A monogamy-of-entanglement game with applications to device-independent quantum cryptography

2013 New J. Phys. 15 103002

(http://iopscience.iop.org/1367-2630/15/10/103002)

New Journal of Physics
The open access journal for physics

A monogamy-of-entanglement game with applications to device-independent quantum cryptography

Marco Tomamichel[1,3], **Serge Fehr**[2,3], **Jędrzej Kaniewski**[1] **and Stephanie Wehner**[1]

[1] Centre for Quantum Technologies (CQT), National University of Singapore, Singapore
[2] Centrum Wiskunde and Informatica (CWI), Amsterdam, The Netherlands
E-mail: cqtmarco@nus.edu.sg and serge.fehr@cwi.nl

New Journal of Physics **15** (2013) 103002 (24pp)
Received 29 May 2013
Published 2 October 2013
Online at http://www.njp.org/
doi:10.1088/1367-2630/15/10/103002

Abstract. We consider a game in which two separate laboratories collaborate to prepare a quantum system and are then asked to guess the outcome of a measurement performed by a third party in a random basis on that system. Intuitively, by the uncertainty principle and the monogamy of entanglement, the probability that *both* players simultaneously succeed in guessing the outcome correctly is bounded. We are interested in the question of how the success probability scales when many such games are performed in parallel. We show that any strategy that maximizes the probability to win every game individually is also optimal for the parallel repetition of the game. Our result implies that the optimal guessing probability can be achieved without the use of entanglement. We explore several applications of this result. Firstly, we show that it implies security for standard BB84 quantum key distribution when the receiving party uses *fully untrusted measurement devices*, i.e. we show that BB84 is one-sided device independent. Secondly, we show how our result can be used to prove

[3] Authors to whom any correspondence should be addressed.

security of a one-round position-verification scheme. Finally, we generalize a well-known uncertainty relation for the guessing probability to quantum side information.

Contents

1. Introduction

Apart from their obvious entertainment value, games among multiple (competing) players often provide an intuitive way to understand complex problems. For example, we may understand Bell inequalities in physics [4], or interactive proofs in computer science [5], as a game played by a referee against multiple provers [16, 21]. Here we investigate a simple quantum multiplayer game whose analysis enables us to tackle several open questions in quantum cryptography.

1.1. Monogamy game

We consider a game played among three parties: Alice, Bob and Charlie (these players should be seen as operating in three different laboratories). In this game, Alice takes the role of a referee and is assumed to be honest whereas Bob and Charlie form a team determined to beat Alice. A monogamy-of-entanglement game G consists of a list of measurements, $\mathcal{M}^\theta = \{F_x^\theta\}_{x\in\mathcal{X}}$, indexed by $\theta \in \Theta$, on a d-dimensional quantum system.

Preparation phase. Bob and Charlie agree on a *strategy* and prepare an arbitrary quantum state ρ_{ABC}, where ρ_A has dimension d. They pass ρ_A to Alice and hold on to ρ_B and ρ_C, respectively. After this phase, Bob and Charlie are no longer allowed to communicate.

Question phase. Alice chooses $\theta \in \Theta$ uniformly at random and measures ρ_A using $\mathcal{M}^\theta$ to obtain the *measurement outcome*, $x \in \mathcal{X}$. She then announces θ to Bob and Charlie.

Answer phase. Bob and Charlie independently form a guess of x by performing a measurement (which may depend on θ) on their respective shares of the quantum state.

Winning condition. The game is won if *both* Bob and Charlie guess x correctly.

From the perspective of classical information processing, our game may appear somewhat trivial—after all, if Bob and Charlie were to provide some classical information k to Alice who would merely apply a random function f_θ, they could predict the value of $x = f_\theta(k)$ perfectly from k and θ. In quantum mechanics, however, the well-known uncertainty principle [25] places a limit on how well observers can predict the outcome x of incompatible measurements.

To exemplify this, we will in the following focus on the game $\mathsf{G}_{\mathrm{BB84}}$ in which Alice measures a qubit in one of the two BB84 bases [7] to obtain a bit $x \in \{01\}$ and use $p_{\mathrm{win}}(\mathsf{G}_{\mathrm{BB84}})$ to denote the probability that Bob and Charlie win, maximized over all strategies. (A strategy is comprised of a tripartite state ρ_{ABC}, and, for each $\theta \in \Theta$, a measurement on B and a measurement on C.) Then, if Bob and Charlie are restricted to classical memory (i.e. they are not entangled with Alice), it is easy to see that they win the game with an (average) probability of at most $1/2 + 1/(2\sqrt{2}) \leqslant p_{\mathrm{win}}(\mathsf{G}_{\mathrm{BB84}})$.[4]

In a fully quantum world, however, uncertainty is not quite the end of the story as indeed Bob and Charlie are allowed to have a *quantum* memory. To illustrate the power of such a memory, consider the same game played just between Alice and Bob. As Einstein *et al* [19] famously observed. If ρ_{AB} is a maximally entangled state, then once Bob learns Alice's choice of measurement θ, he can perform an adequate measurement on his share of the state to obtain x himself. That is, there exists a strategy for Bob to guess x perfectly. Does this change when we add the extra player, Charlie? We can certainly be hopeful as it turns out that quantum entanglement is 'monogamous' [55] in the sense that the more entangled Bob is with Alice, the less entangled Charlie can be. In the extreme case where ρ_{AB} is maximally entangled, even if Bob can guess x perfectly every time, Charlie has to resort to making an uninformed random guess. As both of them have to be correct in order to win the game, this strategy turns out to be worse than optimal.

An analysis of this game thus requires a tightrope walk between uncertainty on the one hand, and the monogamy of entanglement on the other. The following result is a special case of our main result (which we explain further down); a slightly weaker bound had been derived in [14], and the exact value had first been proven by Christandl and Schuch [15][5].

- *Result (informal).* We find $p_{\mathrm{win}}(\mathsf{G}_{\mathrm{BB84}}) = 1/2 + 1/(2\sqrt{2}) \approx 0.85$. Moreover, this value can be achieved when Bob and Charlie have a classical memory only.

Interestingly, we thus see that monogamy of entanglement wins out entirely, canceling the power of Bob and Charlie's quantum memory—the optimal winning probability can be achieved without any entanglement at all. In fact, this strategy results in a higher success probability than the one in which Bob is maximally entangled with Alice and Charlie is classical. In such a case the winning probability can be shown to be at most $1/2$. In spirit, this result is similar to (but not implied by) recent results obtained in the study of non-local games where the addition of one or more extra parties cancels the advantage coming from the use of entanglement [29].

[4] For example, this follows from a proof of an entropic uncertainty relation by Deutsch [18].

[5] However, neither the techniques from [14] nor from [15] work for parallel repetitions.

To employ the monogamy game for quantum cryptographic purposes, we need to understand what happens if we play the same game $\mathsf{G}n$ times in parallel. The resulting game, $\mathsf{G}^{\times n}$, requires both Bob and Charlie to guess the entire *string* $x = x_1 \dots x_n$ of measurement outcomes, where x_j, $j \in [n]$, is generated by measuring ρ_{A_j} (ρ_{A_j} is the quantum state provided by Bob and Charlie in the jth round of the game) in the basis $\mathcal{M}^{\theta_j}$, and $\theta_j \in \Theta$ is chosen uniformly at random. Strategies for Bob and Charlie are then determined by the state $\rho_{A_1 \dots A_n BC}$ (with each A_j being d-dimensional) as well as independent measurements on B and C that produce a guess of the string x, for each value of $\theta = \theta_1 \dots \theta_n \in \Theta^n$. In the following, we say that a game satisfies *parallel repetition* if $p_{\text{win}}(\mathsf{G}^{\times n})$ drops exponentially in n. Moreover, we say that it satisfies *strong parallel repetition* if this exponential drop is maximally fast, i.e. if $p_{\text{win}}(\mathsf{G}^{\times n}) = p_{\text{win}}(\mathsf{G})^n$.

Returning to our example, Bob and Charlie could repeat the strategy that is optimal for a single round n times to achieve a winning probability of $p_{\text{win}}(\mathsf{G}_{\text{BB84}})^n = (1/2 + 1/(2\sqrt{2}))^n \leqslant p_{\text{win}}(\mathsf{G}_{\text{BB84}}^{\times n})$, but is this really the best they can do? Even classically, analyzing the n-fold parallel repetition of games or tasks is typically challenging. Examples include the parallel repetition of interactive proof systems (see e.g. [26, 48]) or the analysis of communication complexity tasks (see e.g. [33]). In a quantum world, such an analysis is often exacerbated further by the presence of entanglement and the fact that quantum information cannot generally be copied. Famous examples include the analysis of the 'parallel repetition' of channels in quantum information theory (where the problem is referred to as the additivity of capacities) (see e.g. [24, 54]), entangled non-local games [30], or the question whether an eavesdropper's optimal strategy in quantum key distribution (QKD) is to perform the optimal strategy for each round. Fortunately, it turns out that strong parallel repetition does hold for our monogamy game.

- *Main result (informal).* We find $p_{\text{win}}(\mathsf{G}_{\text{BB84}}^{\times n}) = (1/2 + 1/(2\sqrt{2}))^n$. More generally, for all monogamy-of-entanglement games using incompatible measurements, we find that $p_{\text{win}}(\mathsf{G}^{\times n})$ decreases exponentially in n. This also holds in the approximate case where Bob and Charlie are allowed to make a small fraction of errors.

Our proofs are appealing in their simplicity and use only tools from linear algebra, inspired by techniques proposed by Kittaneh [32]. Note that, in the more general case, we obtain parallel repetition, albeit not strong parallel repetition.

1.2. Applications

1.2.1. One-sided device independent quantum key distribution (QKD). QKD makes use of quantum mechanical effects to allow two parties, Alice and Bob, to exchange a secret key while being eavesdropped by an attacker Eve [7, 20]. In principle, the security of QKD can be rigorously proven based solely on the laws of quantum mechanics [45, 50, 53]; in particular, the security does not rely on the assumed hardness of some computational problem. However, these security proofs typically make stringent assumptions about the devices used by Alice and Bob to prepare and measure the quantum states that are communicated. These assumptions are not necessarily satisfied by real-world devices, leaving the implementations of QKD schemes open to hacking attacks [40].

One way to counter this problem is by protecting the devices in an ad hoc manner against known attacks. This is somewhat unsatisfactory in that the implementation may still

be vulnerable to *unknown* attacks, and the fact that the scheme is in principle provably secure loses a lot of its significance.

Another approach is to try to remove the assumptions on the devices necessary for the security proof; this leads to the notion of *device-independent* (DI) QKD. This line of research can be traced back to Mayers and Yao [46] (see also [1, 2]). After some limited results (see e.g. [23, 44]), the possibility of DI QKD has recently been shown in the most general case by Reichardt *et al* in [49] and by Vazirani and Vidick in [61]. In a typical DI QKD scheme, Alice and Bob check if the classical data obtained from the quantum communication violates a Bell inequality, which in turn ensures that there is some amount of fresh randomness in the data that cannot be known by Eve. This can then be transformed into a secret key using standard cryptographic techniques like information reconciliation and randomness extraction.

While this argument shows that DI QKD is theoretically possible, the disadvantage of such schemes is that they require a *long-distance detection-loophole-free* violation of a Bell inequality by Alice and Bob. This makes fully DI QKD schemes very hard to implement and very sensitive to any kind of noise and to inefficiencies of the physical devices: any deficiency will result in a lower observed (loophole free) Bell inequality violation, and currently conceivable experimental parameters are insufficient to provide provable security. Trying to find ways around this problem is an active line of research, see e.g. [10, 22, 37, 39, 47].

Here, we follow a somewhat different approach, not relying on Bell tests, but making use of the *monogamy of entanglement*. Informally, the latter states that if Alice's state is fully entangled with Bob's, then it cannot be entangled with Eve's, and vice versa. As a consequence, if Alice measures a quantum system by randomly choosing one of two incompatible measurements, it is impossible for Bob and Eve to *both* have low entropy about Alice's measurement outcome. Thus, if one can verify that Bob has low entropy about Alice's measurement during the run of the scheme, it is guaranteed that Eve's entropy is high, and thus that a secret key can be distilled.

