One-Sided Device-Independent QKD and Position-based Cryptography from Monogamy Games

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

[1] Centre for Quantum Technologies, National University of Singapore
cqtmarco@nus.edu.sg, j.kaniewski@nus.edu.sg, wehner@comp.nus.edu.sg
[2] CWI Amsterdam, The Netherlands
serge.fehr@cwi.nl

Abstract. A serious concern with quantum key distribution (QKD) schemes is that, when under attack, the quantum devices in a real-life implementation may behave differently than modeled in the security proof. This can lead to real-life attacks against provably secure QKD schemes.
In this work, we show that the standard BB84 QKD scheme is *one-sided device-independent*. This means that security holds even if Bob's quantum device is arbitrarily malicious, as long as Alice's device behaves as it should. Thus, we can completely remove the trust into Bob's quantum device *for free*, without the need for changing the scheme, and without the need for hard-to-implement loophole-free violations of Bell inequality, as is required for fully (meaning two-sided) device-independent QKD.
For our analysis, we introduce a new quantum game, called a *monogamy-of-entanglement* game, and we show a strong parallel repetition theorem for this game. This new notion is likely to be of independent interest and to find additional applications. Indeed, besides the application to QKD, we also show a direct application to *position-based quantum cryptography*: we give the first security proof for a one-round position-verification scheme that requires only single-qubit operations.

1 Introduction

Background. Quantum key distribution (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 [5,11]. In principle, the security of QKD can be rigorously proven based solely on the laws of quantum mechanics [27,33,31]; 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 [25].

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

 The version published by Springer-Verlag is available at 10.1007/978-3-642-38348-9_36. The full version of the article, with a slightly different title, is available at http://arxiv.org/abs/1210.4359 and also appeared in New J. Phys. 15 (2013) 103002.

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 [28] as well as [2,1]. After some limited results [26,13], the possibility of DI QKD has recently been shown in the most general case by Reichhardt *et al.* in [30]. 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 *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. [12,24,7,23].

Our Result. 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 [5] 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.

One-sided DI security of BB84 was first claimed in [38]. 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 [37,6] of [38].

One-sided DI security is obviously weaker than fully DI security (as e.g. achieved in [30]). Still, what is interesting is that there is no need for a new scheme — good old BB84 does it. In that sense, we obtain one-sided DI security *for free*. In particular, no hard-to-implement loophole-free Bell tests are needed.

Despite the practical motivation, our result is of theoretical nature. This is because, as in all contemporary fully DI schemes, our analysis (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 [25].

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 6-state scheme). 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 into 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.

Technique. In order to prove one-sided DI security of BB84, we introduce and study a new quantum game, which we call a *monogamy of entanglement* game (or simply a *monogamy* game). This is a game of a specific form, played by three parties, Alice, Bob and Charlie. Of central importance to us is the monogamy game $\mathsf{G}_{\mathrm{BB84}}^{\times n}$, which is as follows.

Preparation Phase: Bob and Charlie agree on and prepare an arbitrary quantum state ρ_{ABC}, where ρ_A consists of n qubits. 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 $\theta \in \{0,1\}^n$ uniformly at random and announces θ to Bob and Charlie. Additionally, she measures every qubit ρ_{A_i} of ρ_A in the computational basis if $\theta_i = 0$, and in the Hadamard basis if $\theta_i = 1$. This results in a bit string $x \in \{0,1\}^n$.

Answer Phase: Bob and Charlie independently form a guess of x by performing measurements (which may depend on θ) on ρ_B and ρ_C, respectively.

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 randomly chosen function f_θ, they could predict the value of $x = f_\theta(k)$ perfectly from k and θ. In quantum mechanics, however, the outcome of a measurement is in general not deterministic, and the well-known uncertainty principle [15] places a limit on how well observers can predict the outcome of incompatible measurements. For instance, if Bob and Charlie were restricted to classical memory (i.e., ρ_B and ρ_C are "empty"), it is not too hard to see that the best strategy gives a winning probability of $(\frac{1}{2} + \frac{1}{2\sqrt{2}})^n \approx 0.85^n$.

