xy} := \sum_{c\in\{0,1\}} \left[F_c^{xy} \otimes \sum_{a\in\mathcal{A}:a[y]=c} P_a^x \otimes \sum_{b\in\mathcal{B}:b[x]=c} Q_b^y \right]. \tag{199}$$

We begin by providing a simplified form of Eq. (199). Let

$$P_{000}^x = \mathbb{I}_{Q_A} - P_{011}^x - P_{101}^x - P_{110}^x, \tag{200}$$
$$Q_{111}^y = \mathbb{I}_{Q_B} - Q_{001}^y - Q_{010}^y - Q_{100}^y, \tag{201}$$
$$F_1^{xy} = \mathbb{I}_{Q_C} - F_0^{xy} \tag{202}$$

for all $x, y \in \{0, 1, 2\}$. A straightforward calculation then shows that Eq. (199) reduces to

$$\Pi^{xy} = \sum_{a:a[y]=1} \sum_{b:b[x]=0} \left[\frac{1}{2} F_0^{xy} \otimes \mathbb{I}_{Q_A} \otimes Q_b^y + \frac{1}{2}(1 - F_0^{xy}) \otimes P_a^x \otimes \mathbb{I}_{Q_B} - \mathbb{I}_{Q_C} \otimes P_a^x \otimes Q_b^y \right]. \tag{203}$$

Now, let

$$\Pi_{AB}^{xy} := \frac{1}{9} \sum_{c\in\{0,1\}} \mathbb{I}_{Q_C} \otimes \sum_{a\in\mathcal{A}:a[y]=c} P_a^x \otimes \sum_{b\in\mathcal{B}:b[x]=c} Q_b^y, \tag{204}$$

$$\Pi_{AC}^{xy} := \frac{1}{9} \sum_{c\in\{0,1\}} F_c^{xy} \otimes \sum_{a\in\mathcal{A}:a[y]=c} P_a^x \otimes \mathbb{I}_{Q_B}, \tag{205}$$

$$\Pi_{BC}^{xy} := \frac{1}{9} \sum_{c\in\{0,1\}} F_c^{xy} \otimes \mathbb{I}_{Q_A} \otimes \sum_{b\in\mathcal{B}:b[x]=c} Q_b^y. \tag{206}$$

Without changing the optimum we add the following constraints to the optimization problem in Eq. (198):

$$\langle\phi| \sum_{xy} \Pi_{AB}^{xy} |\phi\rangle \geq \frac{8}{9}, \tag{207}$$

$$\langle\phi| \sum_{xy} \Pi_{AC}^{xy} |\phi\rangle \geq \frac{8}{9}, \tag{208}$$

$$\langle\phi| \sum_{xy} \Pi_{BC}^{xy} |\phi\rangle \geq \frac{8}{9}. \tag{209}$$

Indeed, since the classical value of MSG_3 is $\frac{8}{9}$, we expect each pair of parties to succeed with probability at least $\frac{8}{9}$ when using a quantum strategy.

Applying the NPA hierarchy to the optimization problem in Eq. (198) with the simplified expression in Eq. (199) and the additional constraints from Eq. (207)-(209) yields the approximate value of $\frac{8.00077}{9}$ reported in Theorem 4 (see the code in supplemental material [55]). We found that these heuristical changes significantly improved the value output by the NPA hierarchy. We used a mixed relaxation of the hierarchy, combining level 2 and two thirds of the monomials of the form $P \otimes Q \otimes F$ (which were themselves picked arbitrarily by selecting two out of every three in the list $[P, Q, F]_{P,Q,F}$ in order).

Lastly, we remark that the constraints in Eq. (208) and (209) need to be removed when optimizing the constrained problem in Eq. (176) to generate Figure 6.