Based on this idea, we show that the standard BB84 QKD scheme [7] is *one-sided* DI. This means that only Alice's quantum device has to be trusted, but no assumption about Bob's measurement device has to be made in order to prove security. Beyond that it does not communicate the measurement outcome to Eve, Bob's measurement device may be arbitrarily malicious.

- *Application to QKD (informal).* We show that the BB84 QKD scheme is secure in the setting of fully one-sided device independence and provide a complete security analysis for finite key lengths.

One-sided DI security of BB84 was first claimed in [60]. However, a close inspection of their proof sketch, which is based on an entropic uncertainty relation with quantum side information, reveals that their arguments are insufficient to prove full one-sided DI security (as confirmed by the authors). It needs to be assumed that Bob's measurement device is *memoryless*. The same holds for the follow up work [9, 58] of [60].

Despite the practical motivation, our result is at this point of theoretical nature. This is because, as in all contemporary fully DI schemes, our analysis here (implicitly) assumes that every qubit sent by Alice is indeed received by Bob, or, more generally, whether it is received or not does not depend on the basis it is to be measured in; this is not necessarily satisfied in practical implementations—and some recent attacks on QKD take advantage of exactly this effect by blinding the detectors whenever a measurement in a basis not to Eve's liking is attempted [40]. We remark here that this unwanted assumption can be removed in principle

Table 1. Comparison of recent fully and partially DI security proofs for QKD.

	Reichardt *et al* [49]	Vazirani/Vidick [61]	This work	Tomamichel *et al* [59][a]
Protocol	E91-based [20]	E91-based	BBM92 [6]/BB84 [7]	Asymmetric BB84 [38]
Device assumptions	None	None	Trusted Alice[b]	Trusted Alice[b], memoryless Bob
Noise tolerance	0%	1.2%	1.5%	11%
Key rate (zero noise)	0%	2.5%	22.8%/11.4%[c]	1
Finite key analysis	No	No	Yes	Yes

[a] For comparison, this proof achieves maximum noise tolerance and key rate for BB84. See also [9].
[b] Combining our results with results on self-testing in [37, 57], one can reduce the assumption to memoryless for Alice.
[c] This loss of a factor $\frac{1}{2}$ is due to sifting when moving from BBM92 to BB84.

by a refined analysis along the lines of Branciard *et al* [9].[6] While this leads to a significantly lower key rate, the analysis in [9] suggests that the loss tolerance for one-sided DI QKD is higher than for fully DI QKD. More precisely, while DI QKD requires a detection-loophole-free violation of a Bell inequality, for one-sided DI QKD a loophole-free violation of a steering inequality is sufficient, and such a violation has recently been shown [63].

Our analysis of BB84 QKD with one-sided DI security admits a noise level of up to 1.5%. This is significantly lower than the 11% tolerable for standard (i.e. not DI) security. We believe that this is not inherent to the scheme but an artifact of our analysis. Improving this bound by means of a better analysis is an open problem (it *can* be slightly improved by using a better scheme, e.g. the six-state scheme [11]). Nonetheless, one-sided DI QKD appears to be an attractive alternative to DI QKD in an asymmetric setting, when we can expect from one party, say, a server, to invest in a very carefully designed, constructed and tested apparatus, but not the other party, the user, and/or in case of a star network with one designated link being connected with many other links.

A comparison to other recent results on DI QKD is given in table 1. The noise tolerance is determined using isotropic noise.

1.2.2. Position verification. Our second application is to the task of *position verification*. Here, we consider a one-dimensional setting where a *prover* wants to convince two *verifiers* that he controls a certain position, *pos*. The verifiers are located at known positions around *pos*, honest, and connected by secure communication channels. Moreover, all parties are assumed to have synchronized clocks, and the message delivery time between any two parties is assumed to be proportional to the distance between them. Finally, all local computations are assumed to be instantaneous.

Position verification and variants thereof (like *distance bounding*) is a rather well-studied problem in the field of wireless security (see e.g. [14]). It was shown in [14] that in the presence of colluding adversaries at different locations, position verification is impossible classically, even with computational hardness assumptions. That is, the prover can always trick the verifiers into believing that he controls a position. The fact that the classical attack requires the adversary

[6] There, the protocol of [59] was amended to account for photon losses.

to *copy* information, initially gave hope that we may circumvent the impossibility result using quantum communication [13, 31, 42, 43]. However, such schemes were subsequently broken [36] and indeed a general impossibility proof holds [12]: without any restriction on the adversaries, in particular on the amount of pre-shared entanglement they may hold, no quantum scheme for position verification can be secure. This impossibility proof was constructive but required the dishonest parties to share a number of Einstein–Podolsky–Rosen (EPR) pairs [19] that grows doubly exponentially in the number of qubits the honest parties exchange. Using port-based teleportation, as introduced by Ishizaka and Hiroshima [27, 28], this was reduced by Beigi and König [3] to a single exponential amount. On the other hand, there are schemes for position verification that are provably secure against adversaries that have no pre-shared entanglement, or only hold a couple of entangled qubits [3, 12, 13, 36].

However, all known schemes that are provably secure with a negligible soundness error (the maximal probability that a coalition of adversaries can pass the position verification test for position *pos* without actually controlling that specific position) against adversaries with no or with bounded pre-shared entanglement are either *multi-round* schemes, or require the honest participants to manipulate large quantum states.

- *Application to position verification (informal).* We present the first provably secure *one-round* position verification scheme with negligible soundness error in which the honest parties are only required to perform single qubit operations. We prove its security against adversaries with an amount of pre-shared entanglement that is *linear* in the number of qubits transmitted by the honest parties.

1.2.3. Entropic uncertainty relation. The final application of our monogamy game is to entropic uncertainty relations with quantum side information [8]. Our result is in the spirit of [17, 60] which shows an uncertainty relation for a tripartite state ρ_{ABC} for measurements on A, trading off the uncertainty between the two observers B and C as in our monogamy game.

- *Application to entropic uncertainty relations.* For any two general (positive operator valued measure (POVM)) measurements, $\{N_x^0\}_x$ and $\{N_x^1\}_x$, we find

$$H_{\min}(X|B\Theta)_\rho + H_{\min}(X|C\Theta)_\rho \geqslant -2\log\frac{1+\sqrt{c}}{2}, \quad \text{where} \quad c = \max_{x,z}\left\|\sqrt{N_x^0}\sqrt{N_z^1}\right\|^2.$$

  The entropies are evaluated for the post-measurement state $\rho_{XBC\Theta}$, where X is the outcome of the measurement $\{N_x^\theta\}_x$, where $\Theta \in \{0, 1\}$ is chosen uniformly at random.

1.3. Outline

The remainder of this paper is structured as follows. In section 2, we introduce the basic terminology and notation used throughout this work. In section 3, we discuss the monogamy game and prove a strong parallel repetition theorem. Here, we also generalize the game to include the case where Bob and Charlie are allowed to have some errors in their guess and show an upper bound on the winning probability for the generalized game. Sections 4–6 then apply these results to prove security for one-sided DI QKD, a one-round position verification scheme and an entropic uncertainty relation.

2. Technical preliminaries

2.1. Basic notation and terminology

Let $\mathcal{H}$ be an arbitrary, finite dimensional Hilbert space. $\mathcal{L}(\mathcal{H})$ and $\mathcal{P}(\mathcal{H})$ denote *linear* and *positive semi-definite* operators on $\mathcal{H}$, respectively. Note that an operator $A \in \mathcal{P}(\mathcal{H})$ is in particular *Hermitian*, meaning that $A^\dagger = A$. The set of *density operators* on $\mathcal{H}$, i.e. the set of operators in $\mathcal{P}(\mathcal{H})$ with unit trace, is denoted by $\mathcal{S}(\mathcal{H})$. For $A, B \in \mathcal{L}(\mathcal{H})$, we write $A \geqslant B$ to express that $A - B \in \mathcal{P}(\mathcal{H})$. When operators are compared with scalars, we implicitly assume that the scalars are multiplied by the identity operator, which we denote by $1_\mathcal{H}$, or 1 if $\mathcal{H}$ is clear from the context. A *projector* is an operator $P \in \mathcal{P}(\mathcal{H})$ that satisfies $P^2 = P$. A *POVM* (short for *positive operator valued measure*) is a set $\{N_x\}_x$ of operators $N_x \in \mathcal{P}(\mathcal{H})$ such that $\sum_x N_x = 1$, and a POVM is called *projective* if all its elements N_x are projectors. We use the *trace distance*

$$\Delta(\rho, \sigma) := \max_{0 \leqslant E \leqslant 1} \mathrm{tr}(E(\rho - \sigma)) = \tfrac{1}{2}\mathrm{tr}|\rho - \sigma|, \quad \text{where } |L| = \sqrt{L^\dagger L}$$

as a metric on density operators $\rho, \sigma \in \mathcal{S}(\mathcal{H})$.

The most prominent example of a Hilbert space is the qubit, $\mathcal{H} \equiv \mathbb{C}^2$. The vectors $|0\rangle$ and $|1\rangle$ form its *rectilinear* (or computational) basis, and the vectors $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ form its *diagonal* (or Hadamard) basis, where H denotes the Hadamard matrix. More generally, we often consider systems composed of n qubits, $\mathcal{H} \equiv \mathbb{C}^2 \otimes \cdots \otimes \mathbb{C}^2$. For $x, \theta \in \{0, 1\}^n$, we write $|x^\theta\rangle$ as a shorthand for the state vector $H^{\theta_1}|x_1\rangle \otimes \cdots \otimes H^{\theta_n}|x_n\rangle \in \mathcal{H}$.

2.2. The Schatten ∞-norm

For $L \in \mathcal{L}(\mathcal{H})$, we use the Schatten ∞-norm $\|L\| := \|L\|_\infty = s_1(L)$, which evaluates the largest singular value of L. It is easy to verify that this norm satisfies $\|L\|^2 = \| L^\dagger L \| = \| LL^\dagger \|$. Also, for $A, B \in \mathcal{P}(\mathcal{H})$, $\| A \|$ coincides the largest eigenvalue of A, and $A \leqslant B$ implies $\|A\| \leqslant \|B\|$. Finally, for block-diagonal operators we have $\|A \oplus B\| = \max\{\|A\|, \|B\|\}$. We will also need the following norm inequality.

Lemma 1 *Let $A, B, L \in \mathcal{L}(\mathcal{H})$ such that $A^\dagger A \geqslant B^\dagger B$. Then, it holds that $\| AL \| \geqslant \| BL \|$.*

Proof. First, note that $A^\dagger A \geqslant B^\dagger B$ implies that $L^\dagger A^\dagger A L \geqslant L^\dagger B^\dagger B L$ holds for an arbitrary linear operator L. By taking the norm we arrive at $\|L^\dagger A^\dagger A L\| \geqslant \|L^\dagger B^\dagger B L\|$, which is equivalent to $\|AL\| \geqslant \|BL\|$. □

In particular, if $A, A', B, B' \in \mathcal{P}(\mathcal{H})$ satisfy $A' \geqslant A$ and $B' \geqslant B$ then applying the lemma twice (to the square roots of these operators) gives $\|\sqrt{A'}\sqrt{B'}\| \geqslant \|\sqrt{A'}\sqrt{B}\| \geqslant \|\sqrt{A}\sqrt{B}\|$. For projectors the square roots can be omitted.

One of our main tools is the following lemma 2, which bounds the Schatten norm of the sum of n positive semi-definite operators by means of their pairwise products. We derive the bound using a construction due to Kittaneh [32], which was also used by Schaffner [52] to derive a similar, but less general, result.

We call two permutations $\pi : [N] \to [N]$ and $\pi' : [N] \to [N]$ of the set $[N] := \{1, \ldots, N\}$ *orthogonal* if $\pi(i) \neq \pi'(i)$ for all $i \in [N]$. There always exists a set of N permutations of $[N]$ that are mutually orthogonal (for instance the N cyclic shifts).