In a fully quantum world, however, uncertainty is not quite the end of the story, as indeed Bob and Charlie are allowed to have *quantum* memory. To illustrate the power of such a memory, consider the same game played just between Alice and Bob. As Einstein, Podolsky and Rosen famously observed [10]: 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 is known that quantum entanglement is "monogamous" [34] 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 (see below).

An analysis of our game thus requires a tightrope walk between uncertainty on the one hand, and the monogamy of entanglement on the other. Writing $p_{\text{win}}(\mathsf{G}_{\text{BB84}}^{\times n})$ for the maximal winning probability, maximized over the choice of the initial state ρ_{ABC} and over the measurements performed by Bob and Charlie, we prove that

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

We thus see that, interestingly, monogamy of entanglement wins out entirely, cancelling the power of Bob and Charlie's quantum memory — the optimal winning probability can be achieved without any entanglement at all. We also show a generalization of (1), which upper bounds $p_{\text{win}}(\mathsf{G}_{\text{BB84}}^{\times n})$ for a variant of the game $\mathsf{G}_{\text{BB84}}^{\times n}$ for which Bob and Charlie need to guess the string x only *approximately*.

Our result in particular implies that $p_{\text{win}}(\mathsf{G}_{\text{BB84}}^{\times n}) = p_{\text{win}}(\mathsf{G}_{\text{BB84}})^n$, i.e., *strong parallel repetition* holds. This means that one cannot play n parallel executions of the game $\mathsf{G}_{\text{BB84}} = \mathsf{G}_{\text{BB84}}^{\times 1}$ better than repeating the optimal strategy for one execution n times. Even classically, analyzing the n-fold parallel repetition of games or tasks is typically challenging. In many cases, only non-strong parallel repetition holds, meaning that $p_{\text{win}}(\mathsf{G}^{\times n}) \leq \varepsilon^n$ for some $\varepsilon < 1$, but with $\varepsilon > p_{\text{win}}(\mathsf{G})$. Furthermore, proving such (strong or not) parallel repetition theorems tends to be intriguingly difficult; examples include the parallel repetition of interactive proof systems (see e.g. [29]) or the analysis of communication complexity tasks (see e.g. [19]). 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. [14], entangled non-local games [16], or the question whether an eavesdropper's optimal strategy in QKD is to perform the optimal strategy for each round.

In this light, our proof of (1) is surprisingly simple. It is inspired by techniques due to Kittaneh [18] and uses merely tools from linear algebra. At the core of the

proof is a newly derived operator norm inequality that bounds the norm $\|\sum_i A_i\|$ of the sum of positive semi-definite operators $A_1, \ldots, A_N$ via the respective norms of the square root of pairwise products $A_i A_j$.

In the context of one-sided DI QKD, it turns out that the game $\mathsf{G}_{\mathrm{BB84}}^{\times n}$ pretty much captures an execution of BB84, with Eve playing the role of Charlie, and considering a *gedankenexperiment* where Eve *measures* her quantum side information in order to try to guess the raw key x Alice obtains. Our bound on $p_{\mathrm{win}}(\mathsf{G}_{\mathrm{BB84}}^{\times n})$ then implies that no matter what measurement Bob's device performs, if the outcome of his measurement is strongly correlated to Alice's raw key x, then Eve has a hard time in guessing x. The latter holds for any measurement Eve may perform, and as such it follows that x has lower bounded min-entropy conditioned on Eve's quantum side information. As a consequence, a secret key can be extracted from x using standard techniques.

Further Application. We expect our notion of and our results on monogamy games to find other applications. Indeed, one additional direct application is to *position verification*. Here, we consider a 1-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*, and they are 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.

Position verification and variants thereof (like *distance bounding*) is a rather well-studied problem in the field of wireless security (see e.g. the references in [9]). It was shown in [9] 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 to *copy* information, initially gave hope that we may circumvent the impossibility result using quantum communication. However, such schemes were subsequently broken [17,22] and indeed a general impossibility proof holds [8]: 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 EPR pairs that grows doubly-exponentially in the number of qubits the honest parties exchange. 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 [8,22,3].

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.

In the full version [36], 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.

Outline. In Section 2, we introduce the terminology and notation used throughout this work, and we derive the operator norm inequality that is central to our main result. In Section 3, we discuss the monogamy game $\mathsf{G}_{\mathrm{BB84}}^{\times n}$, prove a strong parallel repetition theorem, and discuss some generalizations. In Section 4, we then make use of these results to prove one-sided DI security of BB84. The application to position verification is given in the full version [36].

2 Technical Preliminaries

Basic Notation and Terminology. We assume the reader to be familiar with the basic concepts of quantum information theory; we merely fix some notation and terminology here.

Let $\mathcal{H}$ be an arbitrary, finite dimensional complex 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 $A \geq B$ 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*

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

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

The most prominent example of a Hilbert space is the qubit space, $\mathcal{H} \equiv \mathbb{C}^2$. The vectors $|0\rangle = \binom{1}{0}$ and $|1\rangle = \binom{0}{1}$ form the *computational* basis, and the vectors $H|0\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $H|1\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$ the *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 $H^{\theta_1}|x_1\rangle \otimes \cdots \otimes H^{\theta_n}|x_n\rangle \in \mathcal{H}$.

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 with the largest eigenvalue of A, and $A \leq B$ implies $\|A\| \leq \|B\|$. Finally, for any block-diagonal operator $A \oplus B$ we have $\|A \oplus B\| = \max\{\|A\|, \|B\|\}$.

We need the following fact. Note that the statement does not hold in general if the projectors are replaced by general positive semi-definite operators.

Lemma 2.1. *Let $P, Q \in \mathcal{P}(\mathcal{H})$ be projectors with $P \leq Q$, and let $L \in \mathcal{L}(\mathcal{H})$. Then, it holds that $\|PL\| \leq \|QL\|$ and $\|LP\| \leq \|LQ\|$.*

Proof. $\|PL\|^2 = \|L^\dagger P^\dagger PL\| = \|L^\dagger PL\| \leq \|L^\dagger QL\| = \|L^\dagger Q^\dagger QL^\dagger\| = \|QL\|^2$, and the proof of the second statement follows analogously. □

Applying the lemma twice, we get $\|PQ\|^2 \leq \|P'Q\|^2 \leq \|P'Q'\|^2 = \|P'Q'P'\|$ for any two pairs of projectors satisfying $P \leq P'$ and $Q \leq Q'$.

One of our main tools is the following Lemma 2.2, 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 [18], which was also used by Schaffner [32] 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 $i \in [N]$. The N cyclic shifts for instance form a set of N permutations of $[N]$ that are mutually orthogonal.

Lemma 2.2. *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,*

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

Proof. We define $X = [X_{ij}]$ as the $N \times N$ block-matrix with blocks given by $X_{ij} = \delta_{j1}\sqrt{A_i}$. The two matrices $X^\dagger X$ and $XX^\dagger$ are easy to evaluate, namely $(X^\dagger X)_{ij} = \delta_{i1}\delta_{j1}\sum_i A_i$ and $(XX^\dagger)_{ij} = \sqrt{A_i}\sqrt{A_j}$, respectively. As such, we see that $\left\|\sum_i A_i\right\| = \|X^\dagger X\| = \left\|XX^\dagger\right\|$.

Next, we decompose $XX^\dagger$ into $XX^\dagger = D_1 + D_2 + \ldots D_N$, where the matrices D_k are defined by the permutations π^k, respectively, as $(D_k)_{ij} = \delta_{j,\pi^k(i)}\sqrt{A_i}\sqrt{A_j}$. The requirement on the permutations 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 $D'_k = \bigoplus_i \sqrt{A_i}\sqrt{A_{\pi^k(i)}}$ by a unitary rotation. Hence, using triangle inequality and the unitary invariance of the norm, we get $\left\|\sum_k A_k\right\| = \left\|XX^\dagger\right\| \leq \sum_k \|D_k\| = \sum_k \|D'_k\| = \sum_k \max_i \left\|\sqrt{A_i}\sqrt{A_{\pi^k(i)}}\right\|$. □

CQ-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 [31] 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 [20] $H_{\min}(X|B)_\rho := -\log p_{\text{guess}}(X|B)_\rho$, where

$$p_{\text{guess}}(X|B)_\rho := \max_{\{N_x\}_x} \sum_x p_x \operatorname{tr}(\rho_B^x N_x).$$