Lemma 2 *Let $A_1, A_2, \ldots, A_N \in \mathcal{P}(\mathcal{H})$, and let $\{\pi^k\}_{k\in[N]}$ be a set of N mutually orthogonal permutations of $[N]$. Then*

$$\left\| \sum_{i\in[N]} A_i \right\| \leqslant \sum_{k\in[N]} \max_{i\in[N]} \left\| \sqrt{A_i}\sqrt{A_{\pi^k(i)}} \right\| . \tag{1}$$

Proof. We define $X = [X_{ij}]$ as the $N \times N$ block-matrix with blocks given by $X_{ij} = \delta_{j1}\sqrt{A_i}$. Then, the matrices $X^\dagger X$ and $XX^\dagger$ are easy to evaluate, namely, $(X^\dagger X)_{ij} = \delta_{i1}\delta_{j1}\sum_i A_i$, as well as $XX^\dagger$ and $(XX^\dagger)_{ij} = \sqrt{A_i}\sqrt{A_j}$. We have

$$\left\| \sum_{i\in[N]} A_i \right\| = \|X^\dagger X\| = \|XX^\dagger\| .$$

Next, we decompose $XX^\dagger = D_1 + D_2 + \cdots + D_N$, where the matrices D_k are defined by the permutations π^k, respectively, as $(D_k)_{ij} = \delta_{j,\pi^k(i)}\sqrt{A_i}\sqrt{A_j}$. Note that the requirement that the permutations are mutually orthogonal ensures that $XX^\dagger = \sum_k D_k$. Moreover, since the matrices D_k are constructed such that they contain exactly one non-zero block in each row and column, they can be transformed into a block-diagonal matrix

$$D'_k = \bigoplus_{i\in[N]} \sqrt{A_i}\,\sqrt{A_{\pi^k(i)}}$$

by a unitary rotation. Hence, using the triangle inequality and unitary invariance of the norm, we get $\|\sum_k A_k\| \leqslant \sum_k \|D_k\| = \sum_k \|D'_k\|$, which implies (1) since $\|\bigoplus_i L_i\| = \max_i \{\|L_i\|\}$. □

A special case of the lemma states that $\|A_1 + A_2\| \leqslant \max\{\|A_1\|, \|A_2\|\} + \|\sqrt{A_1}\sqrt{A_2}\|$.

2.3. Classical-quantum states and min-entropy

A state $\rho_{XB} \in \mathcal{S}(\mathcal{H}_X \otimes \mathcal{H}_B)$ is called a *classical-quantum* (CQ) state with classical X over $\mathcal{X}$, if it is of the form

$$\rho_{XB} = \sum_{x\in\mathcal{X}} p_x |x\rangle\langle x|_X \otimes \rho_B^x,$$

where $\{|x\rangle\}_{x\in\mathcal{X}}$ is a fixed basis of $\mathcal{H}_X$, $\{p_x\}_{x\in\mathcal{X}}$ is a probability distribution, and $\rho_B^x \in \mathcal{S}(\mathcal{H}_B)$. For such a state, X can be understood as a random variable that is correlated with (potentially quantum) side information B.

If $\lambda : \mathcal{X} \to \{0, 1\}$ is a predicate on $\mathcal{X}$, then we denote by $\Pr_\rho[\lambda(X)]$ the probability of the *event* $\lambda(X)$ under ρ; formally, $\Pr_\rho[\lambda(X)] = \sum_x p_x\,\lambda(x)$. We also define the state $\rho_{XB|\lambda(X)}$, which is the state of the X and B conditioned on the event $\lambda(X)$. Formally,

$$\rho_{XB|\lambda(X)} = \frac{1}{\Pr_\rho[\lambda(X)]} \sum_x p_x \lambda(x) |x\rangle\langle x|_X \otimes \rho_B^x.$$

For a CQ-state $\rho_{XB} \in \mathcal{S}(\mathcal{H}_X \otimes \mathcal{H}_B)$, the *min-entropy* of X conditioned on B [50] can be expressed in terms of the maximum probability that a measurement on B yields the correct value of X, i.e. the guessing probability. Formally, we define [34]

$$H_{\min}(X|B)_\rho := -\log p_{\text{guess}}(X|B)_\rho, \quad \text{where} \quad p_{\text{guess}}(X|B)_\rho := \max_{\{N_x\}_x} \sum_x p_x \operatorname{tr}(\rho_B^x N_x).$$

Here, the optimization is taken over all POVMs $\{N_x\}_x$ on B, and here and throughout this paper, log denotes the binary logarithm.

In case of a CQ-state $\rho_{XB\Theta}$ with classical X, and with additional classical side information Θ, we can write $\rho_{XB\Theta} = \sum_\theta p_\theta |\theta\rangle\langle\theta| \otimes \rho^\theta_{XB}$ for CQ states ρ^θ_{XB}. The min-entropy of X conditioned on B and Θ then evaluates to

$$H_{\min}(X|B\Theta)_\rho = -\log p_{\text{guess}}(X|B\Theta)_\rho, \quad \text{where} \quad p_{\text{guess}}(X|B\Theta)_\rho = \sum_\theta p_\theta \, p_{\text{guess}}(X|B)_{\rho^\theta}. \quad (2)$$

An intuitive explanation of the latter equality is that the optimal strategy to guess X simply chooses an optimal POVM on B depending on the value of Θ.

An overview of the min-entropy and its properties can be found in [50, 56]; we merely point out the *chain rule* here: for a CQ-state $\rho_{XB\Theta}$ with classical X and Y, where Y is over an arbitrary set $\mathcal{Y}$ with cardinality $|\mathcal{Y}|$, it holds that $H_{\min}(X|BY)_\rho \geqslant H_{\min}(X|B)_\rho - \log|\mathcal{Y}|$.

3. Parallel repetition of monogamy games

In this section, we investigate and show strong parallel repetition for the game G_{BB84}. Then, we generalize our analysis to allow arbitrary measurements for Alice and consider the situation where Bob and Charlie are allowed to make some errors. But to start with, we need some formal definitions.

Definition 1. *A monogamy-of-entanglement game* G *consists of a finite dimensional Hilbert space* $\mathcal{H}_A$ *and a list of measurements* $\mathcal{M}^\theta = \{F^\theta_x\}_{x\in\mathcal{X}}$ *on a* $\mathcal{H}_A$*, indexed by* $\theta \in \Theta$*, where* $\mathcal{X}$ *and* Θ *are finite sets.*

We typically use less bulky terminology and simply call G a *monogamy game*. Note that for any positive integer n, the n-fold *parallel repetition* of G, denoted as $\mathsf{G}^{\times n}$ and naturally specified by $\mathcal{H}_A^{\otimes n}$ and $\{F^{\theta_1}_{x_1} \otimes \cdots \otimes F^{\theta_n}_{x_n}\}_{x_1,\ldots,x_n}$ for $\theta_1, \ldots, \theta_n \in \Theta$, is again a monogamy game.

Definition 2. *We define a strategy* $\mathcal{S}$ *for a monogamy game* G *as a list*

$$\mathcal{S} = \{\rho_{ABC},\ P^\theta_x,\ Q^\theta_x\}_{\theta\in\Theta, x\in\mathcal{X}}, \quad (3)$$

where $\rho_{ABC} \in \mathcal{S}(\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$*, and* $\mathcal{H}_B$ *and* $\mathcal{H}_C$ *are arbitrary finite dimensional Hilbert spaces. Furthermore, for all* $\theta \in \Theta$*,* $\{P^\theta_x\}_{x\in\mathcal{X}}$ *and* $\{Q^\theta_x\}_{x\in\mathcal{X}}$ *are POVMs on* $\mathcal{H}_B$ *and* $\mathcal{H}_C$*, respectively. A strategy is called pure if the state* ρ_{ABC} *is pure and all the POVMs are projective.*

If $\mathcal{S}$ is a strategy for game G, then the n-fold parallel repetition of $\mathcal{S}$, which is naturally given, is a particular strategy for the parallel repetition $\mathsf{G}^{\times n}$; however, it is important to realize that there exist strategies for $\mathsf{G}^{\times n}$ that are not of this form. In general, a strategy $\mathcal{S}_n$ for $\mathsf{G}^{\times n}$ is given by an arbitrary state $\rho_{A_1\ldots A_n BC} \in \mathcal{S}(\mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ (with arbitrary $\mathcal{H}_B$ and $\mathcal{H}_C$) and by arbitrary POVM elements on $\mathcal{H}_B$ and $\mathcal{H}_C$, respectively not necessarily in product form.

The winning probability for a game G and a fixed strategy $\mathcal{S}$, denoted by $p_{\text{win}}(\mathsf{G}, \mathcal{S})$, is defined as the probability that the measurement outcomes of Alice, Bob and Charlie agree when Alice measures in the basis determined by a randomly chosen $\theta \in \Theta$ and Bob and Charlie apply their respective POVMs $\{P^\theta_x\}_x$ and $\{Q^\theta_x\}_x$. The optimal winning probability, $p_{\text{win}}(\mathsf{G})$, maximizes the winning probability over all strategies. The following makes this formal.

Definition 3. *The winning probability for a monogamy game* G *and a strategy* $\mathcal{S}$ *is defined as*

$$p_{\text{win}}(\mathsf{G}, \mathcal{S}) := \sum_{\theta\in\Theta} \frac{1}{|\Theta|}\text{tr}(\Pi^\theta \rho_{ABC}), \quad \textit{where} \quad \Pi^\theta := \sum_{x\in\mathcal{X}} F_x^\theta \otimes P_x^\theta \otimes Q_x^\theta. \tag{4}$$

The optimal winning probability is

$$p_{\text{win}}(\mathsf{G}) := \sup_{\mathcal{S}} p_{\text{win}}(\mathsf{G}, \mathcal{S}), \tag{5}$$

where the supremum is taken over all strategies $\mathcal{S}$ *for* G.

In fact, due to a standard purification argument and Neumark's dilation theorem, we can restrict the supremum to pure strategies (cf lemma 9 in appendix A).

3.1. Strong parallel repetition for G_{BB84}

We are particularly interested in the game G_{BB84} and its parallel repetition $\mathsf{G}_{\text{BB84}}^{\times n}$. The latter is given by $\mathcal{H}_A = (\mathbb{C}^2)^{\otimes n}$ and the projectors $F_x^\theta = |x^\theta\rangle\langle x^\theta| = H^{\theta_1}|x_1\rangle\langle x_1|H^{\theta_1} \otimes \cdots \otimes H^{\theta_n}|x_n\rangle\langle x_n|H^{\theta_n}$ for $\theta, x \in \{0,1\}^n$. The following is our main result.

Theorem 3 *For any* $n \in \mathbb{N}$, $n \geqslant 1$, *we have*

$$p_{\text{win}}(\mathsf{G}_{\text{BB84}}^{\times n}) = \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n. \tag{6}$$

Proof. We first show that this guessing probability can be achieved. For $n = 1$, consider the following strategy. Bob and Charlie prepare the state $|\phi\rangle := \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle$ and send it to Alice. Then, they guess that Alice measures outcome 0, independent of θ. Formally, this is the strategy $\mathcal{S}_1 = \{|\phi\rangle\langle\phi|, P_x^\theta = \delta_{x0}, Q_x^\theta = \delta_{x0}\}$. The optimal winning probability is thus bounded by the winning probability of this strategy

$$p_{\text{win}}(\mathsf{G}_{\text{BB84}}) \geqslant \left(\cos\frac{\pi}{8}\right)^2 = \frac{1}{2} + \frac{1}{2\sqrt{2}}$$

and the lower bound on p_{win} implied by equation (6) follows by repeating this simple strategy n times.