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 $\rho_{XB\Theta} = \sum_\theta p_\theta |\theta\rangle\langle\theta| \otimes \rho_{XB}^\theta$ for CQ states ρ_{XB}^θ. The min-entropy of X conditioned on B and Θ then evaluates to $H_{\min}(X|B\Theta)_\rho = -\log p_{\text{guess}}(X|B\Theta)_\rho$, where $p_{\text{guess}}(X|B\Theta)_\rho = \sum_\theta p_\theta \, p_{\text{guess}}(X|B)_{\rho^\theta}$. 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 [35]. We merely point out the *chain rule* here: for a CQ-state $\rho_{XB\Theta}$ with classical X and Θ, where Θ is over $\{0,1\}^n$, it holds that $H_{\min}(X|B\Theta)_\rho \geq H_{\min}(X|B)_\rho - n$.

3 Parallel Repetition of Monogamy Games

In this section, we formalize the notion of a monogamy game, and we show strong parallel repetition for the game $\mathsf{G}_{\text{BB84}}^{\times n}$. Then, we generalize our analysis to arbitrary projective measurements for Alice, and to the case where Bob and Charlie are allowed to make some errors.

Definition 3.1. *A* monogamy-of-entanglement game G *consists of a finite dimensional Hilbert space* $\mathcal{H}_A$ *and a list of projective measurements* $\mathcal{M}^\theta = \{F_x^\theta\}_{x\in\mathcal{X}}$ *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 $\{F_{x_1}^{\theta_1} \otimes \cdots \otimes F_{x_n}^{\theta_n}\}_{x_1,\ldots,x_n}$ for $\theta_1, \ldots, \theta_n \in \Theta$, is again a monogamy game.

Definition 3.2. *We define a* strategy $\mathcal{S}$ *for a monogamy game* G *as a list*

$$\mathcal{S} = \left\{\rho_{ABC},\, P_x^\theta,\, Q_x^\theta\right\}_{\theta\in\Theta, x\in\mathcal{X}}, \tag{2}$$

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 $\theta \in \Theta$, $\{P_x^\theta\}_{x\in\mathcal{X}}$ and $\{Q_x^\theta\}_{x\in\mathcal{X}}$ 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 $\rho_{A_1\dots A_n BC} \in \mathcal{S}(\mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B \otimes \mathcal{H}_C)$ (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 $\{P_x^\theta\}_x$ and $\{Q_x^\theta\}_x$. The optimal winning probability, $p_{\text{win}}(\mathsf{G})$, maximizes the winning probability over all strategies. The following makes this formal.

Definition 3.3. *The winning probability for a monogamy game G and a strategy $\mathcal{S}$ is defined as*

$$p_{\text{win}}(\mathsf{G}, \mathcal{S}) := \sum_{\theta\in\Theta} \frac{1}{|\Theta|} \operatorname{tr}\big(\Pi^\theta \rho_{ABC}\big), \quad \text{where} \quad \Pi^\theta := \sum_{x\in\mathcal{X}} F_x^\theta \otimes P_x^\theta \otimes Q_x^\theta \,. \tag{3}$$

The optimal winning probability is $p_{\text{win}}(\mathsf{G}) := \sup_{\mathcal{S}}\ p_{\text{win}}(\mathsf{G}, \mathcal{S})$, 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. [36]).

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 shows the exact value of $p_{\text{win}}(\mathsf{G}_{\text{BB84}}^{\times n})$, and in particular it shows strong parallel repetition.

Theorem 3.4. *For any $n \in \mathbb{N}$, $n \geq 1$, we have*

$$p_{\text{win}}(\mathsf{G}_{\text{BB84}}^{\times n}) = \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n . \tag{4}$$

Proof. We first show that this 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 $\mathcal{S}_1 = \big\{|\phi\rangle\langle\phi|, P_x^\theta = \delta_{x0}, Q_x^\theta = \delta_{x0}\big\}$. The optimal winning probability is bounded by the winning probability of this strategy,

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

and the lower bound in Eq. (4) follows by repeating this simple strategy n times.

To show that this simple strategy is optimal, let us now fix an arbitrary, pure strategy $\mathcal{S}_n = \{\rho_{A_1\dots A_n BC}, P_x^\theta, Q_x^\theta\}$. From the definition of the norm, we have $\mathrm{tr}(M\rho_{ABC}) \leq \|M\|$ for any $M \geq 0$. Using this and Lemma 2.2, we find

$$p_{\mathrm{win}}(\mathsf{G}_{\mathrm{BB84}}^{\times n}, \mathcal{S}_n) \leq \frac{1}{2^n}\Big\|\sum_\theta \Pi^\theta\Big\| \leq \frac{1}{2^n}\sum_k \max_\theta \big\|\Pi^\theta \Pi^{\pi^k(\theta)}\big\|, \tag{5}$$

where the optimal permutations π^k are to be determined later. Hence, the problem is reduced to bounding the norms $\big\|\Pi^\theta \Pi^{\theta'}\big\|$, where $\theta' = \pi^k(\theta)$. The trivial upper bound on these norms, 1, leads to $p_{\mathrm{win}}(\mathsf{G}_{\mathrm{BB84}}^{\times n}, \mathcal{S}_n) \leq 1$. 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' (i.e., $t = |\mathcal{T}|$). 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 $|x_{\mathcal{T}}^\theta\rangle$ 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 $\Pi^\theta \leq \bar{P}$ and $\Pi^{\theta'} \leq \bar{Q}$, we can bound $\big\|\Pi^\theta \Pi^{\theta'}\big\|^2 \leq \big\|\bar{P}\bar{Q}\bar{P}\big\|$ using Lemma 2.1. Moreover,

$$\begin{aligned}
\bar{P}\bar{Q}\bar{P} &= \sum_{x,y,z} |x_{\mathcal{T}}^\theta\rangle\langle x_{\mathcal{T}}^\theta|\, y_{\mathcal{T}}^{\theta'}\rangle\langle y_{\mathcal{T}}^{\theta'}|\, z_{\mathcal{T}}^\theta\rangle\langle z_{\mathcal{T}}^\theta| \otimes 1_{\mathcal{T}^c} \otimes P_x^\theta P_z^\theta \otimes Q_y^{\theta'} \\
&= \sum_{x,y} |\langle x_{\mathcal{T}}^\theta | y_{\mathcal{T}}^{\theta'}\rangle|^2\, |x_{\mathcal{T}}^\theta\rangle\langle x_{\mathcal{T}}^\theta| \otimes 1_{\mathcal{T}^c} \otimes P_x^\theta \otimes Q_y^{\theta'} \\
&= 2^{-t} \sum_x |x_{\mathcal{T}}^\theta\rangle\langle x_{\mathcal{T}}^\theta| \otimes 1_{\mathcal{T}^c} \otimes P_x^\theta \otimes 1_C,
\end{aligned}$$

where we used that $P_x^\theta P_z^\theta = \delta_{xz} P_x^\theta$ and $|\langle x_{\mathcal{T}}^\theta | y_{\mathcal{T}}^{\theta'}\rangle|^2 = 2^{-t}$. 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 $\big\|\Pi^\theta \Pi^{\theta'}\big\| \leq \sqrt{2^{-t}}$. 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 (5), 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 Eq. (5) evaluates to

$$\frac{1}{2^n}\sum_k \max_\theta \big\|\Pi^\theta \Pi^{\pi^k(\theta)}\big\| \leq \frac{1}{2^n}\sum_{t=0}^n \binom{n}{t}\Big(\frac{1}{\sqrt{2}}\Big)^t = \Big(\frac{1}{2} + \frac{1}{2\sqrt{2}}\Big)^n.$$

As this bound applies to all pure strategies, we conclude the proof. □

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 projective measurements $\{F_x^\theta\}_{x\in\mathcal{X}}$, 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, $c(\mathsf{G}) := \max \|F_x^\theta F_{x'}^{\theta'}\|^2$, where the max is over all $\theta \neq \theta' \in \Theta$ and all $x, x' \in \mathcal{X}$. $c(\mathsf{G})$ satisfies $1/|\mathcal{X}| \leq c(\mathsf{G}) \leq 1$ 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 [21]. 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 3.4 to the case where Bob and Charlie are not required to guess *perfectly* but are allowed to make some errors. The maximal winning probability in this case is defined as follows, where we again restrict to pure strategies.

Definition 3.5. *Let $\mathcal{Q} = \{(\pi_B^q, \pi_C^q)\}_q$ 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*

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

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 3.4. The proof closely follows the proof of the upper bound in Theorem 3.4, and is deferred to the full version [36].