To show that this simple strategy is optimal, let us now fix an arbitrary, pure strategy $\mathcal{S}_n = \{\rho_{A_1\ldots A_n BC}, P_x^\theta, Q_x^\theta\}$. From the definition of the norm, we have $\text{tr}(M\rho_{ABC}) \leqslant \| M \|$ for any $M \geqslant 0$. Using this and lemma 2, we find

$$p_{\text{win}}(\mathsf{G}_{\text{BB84}}^{\times n}, \mathcal{S}_n) = \sum_\theta \frac{1}{2^n}\text{tr}(\Pi^\theta \rho_{A_1\ldots A_n BC}) \leqslant \frac{1}{2^n}\left\| \sum_\theta \Pi^\theta \right\| \leqslant \frac{1}{2^n}\sum_k \max_\theta \| \Pi^\theta \Pi^{\pi^k(\theta)} \|, \tag{7}$$

where the optimal permutations π^k are to be determined later. Hence, the problem is reduced to bounding the norms $\| \Pi^\theta \Pi^{\theta'} \|$, where $\theta' = \pi^k(\theta)$. The trivial upper bound on these norms, 1, leads to $p_{\text{win}}(\mathsf{G}_{\text{BB84}}^{\times n}, \mathcal{S}_n) \leqslant 1$. However, most of these norms are actually very small as we see below.

For fixed θ and k, we denote by $\mathcal{T}$ the set of indices where θ and θ' differ, by $\mathcal{T}^c$ its complement, and by t the Hamming distance between θ and θ' (hence, $t = |\mathcal{T}|$). We consider the projectors

$$\bar{P} = \sum_x |x_{\mathcal{T}}^\theta\rangle\langle x_{\mathcal{T}}^\theta| \otimes 1_{\mathcal{T}^c} \otimes P_x^\theta \otimes 1_C \quad \text{and} \quad \bar{Q} = \sum_x |x_{\mathcal{T}}^{\theta'}\rangle\langle x_{\mathcal{T}}^{\theta'}| \otimes 1_{\mathcal{T}^c} \otimes 1_B \otimes Q_x^{\theta'},$$

where $|x^\theta_{\mathcal{T}}\rangle$ is $|x^\theta\rangle$ restricted to the systems corresponding to rounds with index in $\mathcal{T}$, and $1_{\mathcal{T}^c}$ is the identity on the remaining systems.

Since $\Pi^\theta \leqslant \bar{P}$ and $\Pi^{\theta'} \leqslant \bar{Q}$, we can bound $\|\Pi^\theta \Pi^{\theta'}\|^2 \leqslant \|\bar{P}\bar{Q}\|^2 = \|\bar{P}\bar{Q}\bar{P}\|$ using lemma 1. Moreover, it turns out that the operator $\bar{P}\bar{Q}\bar{P}$ has a particularly simple form, namely

$$\begin{aligned}\bar{P}\bar{Q}\bar{P} &= \sum_{x,y,z} |x^\theta_{\mathcal{T}}\rangle\langle x^\theta_{\mathcal{T}}|y^{\theta'}_{\mathcal{T}}\rangle\langle y^{\theta'}_{\mathcal{T}}|z^\theta_{\mathcal{T}}\rangle\langle z^\theta_{\mathcal{T}}| \otimes 1_{\mathcal{T}^c} \otimes P^\theta_x P^\theta_z \otimes Q^{\theta'}_y \\ &= \sum_{x,y} |\langle x^\theta_{\mathcal{T}}|y^{\theta'}_{\mathcal{T}}\rangle|^2 \, |x^\theta_{\mathcal{T}}\rangle\langle x^\theta_{\mathcal{T}}| \otimes 1_{\mathcal{T}^c} \otimes P^\theta_x \otimes Q^{\theta'}_y \\ &= 2^{-t} \sum_x |x^\theta_{\mathcal{T}}\rangle\langle x^\theta_{\mathcal{T}}| \otimes 1_{\mathcal{T}^c} \otimes P^\theta_x \otimes 1_C,\end{aligned}$$

where we used that $P^\theta_x P^\theta_z = \delta_{xz} P^\theta_x$ and $|\langle x^\theta_{\mathcal{T}}|y^{\theta'}_{\mathcal{T}}\rangle|^2 = 2^{-t}$. The latter relation follows from the fact that the two bases are diagonal to each other on each qubit with index in $\mathcal{T}$. From this follows directly that $\|\bar{P}\bar{Q}\bar{P}\| = 2^{-t}$. Hence, we find $\|\Pi^\theta \Pi^{\theta'}\| \leqslant \sqrt{2^{-t}}$. Note that this bound is independent of the strategy and only depends on the Hamming distance between θ and θ'.

To minimize the upper bound in (7), we should choose permutations π^k that produce tuples $(\theta, \theta' = \pi^k(\theta))$ with the same Hamming distance as this means that the maximization is over a uniform set of elements. A complete mutually orthogonal set of permutations with this property is given by the bitwise XOR, $\pi^k(\theta) = \theta \oplus k$, where we interpret k as an element of $\{0,1\}^n$. Using this construction, we get exactly $\binom{n}{t}$ permutations that create pairs with Hamming distance t, and the bound in equation (7) evaluates to

$$p_{\text{win}}(\mathsf{G}^{\times n}_{\text{BB84}}, \mathcal{S}_n) \leqslant \frac{1}{2^n} \sum_k \max_\theta \|\Pi^\theta \Pi^{\pi^k(\theta)}\| \leqslant \frac{1}{2^n} \sum_{t=0}^{n} \binom{n}{t} \left(\frac{1}{\sqrt{2}}\right)^t = \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n.$$

Since this bound applies to all pure strategies, lemma 9 concludes the proof. □

3.2. *Arbitrary games, and imperfect guessing*

The above upper-bound techniques can be generalized to an arbitrary monogamy game, G, specified by an arbitrary finite dimensional Hilbert space $\mathcal{H}_A$ and arbitrary measurements $\{F^\theta_x\}_{x\in\mathcal{X}}$, indexed by $\theta \in \Theta$, and with arbitrary finite $\mathcal{X}$ and Θ. The only additional parameter relevant for the analysis is the *maximal overlap* of the measurements

$$c(\mathsf{G}) := \max_{\substack{\theta,\theta'\in\Theta \\ \theta\neq\theta'}} \max_{x,\,x'\in\mathcal{X}} \left\| \sqrt{F^\theta_x}\sqrt{F^{\theta'}_{x'}} \right\|^2,$$

which satisfies $1/|\mathcal{X}| \leqslant c(\mathsf{G}) \leqslant 1$ and $c(\mathsf{G}^{\times n}) = c(\mathsf{G})^n$. This is in accordance with the definition of the overlap as it appears in entropic uncertainty relations, e.g. in [35]. Note also that in the case of G_{BB84}, we have $c(\mathsf{G}_{\text{BB84}}) = \frac{1}{2}$.

In addition to considering arbitrary monogamy games, we also generalize theorem 3 to the case where Bob and Charlie are not required to guess the outcomes *perfectly* but are allowed to make some errors. The maximal winning probability in this case is defined as follows, where we employ an argument analogous to lemma 9 in order to restrict to pure strategies.

Definition 4. *Let $\mathcal{Q} = \{(\pi^q_B, \pi^q_C)\}_q$ be a set of pairs of permutations of $\mathcal{X}$, indexed by q, with the meaning that in order to win, Bob and Charlie's respective guesses for x must form a pair*

in $\{(\pi_B^q(x), \pi_C^q(x))\}_q$. *Then, the optimal winning probability of* G *with respect to* $\mathcal{Q}$ *is*

$$p_{\text{win}}(\mathsf{G};\,\mathcal{Q}) := \sup_{\mathcal{S}} \sum_{\theta\in\Theta} \frac{1}{|\Theta|}\text{tr}(A^\theta \rho_{ABC}) \quad \text{with} \quad A^\theta := \sum_{x\in\mathcal{X}} F_x^\theta \otimes \sum_q P^\theta_{\pi_B^q(x)} \otimes Q^\theta_{\pi_C^q(x)},$$

where the supremum is taken over all pure strategies $\mathcal{S}$ *for* G.

We find the following upper bound on the guessing probability, generalizing the upper bound on the optimal winning probability established in theorem 3.

Theorem 4. *For any positive* $n \in \mathbb{N}$, *we have*

$$p_{\text{win}}(\mathsf{G}^{\times n};\,\mathcal{Q}) \leqslant |\mathcal{Q}|\Big(\frac{1}{|\Theta|} + \frac{|\Theta|-1}{|\Theta|}\sqrt{c(\mathsf{G})}\Big)^n.$$

Recall that in case of G_{BB84}, we have $|\mathcal{Q}| = 1$, $|\Theta| = 2$, and $c(\mathsf{G}_{\text{BB84}}) = \frac{1}{2}$, leading to the bound stated in theorem 3.

Proof. We closely follow the proof of the upper bound in theorem 3. For any pure strategy $\mathcal{S}_n = \{\rho_{A_1\ldots A_n BC},\, P_x^\theta,\, Q_x^\theta\}$, we bound

$$\sum_\theta \frac{1}{|\Theta|^n}\text{tr}(A^\theta \rho_{A_1\ldots A_n BC}) \leqslant \frac{1}{|\Theta|^n}\Big\|\sum_\theta A^\theta\Big\| \leqslant \frac{1}{|\Theta|^n}\sum_q\sum_k \max_\theta \Big\|\sqrt{A_q^\theta}\sqrt{A_q^{\pi^k(\theta)}}\Big\|, \tag{8}$$

where we introduce $A_q^\theta := \sum_x \big(\bigotimes_{\ell=1}^n F_{x_\ell}^{\theta_\ell}\big) \otimes P^\theta_{\pi_B^q(x)} \otimes Q^\theta_{\pi_C^q(x)}$. We now fix θ and θ' and bound the norms $\|\sqrt{A_q^\theta}\sqrt{A_q^{\theta'}}\|$. Let $\mathcal{T}$ be the set of indices where θ and θ' differ. We choose

$$B = \sum_x \bigotimes_{\ell\in\mathcal{T}} F_{x_\ell}^{\theta_\ell} \otimes 1_{\mathcal{T}^c} \otimes P^\theta_{\pi_B^q(x)} \otimes 1_C \;\text{ and }\; C = \sum_x \bigotimes_{\ell\in\mathcal{T}} F_{x_\ell}^{\theta'_\ell} \otimes 1_{\mathcal{T}^c} \otimes 1_B \otimes Q^{\theta'}_{\pi_C^q(x)},$$

which satisfy $B \geqslant A_q^\theta$ and $C \geqslant A_q^{\theta'}$. Hence, from lemma 1 we obtain $\|\sqrt{A_q^\theta}\sqrt{A_q^{\theta'}}\| \leqslant \|\sqrt{B}\sqrt{C}\|$. We evaluate

$$\|\sqrt{B}\sqrt{C}\| = \Big\|\sum_{x,y}\bigotimes_{\ell\in\mathcal{T}}\sqrt{F_{x_\ell}^{\theta_\ell}}\sqrt{F_{y_\ell}^{\theta'_\ell}} \otimes 1_{\mathcal{T}^c} \otimes P^\theta_{\pi_B^q(x)} \otimes Q^{\theta'}_{\pi_C^q(y)}\Big\| = \max_{x,y}\Big\|\bigotimes_{\ell\in\mathcal{T}}\sqrt{F_{x_\ell}^{\theta_\ell}}\sqrt{F_{y_\ell}^{\theta'_\ell}}\Big\| \leqslant c(\mathsf{G})^t.$$