Theorem 3.6. *For any positive $n \in \mathbb{N}$, we have*

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

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 3.4.

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 $d(x,y) \leq \gamma\, n$ and $d(x,z) \leq \gamma'\, n$, where $d(\cdot,\cdot)$ denotes the Hamming distance and y, z are Bob's and Charlie's guesses, respectively. In this case, we let $\mathcal{Q}^n_{\gamma,\gamma'}$ consist of 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 γ and γ', respectively. One can upper bound $|\mathcal{Q}^n_{\gamma,\gamma'}| \leq 2^{nh(\gamma)+nh(\gamma')}$, where $h(\cdot)$ denotes the binary entropy. We thus find

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

4 Application: One-Sided Device-Independent QKD

In the following, we assume some familiarity with quantum key distribution (QKD). For simplicity, we consider an entanglement-based [11] variant of the BB84 QKD scheme [5], 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 [4]. It is straightforward to verify that this implication also holds in the one-sided device-independent 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 $0 \leq \gamma < \frac{1}{2}$. 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, and ℓ is the length (in bits) of the final key. Finally, γ is the tolerated error in Bob's measurement results.

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 universal$_2$ hash function $F : \{0,1\}^{n-t} \to \{0,1\}^\ell$ 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}.

Fig. 1. An entanglement-based QKD scheme **E-QKD**.

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

$$\Pr_{\rho}[K \neq \perp] \cdot \Delta(\rho_{KE^+|K\neq\perp}, \mu_K \otimes \rho_{E^+|K\neq\perp}) \leq \delta\,. \tag{6}$$

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.

Theorem 4.1. *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*

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

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 $\log(1/\beta_\circ) > 2h(\gamma)$, which roughly requires that $\gamma \leq 0.015$. Hence, the scheme can tolerate a noise level up to 1.5% asymptotically.[3]

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 $\rho_{\Theta TABE} = \rho_\Theta \otimes \rho_T \otimes |\psi_{ABE}\rangle\langle\psi_{ABE}|$ 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 Fig. 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.[4] For this purpose, we consider an arbitrary measurement strategy

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

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

of Eve that aims to guess X. Such a strategy is given by — for 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

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

with $\beta = 2^{h(\gamma+\varepsilon)} \cdot \beta_\circ$, 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.

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

where Ω denotes the event $\Omega = \{d_{\mathrm{rel}}(X,Y) \leq d_{\mathrm{rel}}(X_T,Y_T) + \varepsilon\}$, 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 $\Delta(\rho_{\Theta TXYE}, \tilde{\rho}_{\Theta TXYE}) \leq 1 - \Pr_\rho[\Omega]$, and by Hoeffding's inequality,

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

Moreover, note that the event $d_{\mathrm{rel}}(X_T,Y_T) \leq \gamma$ implies $d_{\mathrm{rel}}(X,Y) \leq \gamma + \varepsilon$ 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

$$\begin{aligned} \Pr_{\tilde{\rho}}[d_{\mathrm{rel}}(X_T,Y_T) \leq \gamma \wedge Z=X] &\leq \Pr_{\tilde{\rho}}[d_{\mathrm{rel}}(X,Y) \leq \gamma+\varepsilon \wedge Z=X] \\ &\leq \Pr_\rho[d_{\mathrm{rel}}(X,Y) \leq \gamma+\varepsilon \wedge Z=X] \leq \beta^n. \end{aligned} \tag{7}$$

We now introduce the event $\Gamma = \{d_{\mathrm{rel}}(X_T,Y_T) \leq \gamma\}$, which corresponds to the event that Bob does not abort the protocol. Expanding the left hand side of (7) 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

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

where $\alpha \geq 0$ is determined by $\Pr_{\tilde{\rho}}[\Gamma] = \beta^{\alpha n}$. Therefore, by definition of the min-entropy, $H_{\min}(X|\Theta TE,\Gamma)_{\tilde{\rho}} \geq n(1-\alpha)\log(1/\beta)$. (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

$$\begin{aligned} H_{\min}(X|\Theta T X_T S E, \Gamma)_{\tilde{\rho}} &\geq H_{\min}(X X_T S|\Theta T E, \Gamma)_{\tilde{\rho}} - t - s \\ &\geq n(1-\alpha)\log(1/\beta) - t - s\,. \end{aligned} \tag{8}$$

Here, the min-entropy is evaluated for the state $\tilde{\rho}_{X\Theta T X_T S E}$ that is constructed from $\tilde{\rho}_{X\Theta T E}$ by calculating the error syndrome and copying X_T from X as done in the prescription of the protocol. In particular, $\Delta(\tilde{\rho}_{X\Theta T X_T S E}, \rho_{X\Theta T X_T S E}) \leq e^{-2\varepsilon^2 t}$. 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 [31]

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

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

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

Using $\beta = 2^{h(\gamma+\varepsilon)}\beta_\circ$ and applying Lemma 4.2 below concludes the proof. □

Lemma 4.2. *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*

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

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

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

which proves the claim. □

References

1. A. Acín, N. Brunner, N. Gisin, S. Massar, S. Pironio, and V. Scarani. Device-Independent Security of Quantum Cryptography against Collective Attacks. *Phys. Rev. Lett.*, 98(23), 2007. DOI: 10.1103/PhysRevLett.98.230501.
2. J. Barrett, L. Hardy, and A. Kent. No Signaling and Quantum Key Distribution. *Phys. Rev. Lett.*, 95(1), June 2005. DOI: 10.1103/PhysRevLett.95.010503.
3. S. Beigi and R. König. Simplified Instantaneous Non-Local Quantum Computation with Applications to Position-Based Cryptography. *New J. Phys.*, 13(9):093036, Sept. 2011. DOI: 10.1088/1367-2630/13/9/093036.
4. C. Bennett, G. Brassard, and N. Mermin. Quantum Cryptography Without Bell's Theorem. *Phys. Rev. Lett.*, 68(5):557–559, Feb. 1992. DOI: 10.1103/PhysRevLett.68.557.
5. C. H. Bennett and G. Brassard. Quantum Cryptography: Public Key Distribution and Coin Tossing. In *Proc. IEEE Int. Conf. on Comp., Sys. and Signal Process.*, pages 175–179, Bangalore, 1984. IEEE.
6. C. Branciard, E. G. Cavalcanti, S. P. Walborn, V. Scarani, and H. M. Wiseman. One-sided device-independent quantum key distribution: Security, feasibility, and the connection with steering. *Phys. Rev. A*, 85(1):010301, Jan. 2012. DOI: 10.1103/PhysRevA.85.010301.
7. S. Braunstein and S. Pirandola. Side-Channel-Free Quantum Key Distribution. *Phys. Rev. Lett.*, 108(13):130502, Mar. 2012. DOI: 10.1103/PhysRevLett.108.130502.
8. H. Buhrman, N. Chandran, S. Fehr, R. Gelles, V. Goyal, R. Ostrovsky, and C. Schaffner. Position-Based Quantum Cryptography: Impossibility and Constructions. In *Proc. CRYPTO*, pages 429–446, 2011. arXiv: 1009.2490v4.
9. N. Chandran, V. Goyal, R. Moriarty, and R. Ostrovsky. Position Based Cryptography. In *Proc. CRYPTO*, pages 391–407, 2009.
10. A. Einstein, B. Podolsky, and N. Rosen. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Phys. Rev.*, 47(10):777–780, May 1935. DOI: 10.1103/PhysRev.47.777.
11. A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67(6):661–663, Aug. 1991. DOI: 10.1103/PhysRevLett.67.661.
12. N. Gisin, S. Pironio, and N. Sangouard. Proposal for Implementing Device-Independent Quantum Key Distribution Based on a Heralded Qubit Amplifier. *Phys. Rev. Lett.*, 105(7), Aug. 2010. DOI: 10.1103/PhysRevLett.105.070501.
13. E. Hänggi and R. Renner. Device-Independent Quantum Key Distribution with Commuting Measurements. Sept. 2010. arXiv: 1009.1833.
14. M. Hastings. A counterexample to additivity of minimum output entropy. *Nature Physics*, 5:255, 2009.
15. W. Heisenberg. Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik. *Z. Phys.*, 43(3-4):172–198, Mar. 1927.
16. J. Kempe and T. Vidick. Parallel repetition of entangled games. In *Proceedings of the 43rd annual ACM STOC*, pages 353–362, New York, NY, USA, 2011. ACM.
17. A. Kent, W. J. Munro, and T. P. Spiller. Quantum Tagging: Authenticating Location via Quantum Information and Relativistic Signalling Constraints. Aug. 2010. arXiv: 1008.2147.
18. F. Kittaneh. Norm Inequalities for Certain Operator Sums. *Journal of Functional Analysis*, 143(2):337–348, Feb. 1997. DOI: 10.1006/jfan.1996.2957.
19. H. Klauck. A strong direct product theorem for disjointness. In *Proceedings of 42nd ACM STOC*, 2010.