It remains to find suitable permutations π^k and substitute the above bound into (8). Again, we choose permutations with the property that the Hamming distance between θ and $\pi^k(\theta)$ is the same for all $\theta \in \Theta^n$. It is easy to verify that there are $\binom{n}{t}(|\Theta|-1)^t$ permutations for which the (θ-independent) Hamming distance between θ and $\pi^k(\theta)$ is t. Hence

$$\sum_\theta \frac{1}{|\Theta|^n}\text{tr}(\Pi^\theta \rho_{A_1\ldots A_n BC}) \leqslant \frac{|\mathcal{Q}|}{|\Theta|^n}\sum_{t=0}^n \binom{n}{t}(|\Theta|-1)^t\big(\sqrt{c(\mathsf{G})}\big)^t = |\mathcal{Q}|\Big(\frac{1}{|\Theta|} + \frac{|\Theta|-1}{|\Theta|}\sqrt{c(\mathsf{G})}\Big)^n,$$

which concludes the proof. □

One particularly interesting example of the above theorem considers binary measurements, i.e. $\mathcal{X} = \{0, 1\}$, where Alice will accept Bob's and Charlie's answers if and only if they get less than a certain fraction of bits wrong. More precisely, she accepts if $d(x, y) \leqslant \gamma n$ and $d(x, z) \leqslant \gamma' n$, where $d(\cdot,\cdot)$ denotes the Hamming distance and y, z are Bob's and Charlie's guesses, respectively. In this case, we introduce the set $\mathcal{Q}^n_{\gamma,\gamma'}$ that contains all pairs of

permutations (π_B^q, π_C^q) on $\{0,1\}^n$ of the form $\pi_B^q(x) = x \oplus k$, $\pi_C^q(x) = x \oplus k'$, where $q = \{k, k'\}$, and $k, k' \in \{0,1\}^n$ have Hamming weight at most γn and $\gamma' n$, respectively. For $\gamma, \gamma' \leqslant 1/2$, one can upper bound $|\mathcal{Q}^n_{\gamma,\gamma'}| \leqslant 2^{nh(\gamma)+nh(\gamma')}$, where $h(\cdot)$ denotes the binary entropy. We thus find

$$p_{\text{win}}(\mathsf{G}^{\times n}; \mathcal{Q}^n_{\gamma,\gamma'}) \leqslant \left(2^{h(\gamma)+h(\gamma')} \frac{1 + (|\Theta| - 1)\sqrt{c(\mathsf{G})}}{|\Theta|}\right)^n. \tag{9}$$

Similarly, if we additionally require that Charlie guesses the same string as Bob, we analogously define the corresponding set $\mathcal{Q}^n_\gamma$, with reduced cardinality, and

$$p_{\text{win}}(\mathsf{G}^{\times n}; \mathcal{Q}^n_\gamma) \leqslant \left(2^{h(\gamma)} \frac{1 + (|\Theta| - 1)\sqrt{c(\mathsf{G})}}{|\Theta|}\right)^n$$

4. Application I. One-sided device-independent QKD

In the following, we assume some familiarity with QKD. For simplicity, we consider an entanglement-based [20] variant of the BB84 QKD scheme [7], where Bob waits with performing the measurement until Alice tells him the right bases. This protocol is impractical because it requires Bob to store qubits. However, it is well known that security of this impractical version implies security of the original, more practical BB84 QKD scheme [6]. It is straightforward to verify that this implication also holds in the one-sided DI setting we consider here.

The entanglement-based QKD scheme, *E-QKD*, is described in figure 1. It is (implicitly) parameterized by positive integers $0 < t, s, \ell < n$ and a real number $0 \leqslant \gamma < \frac{1}{2}$. Here, n is the number of qubits exchanged between Alice and Bob, t is the size of the sample used for parameter estimation, s is the leakage (in bits) due to error correction, ℓ is the length (in bits) of the final key and γ is the tolerated error in Bob's measurement results. Furthermore, the scheme makes use of a universal$_2$ family $\mathcal{F}$ of hash functions $F : \{0,1\}^{n-t} \to \{0,1\}^\ell$.

A QKD protocol is called *perfectly secure* if it either aborts and outputs an empty key, $K = \perp$, or it produces a key that is uniformly random and independent of Eve's (quantum and classical) information E^+ gathered during the execution of the protocol. Formally, this means that the final state must be of the form $\rho_{KE^+} = \Pr_\rho[K \neq \perp] \cdot \mu_K \otimes \rho_{E^+|K\neq\perp}$ $+ \Pr_\rho[K = \perp] \cdot |\perp\rangle\langle\perp|_K \otimes \rho_{E^+|K=\perp}$, where μ_K is a 2^ℓ-dimensional completely mixed state, and $|\perp\rangle\langle\perp|_K$ is orthogonal to μ_K.

Relaxing this condition, a protocol is called δ-secure if ρ_{KE^+} is δ-close to the above form in trace distance, meaning that ρ_{KE^+} satisfies

$$\Pr_\rho[K \neq \perp] \cdot \Delta(\rho_{KE^+|K\neq\perp}, \mu_K \otimes \rho_{E^+|K\neq\perp}) \leqslant \delta\,. \tag{10}$$

It is well known and has been proven in various ways that E-QKD is δ-secure (with small δ) with a suitable choice of parameters, assuming that all quantum operations are correctly performed by Alice and Bob. We now show that the protocol remains secure even if Bob's measurement device behaves arbitrarily and possibly maliciously. The only assumption is that Bob's device does not communicate with Eve after it received Alice's quantum signals. This restriction is clearly necessary as there would otherwise not be any asymmetry between Bob and Eve's information about Alice's key. Note that the scheme is well known to satisfy *correctness* and *robustness*; hence, we do not argue these here.

State Preparation:: Alice prepares n EPR pairs $\frac{1}{\sqrt{2}}\big(|0\rangle\otimes|0\rangle+|1\rangle\otimes|1\rangle\big)$. Then, of each pair, she keeps one qubit and sends the other to Bob.

Confirmation:: Bob confirms receipt of the n qubits. (After this point, there cannot be any communication between Bob's device and Eve.)

Measurement:: Alice chooses random $\Theta\in\{0,1\}^n$ and sends it to Bob, and Alice and Bob measure the EPR pairs in basis Θ to obtain X and Y, respectively.
(Remember: Bob's device may produce Y in an arbitrary way, using a POVM chosen depending on Θ acting on a state provided by Eve.)

Parameter Estimation:: Alice chooses a random subset $T\subset\{1,\ldots,n\}$ of size t, and sends T and X_T to Bob. If the relative Hamming distance, $d_{\mathrm{rel}}(X_T,Y_T)$, exceeds γ then they abort the protocol and set $K=\perp$.

Error Correction:: Alice sends a syndrome $S(X_{\bar{T}})$ of length s and a random hash function $F:\{0,1\}^{n-t}\to\{0,1\}^{\ell}$ from $\mathcal{F}$ to Bob.

Privacy Amplification:: Alice computes $K=F(X_{T^c})$ and Bob $\hat{K}=F(\hat{X}_{T^c})$, where $\hat{X}_{T^c}$ is the corrected version of Y_{T^c}.

Figure 1. An entanglement-based QKD scheme E-QKD.

Theorem 5. *Consider an execution of E-QKD, with an arbitrary measurement device for Bob. Then, for any $\varepsilon>0$, protocol E-QKD is δ-secure with*

$$\delta=5\mathrm{e}^{-2\varepsilon^2 t}+2^{-\frac{1}{2}\left(\log(1/\beta_\circ)n-h(\gamma+\varepsilon)n-\ell-t-s+2\right)}\quad\text{where}\quad\beta_\circ=\frac{1}{2}+\frac{1}{2\sqrt{2}}.$$

Note that with an optimal error correcting code, the size of the syndrome for large n approaches the Shannon limit $s=nh(\gamma)$. The security error δ can then be made negligible in n with suitable choices of parameters if $\log(1/\beta_\circ)>2\,h(\gamma)$, which roughly requires that $\gamma\leqslant 0.015$. Hence, the scheme can tolerate a noise level up to 1.5% asymptotically[7].

The formal proof is given below. The idea is rather simple. We consider a *gedankenexperiment* where Eve *measures* her system, using an arbitrary POVM, with the goal to guess X. The execution of E-QKD then pretty much coincides with $\mathsf{G}_{\mathrm{BB84}}^{\times n}$, and we can conclude from our results that if Bob's measurement outcome Y is close to X, then Eve must have a hard time in guessing X. Since this holds for any measurement she may perform, this means her min-entropy on X is large and hence the extracted key K is secure.

Proof. Let $\rho_{\Theta T\mathrm{ABE}}=\rho_\Theta\otimes\rho_T\otimes|\psi_{ABE}\rangle\langle\psi_{ABE}|$ be the state before Alice and Bob perform the measurements on A and B, respectively, where system E is held by the adversary Eve. Here, the random variable Θ contains the choice of basis for the measurement, whereas the random variable T contains the choice of subset on which the strings are compared (see the protocol description in figure 1). Moreover, let $\rho_{\Theta TXYE}$ be the state after Alice and Bob measured, where—for every possible value θ—Alice's measurement is given by the projectors $\{|x^\theta\rangle\langle x^\theta|\}_x$, and Bob's measurement by an arbitrary but fixed POVM $\{P_x^\theta\}_x$.

As a *gedankenexperiment*, we consider the scenario where Eve wants to guess the value of Alice's raw key, X. Eve wants to do this during the parameter estimation step of the protocol, exactly *after* Alice broadcast T but *before* she broadcasts X_T.[8] For this purpose, we consider an arbitrary measurement strategy of Eve that aims to guess X. Such a strategy is given by—for

[7] This can be improved slightly by instead considering a six-state protocol [11], where the measurement is randomly chosen among three mutually unbiased bases on the qubit.

[8] Note that the effect of Eve learning X_T is taken into account later, in equation (12).

every basis choice, θ, and every choice of sample, τ—a POVM $\{Q_x^{\theta,\tau}\}_x$. The values of θ and τ have been broadcast over a public channel, and are hence known to Eve at this point of the protocol. She will thus choose a POVM depending on these values to measure E and use the measurement outcome as her guess.

For our *gedankenexperiment*, we will use the state, $\rho_{\Theta TXYZ}$, which is the (purely classical) state that results after Eve applied her measurement on E. Let $\varepsilon > 0$ be an arbitrary constant. By our results from section 3, it follows that for any choices of $\{P_x^\theta\}_x$ and $\{Q_x^{\theta,\tau}\}_x$, we have

$$\Pr_\rho[d_{\mathrm{rel}}(X,Y) \leqslant \gamma+\varepsilon \wedge Z=X] \leqslant p_{\mathrm{win}}(\mathsf{G}_{\mathrm{BB84}}^{\times n}; \mathcal{Q}^n_{\gamma+\varepsilon,0}) \leqslant \beta^n$$

with $\beta = 2^{h(\gamma+\varepsilon)}\beta_\circ$, where d_{rel} denotes the relative Hamming distance. This uses the fact that Alice's measurement outcome is independent of T, and T can in fact be seen as part of Eve's system for the purpose of the monogamy game.

We now construct a state $\tilde{\rho}_{\Theta TXYE}$ as follows:

$$\tilde{\rho}_{\Theta TXYE} = \Pr_\rho[\Omega] \cdot \rho_{\Theta TXYE|\Omega} + (1 - \Pr_\rho[\Omega]) \cdot \sigma_{\Theta TXYE},$$

where Ω denotes the event $\Omega = \{d_{\mathrm{rel}}(X,Y) \leqslant d_{\mathrm{rel}}(X_T,Y_T)+\varepsilon\}$, and we take $\sigma_{T\Theta XYE}$ to be an arbitrary state with classical Θ, T, X and Y for which $d_{\mathrm{rel}}(X,Y) = 1$, and hence $d_{\mathrm{rel}}(X_T,Y_T) = 1$. Informally, the event Ω indicates that the relative Hamming distance of the sample strings X_T and Y_T determined by T was representative of the relative Hamming distance between the whole strings, X and Y, and the state $\tilde{\rho}_{\Theta TXYE}$ is so that this is satisfied with certainty. By construction of $\tilde{\rho}_{\Theta TXYE}$, we have $\Delta(\rho_{\Theta TXYE}, \tilde{\rho}_{\Theta TXYE}) \leqslant 1 - \Pr_\rho[\Omega]$, and by Hoeffding's inequality:

$$1 - \Pr_\rho[\Omega] = \Pr_\rho[d_{\mathrm{rel}}(X,Y) > d_{\mathrm{rel}}(X_T,Y_T)+\varepsilon] \leqslant \mathrm{e}^{-2\varepsilon^2 t}.$$

Moreover, note that the event $d_{\mathrm{rel}}(X_T,Y_T) \leqslant \gamma$ implies $d_{\mathrm{rel}}(X,Y) \leqslant \gamma+\varepsilon$ under $\tilde{\rho}_{\Theta TXYE}$. Thus, for every choice of strategy $\{Q_x^{\theta,\tau}\}_x$ by the eavesdropper, the resulting state $\tilde{\rho}_{\Theta TXYZ}$, obtained by applying $\{Q_x^{\theta,\tau}\}_x$ to E, satisfies

$$\begin{aligned}\Pr_{\tilde{\rho}}[d_{\mathrm{rel}}(X_T,Y_T) \leqslant \gamma \wedge Z=X] &\leqslant \Pr_{\tilde{\rho}}[d_{\mathrm{rel}}(X,Y) \leqslant \gamma+\varepsilon \wedge Z=X] \\ &\leqslant \Pr_\rho[d_{\mathrm{rel}}(X,Y) \leqslant \gamma+\varepsilon \wedge Z=X] \leqslant \beta^n.\end{aligned} \tag{11}$$

The second inequality follows from the definition of $\tilde{\rho}$, in particular the fact that $\Pr_\sigma[d_{\mathrm{rel}}(X,Y) \leqslant \gamma+\varepsilon] = 0$.