20. R. König, R. Renner, and C. Schaffner. The Operational Meaning of Min- and Max-Entropy. *IEEE Trans. on Inf. Theory*, 55(9):4337–4347, Sept. 2009. DOI: 10.1109/TIT.2009.2025545.
21. M. Krishna and K. R. Parthasarathy. An Entropic Uncertainty Principle for Quantum Measurements. *Indian J. Stat.*, 64(3):842–851, Oct. 2002.
22. H.-K. Lau and H.-K. Lo. Insecurity of position-based quantum-cryptography protocols against entanglement attacks. *Phys. Rev. A*, 83(1):1–12, Jan. 2011. DOI: 10.1103/PhysRevA.83.012322.
23. C. C. W. Lim, C. Portmann, M. Tomamichel, R. Renner, and N. Gisin. Device-Independent Quantum Key Distribution with Local Bell Test. July 2012. arXiv: 1208.0023.
24. H.-K. Lo, M. Curty, and B. Qi. Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.*, 108(13):130503, Mar. 2012. DOI: 10.1103/PhysRevLett.108.130503.
25. L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photon.*, 4(10):686–689, Aug. 2010. DOI: 10.1038/nphoton.2010.214.
26. L. Masanes, S. Pironio, and A. Acín. Secure device-independent quantum key distribution with causally independent measurement devices. *Nat. Commun.*, 2:238, Mar. 2011. DOI: 10.1038/ncomms1244.
27. D. Mayers. Quantum Key Distribution and String Oblivious Transfer in Noisy Channels. In *Proc. CRYPTO*, volume 1109 of *LNCS*, pages 343–357. Springer, 1996.
28. D. Mayers and A. Yao. Quantum Cryptography with Imperfect Apparatus. In *Proc. FOCS*, pages 503–509, 1998.
29. R. Raz. A parallel repetition theorem. *SIAM Journal on Computing*, 27:763–803, 1998.
30. B. W. Reichardt, F. Unger, and U. Vazirani. Classical Command of Quantum Systems via Rigidity of CHSH Games. Sept. 2012. arXiv: 1209.0449.
31. R. Renner. *Security of Quantum Key Distribution*. PhD thesis, ETH Zurich, Dec. 2005. arXiv: quant-ph/0512258.
32. C. Schaffner. *Cryptography in the Bounded-Quantum-Storage Model*. Phd thesis, University of Aarhus, Sept. 2007. arXiv: 0709.0289.
33. P. Shor and J. Preskill. Simple Proof of Security of the BB84 Quantum Key Distribution Protocol. *Phys. Rev. Lett.*, 85(2):441–444, July 2000. DOI: 10.1103/PhysRevLett.85.441.
34. B. Terhal. Is Entanglement Monogamous? *IBM J Reasearch and Development*, 48(1):71–78, 2004.
35. M. Tomamichel. *A Framework for Non-Asymptotic Quantum Information Theory*. PhD thesis, ETH Zurich, Mar. 2012. arXiv: 1203.2142.
36. M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner. Strong Parallel Repetition for a Monogamy-of-Entanglement Game. Oct. 2012. arXiv: 1210.4359.
37. M. Tomamichel and M. Hayashi. A Hierarchy of Information Quantities for Finite Block Length Analysis of Quantum Tasks. Aug. 2012. arXiv: 1208.1478.
38. M. Tomamichel and R. Renner. Uncertainty Relation for Smooth Entropies. *Phys. Rev. Lett.*, 106(11), Mar. 2011. DOI: 10.1103/PhysRevLett.106.110506.