Next, we introduce the event $\Gamma = \{d_{\mathrm{rel}}(X_T,Y_T) \leqslant \gamma\}$, which corresponds to the event that Bob does not abort the protocol. Expanding the left-hand side of (11) to $\Pr_{\tilde{\rho}}[\Gamma] \cdot \Pr_{\tilde{\rho}}[Z=X|\Gamma]$ and observing that $\Pr_{\tilde{\rho}}[\Gamma]$ does not depend on the strategy $\{Q_x^{\theta,\tau}\}_x$, we can conclude that

$$\forall\, \{Q_x^{\theta,\tau}\}_x : \Pr_{\tilde{\rho}}[Z=X|\Gamma] \leqslant \beta^{(1-\alpha)n},$$

where $\alpha \geqslant 0$ is determined by $\Pr_{\tilde{\rho}}[\Gamma] = \beta^{\alpha n}$. Therefore, by definition of the min-entropy, $H_{\min}(X|\Theta TE,\Gamma)_{\tilde{\rho}} \geqslant n(1-\alpha)\log(1/\beta)$. (This notation means that the min-entropy of X given Θ, T and E is evaluated for the state $\tilde{\rho}_{\Theta TXYE|\Gamma}$, conditioned on not aborting.) By the chain rule, it now follows that

$$\begin{aligned}H_{\min}(X|\Theta T X_T S E,\Gamma)_{\tilde{\rho}} &\geqslant H_{\min}(X X_T S|\Theta TE,\Gamma)_{\tilde{\rho}} - t - s \\ &\geqslant n(1-\alpha)\log(1/\beta) - t - s.\end{aligned} \tag{12}$$

Here, the min-entropy is evaluated for the state $\tilde{\rho}_{X\Theta TX_TSE}$ that is constructed from $\tilde{\rho}_{X\Theta TE}$ by calculating the error syndrome and copying X_T from X as done in the prescription of the

protocol. In particular, $\Delta(\tilde{\rho}_{X\Theta T X_T S E}, \rho_{X\Theta T X_T S E}) \leqslant \mathrm{e}^{-2\varepsilon^2 t}$. Finally, privacy amplification with universal$_2$ hashing applied to the state $\tilde{\rho}_{X\Theta T X_T S E}$ ensures that the key K satisfies [50, corollary 5.5.2]

$$\Delta(\tilde{\rho}_{K F\Theta T X_T S E|\Gamma},\ \mu_K \otimes \tilde{\rho}_{F\Theta T X_T E|\Gamma}) \leqslant \frac{1}{2}\sqrt{\beta^{(1-\alpha)n}\, 2^{\ell+t+s}}.$$

And, in particular, recalling that $\Pr_{\tilde{\rho}}[\Gamma] = \beta^{\alpha n}$, we have

$$\Pr_{\tilde{\rho}}[\Gamma] \cdot \Delta(\tilde{\rho}_{K F\Theta T X_T S E|\Gamma},\ \mu_K \otimes \tilde{\rho}_{F\Theta T X_T E|\Gamma}) \leqslant \frac{1}{2}\sqrt{\beta^{n}\, 2^{\ell+t+s}}.$$

Using $\beta = 2^{h(\gamma+\varepsilon)}\beta_\circ$ and applying lemma 10 in appendix B concludes the proof. □

5. Application II. A one-round position-verification scheme

The scheme we consider is the parallel repetition of the simple single-qubit scheme that was analyzed in the setting of no pre-shared entanglement in [12]. The analysis shows that the soundness error of the one-round single-qubit scheme is bounded by roughly 89%, and it is suggested to repeat the scheme sequentially in order to reduce this soundness error. We now show that also the *parallel repetition* has an exponentially small soundness error[9]. Finally, we use a simple observation from [3] to argue that the scheme is also secure against adversaries with a linearly bounded amount of entanglement.

The scheme, parameterized by a positive integer n, consists of the following steps.

1. V_0 and V_1 agree on random $x, \theta \in \{0,1\}^n$. V_0 prepares a quantum system Q of n qubits in the state $H^\theta|x\rangle = H^{\theta_1}|x_1\rangle \otimes \cdots \otimes H^{\theta_n}|x_n\rangle \in \mathcal{H}_Q = (\mathbb{C}^2)^{\otimes n}$ and sends it to P. V_1 sends θ to P, so that both arrive at P's claimed position *pos* at the same time.
2. As soon as Q and θ arrive, P measures the ith qubit in basis $\{H^{\theta_i}|0\rangle, H^{\theta_i}|1\rangle\}$ for $i = 1, \ldots, n$. Let $x' \in \{0,1\}^n$ collect the observed bits. P sends x' to V_0 and V_1.
3. If V_0 and V_1 receive x' at the respective time consistent with *pos*, and if $x' = x$, then V_0 and V_1 accept; otherwise, they reject.

It is straightforward to verify that this protocol is correct, meaning that the verifiers accept honest P at position *pos* with certainty (assuming a perfect setting with no noise, etc).

Proposition 6 *The above position verification scheme is* $(\frac{1}{2}+\frac{1}{2\sqrt{2}})^n$*-sound against adversaries* (E_0, E_1) *that hold no entangled state at the time they receive* Q *and* θ*, respectively.*

We stress that a restriction on the entanglement is necessary, as with unbounded entanglement the general impossibility result from [12] applies. In fact, for the specific scheme considered here, already n shared EPR-pairs are sufficient to break it, as shown in [31]. Below, we will extend the security of the scheme to a setting where the adversaries share at most αn entangled qubits, for any constant $\alpha \lesssim 0.22$.

We also point out that our adversary model (with linearly bounded entanglement) is stronger than the one considered by Beigi and König [3] for their schemes: their model not only prohibits quantum communication between the adversaries *before* they obtain the initial

[9] We stress that this was to be expected and does not come as a surprise. However, until now it was unclear how to prove it.

messages from the verifiers (in order to prevent the exchange of entangled states), but also *afterwards*. Here, we allow full quantum communication between the adversaries after they have received the initial respective messages Q and θ.

Proof (sketch). As the colluding dishonest parties E_0 and E_1 share no entanglement, the most general attack is of the following form, where we may assume E_i to be located between V_i and the position pos, for $i \in \{0, 1\}$. Upon receiving the n-qubit system Q (in state $H^\theta|x\rangle$) from V_0, the adversary E_0 applies an isometry $\mathcal{H}_Q \to \mathcal{H}_B \otimes \mathcal{H}_C$ to Q in order to obtain a bipartite system B and C, and forwards C to E_1. Adversary E_1, upon receiving θ from V_1, simply forwards θ to E_0.[10] Then, when E_0 receives θ from E_1, he measures B (using an arbitrary measurement that may depend on θ) and sends the measurement outcome $x'_0 \in \{0, 1\}^n$ to V_0, and, similarly, when E_1 receives system C from E_0, he measures C and sends the measurement outcome $x'_1 \in \{0, 1\}^n$ to V_1. The probability ε that V_0 and V_1 accept is then given by the probability that $x'_0 = x = x'_1$.

From a standard purification argument it follows that the probability ε does not change if in the first step of the protocol, instead of sending Q in state $H^\theta|x\rangle$, V_0 prepares n EPR pairs, sends one half of each pair toward P and only at some later point in time measures the remaining n qubits in the basis $\{H^\theta|y\rangle\}_{y\in\{0,1\}^n}$ to obtain $x \in \{0, 1\}^n$.

Let us now consider the state $|\psi_{ABC}\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C$, consisting of system A with the n qubits that V_0 kept, and the systems B and C obtained by applying the isometry to the qubits E_0 received from V_0. Since the isometry is independent of θ—E_0 needs to decide on it before he finds out what θ is—so is the state $|\psi_{ABC}\rangle$. It is clear that in order to pass the position verification test the adversaries must win a restricted version of the game $\mathsf{G}^{\times n}_{\mathrm{BB84}}$.[11] Therefore, the probability ε that $x'_0 = x = x'_1$ is bounded by $p_{\mathrm{win}}(\mathsf{G}^{\times n}_{\mathrm{BB84}})$. Our theorem 3 thus concludes the proof. □

The security of the position verification scheme can be immediately extended to adversaries that hold a linear amount of shared entanglement.

Corollary 7 *The above position verification scheme is* $d \cdot (\frac{1}{2}+\frac{1}{2\sqrt{2}})^n$*-sound against adversaries* (E_0, E_1) *that share an arbitrary (possibly entangled) state* $\eta_{E_0E_1}$*, such that* $\dim \eta_{E_0E_1} = d$*, at the time they receive* Q *and* θ*, respectively.*

Thus, for any α strictly smaller than $\log(\frac{1}{2}+\frac{1}{2\sqrt{2}})$, for instance for $\alpha = 0.2$, the position verification scheme has exponentially small soundness error (in n) against adversaries that hold at most αn pre-shared entangled qubits.

Corollary 7 is an immediate consequence of proposition 6 above and of lemma V.3 of [3]. The latter states that ε-soundness with no entanglement implies $(d\varepsilon)$-soundness for adversaries that pre-share a d-dimensional state. This follows immediately from the fact that the pre-shared state can be extended to a basis of the d-dimensional state space, and the uniform mixture of all these basis states gives a non-entangled state (namely the completely mixed state). As a consequence, applying the attack, which is based on the entangled state, to the setting with no entanglement, reduces the success probability by at most a factor of d.

[10] This is where the restriction of no entanglement comes into play. If the adversaries shared entanglement their most general strategy would be to perform some joint operation on the respective part of the entangled state and the data they have just received. The impossibility result states that in a scenario with an unlimited amount of entanglement no position verification scheme can be secure.

[11] The extra restriction comes from the fact that they have no access to the qubits kept by V_0 and so the reduced state on those must be fully mixed. It turns out that this restriction does not affect the optimal winning probability.

By the results on imperfect guessing (see section 3.2), at the price of correspondingly weaker parameters, the above results extend to a noise-tolerant version of the scheme, where it is sufficient for x' to be *close*, rather than equal, to x for V_0 and V_1 to accept.

6. Application III. Entropic uncertainty relation

Let ρ be an arbitrary state of a qubit and Θ a uniformly random bit. Then, we may consider the min-entropy of X, where X is the outcome when ρ is measured in either one of two bases with overlap c, as determined by Θ. For this example, it is known that [18, 52]

$$H_{\min}(X|\Theta)_\rho \geqslant -\log \frac{1+\sqrt{c}}{2}. \tag{13}$$

A similar relation follows directly from results by Maassen and Uffink [41], namely

$$H_{\min}(X|\Theta)_\rho + H_{\max}(X|\Theta)_\rho \geqslant -\log c, \tag{14}$$

where $H_{\max}$ denotes the Rényi entropy [51] of order $\frac{1}{2}$.

Recently, entropic uncertainty relations have been generalized to the case where the party guessing X has access to quantum side information [8]. However, note that a party that is maximally entangled with the state of the system to be measured can always guess the outcome of X by applying an appropriate measurement (depending on Θ) on the entangled state. Thus, there cannot be any non-trivial state-independent bound on the entropies above conditioned on quantum side information. Nonetheless, if two disjoint quantum memories are considered, the following generalization of (14) was shown. For an arbitrary tripartite state ρ_{ABC} and X measured on A as prescribed above, one finds [60]

$$H_{\min}(X|B\Theta)_\rho + H_{\max}(X|C\Theta)_\rho \geqslant -\log c\,. \tag{15}$$

In the following, we show a similar generalization of the uncertainty relation in (13) to quantum side information.

Theorem 8 *Let ρ_{ABC} be a quantum state and Θ a uniformly random bit. Given two POVMs $\{F_x^0\}$ and $\{F_x^1\}$ with overlap $c := \max_{x,z} \|\sqrt{F_x^0}\sqrt{F_z^1}\|^2$, we find*

$$p_{\text{guess}}(X|B\Theta)_\rho + p_{\text{guess}}(X|C\Theta)_\rho \leqslant 1+\sqrt{c}$$

and

$$H_{\min}(X|B\Theta)_\rho + H_{\min}(X|C\Theta)_\rho \geqslant -2\log \frac{1+\sqrt{c}}{2},$$

where the quantities are evaluated for the post-measurement state

$$\rho_{XBC\Theta} = \sum_{x,\theta} \frac{1}{2}\,|x\rangle\langle x|_X \otimes \mathrm{tr}_A((F_x^\theta \otimes 1_{BC})\rho_{ABC}) \otimes |\theta\rangle\langle\theta|_\Theta. \tag{16}$$

Proof. First, recall that the min-entropy is defined as (cf equation (2))

$$2^{-H_{\min}(X|B\Theta)_\rho} = p_{\text{guess}}(X|B\Theta)_\rho = \max_{\{P_x^\theta\}} \sum_{x,\theta} p_{x,\theta}\,\mathrm{tr}(\rho_B^{x,\theta} P_x^\theta) = \max_{\{P_x^\theta\}} \frac{1}{2}\sum_{x,\theta} \mathrm{tr}(\rho_{AB}(F_x^\theta \otimes P_x^\theta)),$$

where we used the fact that the post-measurement states given by (16) satisfy $p_{x,\theta}\,\rho_{BC}^{x,\theta} = \frac{1}{2}\mathrm{tr}_A(F_x^\theta \rho_{ABC})$.

In the following argument, we restrict ourselves to the case where the optimal guessing strategies for the min-entropy, $\{P_x^\theta\}$ for Bob and $\{Q_x^\theta\}$ for Charlie, are projective. To see that this is sufficient, note that we can always embed the state ρ_{XBC} into a larger system $\rho_{XB'C'}$ such that the optimal POVMs on B and C can be diluted into an equivalent projective measurement strategy on B' and C', respectively. The data-processing inequality of the min-entropy then tells us that $H_{\min}(X|B\Theta) \geqslant H_{\min}(X|B'\Theta)$ and $H_{\min}(X|C\Theta) \geqslant H_{\min}(X|C'\Theta)$, i.e. it is sufficient to find a lower bound on the smaller quantities, for which the optimal strategy is projective.

For an arbitrary state ρ_{ABC} and optimal projective POVMs $\{P_x^\theta\}$ and $\{Q_x^\theta\}$, we have

$$2^{-H_{\min}(X|B\Theta)_\rho} + 2^{-H_{\min}(X|C\Theta)_\rho} = \frac{1}{2}\sum_{x,\theta} \mathrm{tr}\left(\rho_{ABC}(F_x^\theta \otimes P_x^\theta \otimes 1_C + F_x^\theta \otimes 1_B \otimes Q_x^\theta)\right)$$
$$\leqslant \frac{1}{2}\left\| \sum_{x,\theta} F_x^\theta \otimes P_x^\theta \otimes 1_C + F_x^\theta \otimes 1_B \otimes Q_x^\theta \right\|.$$

We now upper-bound this norm. First, we rewrite

$$\left\| \sum_{x,\theta} F_x^\theta \otimes P_x^\theta \otimes 1_C + F_x^\theta \otimes 1_B \otimes Q_x^\theta \right\| = \left\| \sum_{i,\theta} A_i^\theta \right\| \leqslant \|A_0^0 + A_1^1\| + \|A_1^0 + A_0^1\|,$$

where $A_0^\theta = \sum_x F_x^\theta \otimes P_x^\theta \otimes 1_C$ and $A_1^\theta = \sum_x F_x^\theta \otimes 1_B \otimes Q_x^\theta$ are projectors. Applying lemma 2 twice then yields

$$\|A_0^0 + A_1^1\| + \|A_1^0 + A_0^1\| \leqslant 2 + \left\|\sqrt{A_0^0}\sqrt{A_1^1}\right\| + \left\|\sqrt{A_0^1}\sqrt{A_1^0}\right\|$$
$$\leqslant 2 + 2\max_{x,z} \|\sqrt{F_x^0}\sqrt{F_z^1}\| \leqslant 2 + 2\sqrt{c},$$

where we used that $\| A_i^\theta \| \leqslant 1$. Hence,

$$2^{-H_{\min}(X|B\Theta)_\rho} + 2^{-H_{\min}(X|C\Theta)_\rho} = p_{\mathrm{guess}}(X|B\Theta)_\rho + p_{\mathrm{guess}}(X|C\Theta)_\rho \leqslant 1 + \sqrt{c}$$

and, using the relation between arithmetic and geometric mean, we finally get

$$2^{-H_{\min}(X|B\Theta)_\rho} 2^{-H_{\min}(X|C\Theta)_\rho} \leqslant \left(\frac{1+\sqrt{c}}{2}\right)^2,$$

which implies the statement of the lemma after taking the logarithm on both sides. □

Note that, for n measurements, each in a basis chosen uniformly at random, the above result still only guarantees one bit of uncertainty. In fact, an adaptation of the proof of theorem 8 yields the bound

$$H_{\min}(X^n|B\Theta^n) + H_{\min}(X^n|C\Theta^n) \geqslant -2\log\frac{1+\sqrt{c^n}}{2}.$$

This bound can be approximately achieved using a state that is maximally entangled between A and B with probability $\frac{1}{2}$ and maximally entangled between A and C otherwise. This construction ensures that both conditional min-entropies are low and we thus cannot expect a stronger result. This is in stark contrast to the situation with classical side information in (13) and the alternative uncertainty relation (15), where the lower bound on the uncertainty can be shown to scale linearly in n (cf [60, 62]). Due to this restriction, we expect that the applicability of theorem 8 to quantum cryptography is limited.

7. Conclusion

We introduce the notion of a monogamy-of-entanglement game, and we show a general parallel repetition theorem. For a BB84-based example game, we actually show *strong* parallel repetition, and that a non-entangled strategy is sufficient to achieve the optimal winning probability. Our results have various applications to quantum cryptography.

It remains open to understand which monogamy-of-entanglement games satisfy strong parallel repetition. Another open question is whether (or in what cases) a *concentration theorem* holds, which states that with high probability the fraction of won executions in a parallel repetition cannot be much larger than the probability of winning a single execution.

With respect to our applications, an interesting open problem is to increase the noise level that can be tolerated for one-sided DI security of BB84. It is not clear at all that the rather low noise level of 1.5% we obtain in our analysis is inherent; this may very well be an artifact of our technique. Finally, it would be interesting to extend our analysis to incorporate channel losses following the work of Branciard *et al* [9]. As suggested there, we expect that such an analysis would reveal a higher tolerance for losses as compared to fully DI QKD.

Acknowledgments

We thank Renato Renner for early discussions and Niek J Bouman for bringing this problem to the attention of some of us. MT, JK and SW are funded by the Ministry of Education (MOE) and National Research Foundation Singapore, as well as MOE Tier 3 Grant 'Random numbers from quantum processes' (MOE2012-T3-1-009).

Appendix A. Pure strategies are sufficient

Lemma 9 *In the supremum over strategies in (5), it is sufficient to consider pure strategies.*

Proof. Given any strategy $\mathcal{S} = \{\rho_{ABC}, P_x^\theta, Q_x^\theta\}$ for a game G, we construct a pure strategy $\tilde{\mathcal{S}} = \{|\tilde{\varphi}\rangle\langle\tilde{\varphi}|, \tilde{P}_x^\theta, \tilde{Q}_x^\theta\}$ with $p_{\text{win}}(\mathsf{G}, \tilde{\mathcal{S}}) = p_{\text{win}}(\mathsf{G}, \mathcal{S})$. First, it is clear that purifying ρ_{ABC}, with a purifying register that is appended to C, does not change the value of $p_{\text{win}}(\mathsf{G}, \mathcal{S})$. Hence, we may assume that ρ_{ABC} is already pure: $\rho_{ABC} = |\varphi\rangle\langle\varphi|$. In this case, $p_{\text{win}}(\mathsf{G}, \mathcal{S})$ simplifies to

$$p_{\text{win}}(\mathsf{G}, \mathcal{S}) = \sum_{x,\theta} \frac{1}{|\Theta|} \langle\varphi|(|x^\theta\rangle\langle x^\theta| \otimes P_x^\theta \otimes Q_x^\theta)|\varphi\rangle.$$

Let $\mathcal{H}_X$ be a Hilbert space of dimension $|\mathcal{X}|$ and with basis $\{|x\rangle\}_x$, and let $|\psi_0\rangle$ be an arbitrary, fixed vector in $\mathcal{H}_X$. We now set $|\tilde{\varphi}\rangle = |\varphi\rangle \otimes |\psi_0\rangle \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_C \otimes \mathcal{H}_X$ as well as $\tilde{P}_x^\theta = U_\theta^\dagger(1_B \otimes |x\rangle\langle x|)U_\theta$, where $U_\theta \in \mathcal{L}(\mathcal{H}_B \otimes \mathcal{H}_X)$ is a Neumark dilation unitary that maps

$$|\psi\rangle \otimes |\psi_0\rangle \mapsto \sum_{x\in\mathcal{X}} \sqrt{P_x^\theta}|\psi\rangle \otimes |x\rangle$$

for every $|\psi\rangle \in \mathcal{H}_B$. Then, $\tilde{P}_x^\theta$ is indeed a projection and hence $\tilde{P}_x^\theta = (\tilde{P}_x^\theta)^\dagger \tilde{P}_x^\theta$, and [12]

$$\tilde{P}_x^\theta|\tilde{\varphi}\rangle = U_\theta^\dagger(1_B \otimes |x\rangle\langle x|)U_\theta(|\varphi\rangle \otimes |\psi_0\rangle) = U_\theta^\dagger\sqrt{P_x^\theta}|\varphi\rangle \otimes |x\rangle.$$

[12] It is implicitly understood that $\tilde{P}_x^\theta$ only acts on the BX part of $|\tilde{\varphi}\rangle$, and similarly for U_θ, etc.

Similarly, we define the projection $\tilde{Q}_x^\theta$ (and extend the state $|\tilde{\varphi}\rangle$). It then follows immediately that $p_{\text{win}}(\mathsf{G}, \tilde{\mathcal{S}}) = p_{\text{win}}(\mathsf{G}, \mathcal{S})$. □

Appendix B. Equivalence of QKD security definitions

To prove security of a protocol, it is sufficient to show that the security criterion is satisfied by a state close to the true output state of the protocol. This is due to the following lemma.

Lemma 10 *Let ρ_{XB}, $\tilde{\rho}_{XB} \in \mathcal{S}(\mathcal{H}_X \otimes \mathcal{H}_B)$ be two CQ states with X over $\mathcal{X}$. Also, let $\lambda : \mathcal{X} \to \{0, 1\}$ be a predicate on $\mathcal{X}$ and $\Lambda = \lambda(X)$, and let $\tau_X \in \mathcal{S}(\mathcal{H}_X)$ be arbitrary. Then*

$$\Pr_{\rho}[\Lambda] \cdot \Delta(\rho_{XB|\Lambda},\ \tau_X \otimes \rho_{B|\Lambda}) \leqslant 5\Delta(\rho_{XB},\ \tilde{\rho}_{XB}) + \Pr_{\tilde{\rho}}[\Lambda] \cdot \Delta(\tilde{\rho}_{XB|\Lambda},\ \tau_X \otimes \tilde{\rho}_{B|\Lambda}).$$

Proof. We set $\delta := \Delta(\rho_{XB}, \tilde{\rho}_{XB})$. From $\Delta(\rho_{XB}, \tilde{\rho}_{XB}) = \delta$ it follows in particular that the two distributions P_X and $\tilde{P}_X$ are δ-close, and thus that the state

$$\sigma_{XB} := \Pr_{\rho}[\Lambda] \cdot \tilde{\rho}_{XB|\Lambda} + \Pr_{\rho}[\neg\Lambda] \cdot \tilde{\rho}_{XB|\neg\Lambda}$$

is δ-close to $\tilde{\rho}_{XB}$, and hence 2δ-close to ρ_{XB}, where $\neg\Lambda$ is the negation of the event Λ. Since Λ is determined by X, we can write

$$\Delta(\rho_{XB}, \sigma_{XB}) = \Pr_{\rho}[\Lambda] \cdot \Delta(\rho_{XB|\Lambda},\ \tilde{\rho}_{XB|\Lambda}) + \Pr_{\rho}[\neg\Lambda] \cdot \Delta(\rho_{XB|\neg\Lambda},\ \tilde{\rho}_{XB|\neg\Lambda})$$

from which it follows that $\Pr_\rho[\Lambda] \cdot \Delta(\rho_{XB|\Lambda},\ \tilde{\rho}_{XB|\Lambda}) \leqslant 2\delta$, and, by tracing out X, also that $\Pr_\rho[\Lambda] \cdot \Delta(\rho_{B|\Lambda}, \tilde{\rho}_{B|\Lambda}) \leqslant 2\delta$. We can now conclude that

$$\begin{aligned}\Pr_{\rho}[\Lambda] \cdot \Delta(\rho_{XB|\Lambda},\ \tau_X \otimes \rho_{B|\Lambda}) &\leqslant 4\delta + \Pr_{\rho}[\Lambda] \cdot \Delta(\tilde{\rho}_{XB|\Lambda},\ \tau_X \otimes \tilde{\rho}_{B|\Lambda}) \\ &\leqslant 5\delta + \Pr_{\tilde{\rho}}[\Lambda] \cdot \Delta(\tilde{\rho}_{XB|\Lambda},\ \tau_X \otimes \tilde{\rho}_{B|\Lambda})\end{aligned}$$

which proves the claim. □

References

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

[2] Barrett J, Hardy L and Kent A 2005 No signaling and quantum key distribution *Phys. Rev. Lett.* **95** 010503

[3] Beigi S and König R 2011 Simplified instantaneous non-local quantum computation with applications to position-based cryptography *New J. Phys.* **13** 093036

[4] Bell J S 1964 On the Einstein–Podolsky–Rosen paradox *Physics* **1** 195–200

[5] Ben-Or M, Goldwasser S, Kilian J and Wigderson A 1988 Multi prover interactive proofs: how to remove intractability *Proc. 20th Annu. ACM Symp. on Theory of Computing (STOC '88)* (New York: ACM) pp 113–31

[6] Bennett C, Brassard G and Mermin N 1992 Quantum cryptography without Bell's theorem *Phys. Rev. Lett.* **68** 557–9

[7] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. on Computers, Systems, and Signal Process (Bangalore)* (Piscataway, NJ: IEEE) pp 175–9

[8] Berta M, Christandl M, Colbeck R, Renes J M and Renner R 2010 The uncertainty principle in the presence of quantum memory *Nature Phys.* **6** 659–62

[9] Branciard C, Cavalcanti E G, Walborn S P, Scarani V and Wiseman H M 2012 One-sided device-independent quantum key distribution: security, feasibility and the connection with steering *Phys. Rev.* A **85** 010301
[10] Braunstein S and Pirandola S 2012 Side-channel-free quantum key distribution *Phys. Rev. Lett.* **108** 130502
[11] Bruß D 1998 Optimal Eavesdropping in quantum cryptography with six states *Phys. Rev. Lett.* **81** 3018–21
[12] Buhrman H, Chandran N, Fehr S, Gelles R, Goyal V, Ostrovsky R and Schaffner C 2011 Position-based quantum cryptography: impossibility and constructions *Proc. CRYPTO* pp 429–46 (arXiv:1009.2490v4)
[13] Chandran N, Fehr S, Gelles R, Goyal V and Ostrovsky R 2010 Position-based quantum cryptography arXiv:1005.1750
[14] Chandran N, Goyal V, Moriarty R and Ostrovsky R 2009 Position based cryptography *Advances in Cryptology (CRYTO 2009)* (*Lecture Notes in Computer Science* vol 5677) (Berlin: Springer) pp 391–407
[15] Christandl M and Schuch N 2010 personal communications
[16] Cleve R, Høyer P, Toner B and Watrous J 2004 Consequences and limits of nonlocal strategies *Proc. 19th Conf. on Computational IEEE Complexity* pp 236–49 (arXiv:quant-ph/0404076)
[17] Coles P J, Yu L and Zwolak M 2011 Relative entropy derivation of the uncertainty principle with quantum side informatio arXiv:1105.4865
[18] Deutsch D 1983 Uncertainty in quantum measurements *Phys. Rev. Lett.* **50** 631–3
[19] Einstein A, Podolsky B and Rosen N 1935 Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **47** 777–80
[20] Ekert A K 1991 Quantum cryptography based on Bell's theorem *Phys. Rev. Lett.* **67** 661–3
[21] Feige U and Lovász L 1992 Two-prover one-round proof systems: their power and their problems *Proc. 24th Annu. ACM Symp. on Theory of Computing (STOC '92)* (New York: ACM) pp 733–44
[22] Gisin N, Pironio S and Sangouard N 2010 Proposal for implementing device-independent quantum key distribution based on a Heralded qubit amplifier *Phys. Rev. Lett.* **105** 070501
[23] Hänggi E and Renner R 2010 Device-independent quantum key distribution with commuting measurements arXiv:1009.1833
[24] Hastings M 2009 A counterexample to additivity of minimum output entropy *Nature Phys.* **5** 255
[25] Heisenberg W 1927 Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik *Z. Phys.* **43** 172–98
[26] Holenstein T 2007 Parallel repetition: simplifications and no-signaling case *Proc. 39th Annu. ACM Symp. on Theory of Computing (STOC '07)* (New York: ACM) pp 411–9
[27] Ishizaka S and Hiroshima T 2008 Asymptotic teleportation scheme as a universal programmable quantum processor *Phys. Rev. Lett.* **101** 240501
[28] Ishizaka S and Hiroshima T 2009 Quantum teleportation scheme by selecting one of multiple output ports *Phys. Rev.* A **79** 042306
[29] Ito T and Vidick T 2012 A multi-prover interactive proof for NEXP sound against entangled provers p 47 (arXiv:1207.0550)
[30] Kempe J and Vidick T 2011 Parallel repetition of entangled games *Proc. 43rd Annual STOC* (New York: ACM) pp 353–62
[31] Kent A, Munro W J and Spiller T P 2010 Quantum tagging: authenticating location via quantum information and relativistic signalling constraints arXiv:1008.2147
[32] Kittaneh F 1997 Norm inequalities for certain operator sums *J. Funct. Anal.* **143** 337–48
[33] Klauck H 2010 A strong direct product theorem for disjointness *Proc. 42nd ACM Symp. on Theory of Computing (STOC '10)* (New York: ACM) pp 77–86
[34] König R, Renner R and Schaffner C 2009 The operational meaning of min- and max-entropy *Trans. Inform. IEEE Theory* **55** 4337–47
[35] Krishna M and Parthasarathy K R 2002 An entropic uncertainty principle for quantum measurements *Indian J. Stat.* **64** 842–51
[36] Lau H-K and Lo H-K 2011 Insecurity of position-based quantum-cryptography protocols against entanglement attacks *Phys. Rev.* A **83** 1–12

[37] Lim C C W, Portmann C, Tomamichel M, Renner R and Gisin N 2012 Device-independent quantum key distribution with local Bell test arXiv:1208.0023
[38] Lo H-K, Chau H and Ardehali M 2004 Efficient quantum key distribution scheme and a proof of its unconditional security *J. Cryptol.* **18** 133–65
[39] Lo H-K, Curty M and Qi B 2012 Measurement-device-independent quantum key distribution *Phys. Rev. Lett.* **108** 130503
[40] Lydersen L, Wiechers C, Wittmann C, Elser D, Skaar J and Makarov V 2010 Hacking commercial quantum cryptography systems by tailored bright illumination *Nature Photon.* **4** 686–9
[41] Maassen H and Uffink J 1988 Generalized entropic uncertainty relations *Phys. Rev. Lett.* **60** 1103–6
[42] Malaney R A 2010 Location-dependent communications using quantum entanglement *Phys. Rev.* A **81** 042319
[43] Malaney R A 2010 Quantum location verification in noisy channels arXiv:1004.4689
[44] Masanes L, Pironio S and Acín A 2011 Secure device-independent quantum key distribution with causally independent measurement devices *Nature Commun.* **2** 238
[45] Mayers D 1996 Quantum key distribution and string oblivious transfer in noisy channels *Proc. CRYPTO* (*Lecture Notes in Computer Science* vol 1109) ed N Koblitz (Berlin: Springer) pp 343–57
[46] Mayers D and Yao A 1998 Quantum cryptography with imperfect apparatus *Proc. 39th Annu. Symp. on Foundations of Computer Science* (Washington, DC: IEEE Computer Society) pp 503–509
[47] Pironio S, Masanes L, Leverrier A and Acin A 2012 Device-independent quantum key distribution secure against adversaries with no long-term quantum memory arXiv:1211.1402
[48] Raz R 1998 A parallel repetition theorem *SIAM J. Comput.* **27** 763–803
[49] Reichardt B W, Unger F and Vazirani U 2012 Classical command of quantum systems via rigidity of CHSH Games arXiv:1209.0449
[50] Renner R 2005 Security of quantum key distribution *PhD Thesis* ETH Zurich (arXiv:quant-ph/0512258)
[51] Rényi A 1961 On measures of information and entropy *Proc. Symp. on Mathematical Statistics and Probability* (Berkeley, CA: University of California Press) pp 547–61
[52] Schaffner C 2007 Cryptography in the bounded-quantum-storage model *PhD Thesis* University of Aarhus (arXiv:0709.0289)
[53] Shor P W and Preskill J 2000 Simple proof of security of the BB84 quantum key distribution protocol *Phys. Rev. Lett.* **85** 441–4
[54] Smith G and Yard J 2008 Quantum communication with zero-capacity channels *Science* **321** 1812–5
[55] Terhal B 2004 Is entanglement monogamous? *IBM J. Res. Dev.* **48** 71–8
[56] Tomamichel M 2012 A framework for non-asymptotic quantum information theory *PhD Thesis* ETH Zurich (arXiv:1203.2142)
[57] Tomamichel M and Hänggi E 2013 The link between entropic uncertainty and nonlocality *J. Phys. A: Math. Gen.* **46** 055301
[58] Tomamichel M and Hayashi M 2012 A hierarchy of information quantities for finite block length analysis of quantum tasks arXiv:1208.1478
[59] Tomamichel M, Lim C C W, Gisin N and Renner R 2012 Tight finite-key analysis for quantum cryptography *Nature Commun.* **3** 634
[60] Tomamichel M and Renner R 2011 Uncertainty relation for smooth entropies *Phys. Rev. Lett.* **106** 110506
[61] Vazirani U and Vidick T 2012 Fully device independent quantum key distribution arXiv:1210.1810
[62] Wehner S and Winter A 2010 Entropic uncertainty relations a survey *New J. Phys.* **12** 025009
[63] Wittmann B, Ramelow S, Steinlechner F, Langford N K, Brunner N, Wiseman H M, Ursin R and Zeilinger A 2012 Loophole-free Einstein–Podolsky–Rosen experiment via quantum steering *New J. Phys.* **14** 053030