

Computational Monogamy of Entanglement and Non-Interactive Quantum Key Distribution

Alex B. Grilo¹, Giulio Malavolta², Michael Walter^{3,4,5}, and Tianwei Zhang^{3,6}

¹ Sorbonne Université, CNRS, LIP6

² Bocconi University

³ Faculty of Computer Science, Ruhr University Bochum

⁴ Korteweg-de Vries Institute for Mathematics and QuSoft, University of Amsterdam

⁵ Faculty of Physics, Ludwig Maximilian University of Munich

⁶ Max Planck Institute for Security and Privacy

Abstract. Quantum key distribution (QKD) enables Alice and Bob to exchange a secret key over a public, untrusted quantum channel. Compared to classical key exchange, QKD achieves *everlasting security*: after the protocol execution the key is secure against adversaries that can do unbounded computations. On the flip side, while classical key exchange can be achieved non-interactively (with two simultaneous messages between Alice and Bob), no non-interactive protocol is known that provides everlasting security, even using quantum information.

In this work, we make progress on this problem. Our main technical contribution is a *computational* variant of the celebrated *monogamy of entanglement* game, where the secret is only computationally hidden from the players, rather than information-theoretically. In these settings, we prove a negligible bound on the maximal winning probability over all strategies. As a direct application, we obtain a non-interactive (simultaneous message) QKD protocol from any post-quantum classical non-interactive key exchange, which satisfies everlastingly secure *assuming Alice and Bob agree on the same key*. The protocol only uses EPR pairs and standard and Hadamard basis measurements, making it suitable for near-term quantum hardware. We also propose how to convert this protocol into a two-round protocol that satisfies the standard notion of everlasting security.

Finally, we prove a *no-go theorem* which establishes that (in contrast to the case of ordinary multi-round QKD) entanglement is necessary for non-interactive QKD, i.e., the messages sent by Alice and Bob cannot both be unentangled with their respective quantum memories if the protocol is to be everlastingly secure.

1 Introduction

Quantum key distribution (QKD) [1] enables two parties, commonly referred to as Alice and Bob, to securely exchange a secret key over a public, untrusted quantum channel. In contrast to classical key exchange protocols, QKD offers two main advantages: (i) It requires only authenticated classical channels, which can

be practically implemented using Minicrypt [11] computational assumptions (in contrast, it is widely believed that such assumptions are not sufficient for classical key exchange [12]). (ii) It guarantees *everlasting security*: Even if an adversary becomes unbounded after the protocol execution, no information about the key is leaked. This prevents attacks where the adversary records data to leverage future technological/algorithmic breakthroughs.

Given the fundamental nature of the problem, it is not surprising that QKD has become one of the most well-studied topics in the theory of quantum information [21,18,20,23,19] and in the experimental community [13,16,28]. It is known that three messages are sufficient for building QKD [24]. A recent work [19] achieved the first two-message protocol for QKD with everlasting security, assuming the existence of (quantum-secure) one-way functions.⁷ Two messages are optimal for QKD, but in their protocol, Bob has to send his message after receiving the message from Alice. Therefore, their protocol still requires two rounds of communication – in contrast to classical key exchange, which can be achieved *non-interactively*, that is, using a single round of two *simultaneous messages* between Alice and Bob [6] This prompts the question:

*Can quantum protocols match the round complexity of classical protocols,
while still achieving everlasting security?*

The purpose of this work is to make progress on this question.

1.1 Our Results

In this work we consider the problem of *non-interactive QKD*: we seek a protocol between Alice and Bob that consists of a *single round* of simultaneous messages where, at the end of the interaction, Alice and Bob agree on a secret key. We consider an attacker that is computationally bounded during the execution of the protocol, but afterwards can perform arbitrary (computationally unbounded) computations. In this setting, we present both positive and negative results.

Constructions. On the positive side, we show how to construct a non-interactive QKD protocol from any post-quantum classical non-interactive key exchange (NIKE). The latter can be achieved from a variety of assumptions, including the hardness of the learning with errors (LWE) problem [9] or of computational problems related to isogenies in elliptic curves [5]. Our protocol satisfies a weak notion of *everlasting security*: roughly speaking, it everlasting security holds provided Alice and Bob agree on the same shared key.⁸ Furthermore, in our protocol, only the message sent from Alice to Bob is quantum, while Bob’s message is entirely classical.

⁷ The same work also shows that computational assumptions are necessary in the two-message settings.

⁸ More precisely we show a notion of *search* hardness, i.e., we prove that the shared key of Alice and Bob is hard to guess, conditioned on Alice and Bob agreeing on the same key. We keep this aspect deliberately informal at this point, and we will make things more precise in the subsequent sections.

Our security proof relies on a *computational* variant of the *monogamy-of-entanglement game* of [25]. While in the original game a random basis choice θ is informationally hidden until the parties have agreed on a quantum state, in our game the basis choice is only *computationally* hidden (that is, it is only hidden for efficient algorithms). The game proceeds by Alice, Bob, and Charlie jointly applying an efficient algorithm that prepares a shared quantum state of their systems ABC . Then Alice and Bob measure A and B in the θ -basis to obtain outcomes K_A and K_B , respectively, while Charlie is allowed to apply an arbitrary (possibly inefficient) measurement to obtain outcome K_C . The players win if $K_A = K_B = K_C$. We describe the game more formally in the technical outline below (Section 1.2). Our main technical contribution is the following theorem, which can be understood as a computational monogamy of entanglement result:

Theorem 1 (Informal). *If θ is computationally hidden, the winning probability of the players in the above-described computational monogamy-of-entanglement game is negligible.*

We believe that this result may be of independent interest and find other applications. As a corollary, we obtain the following non-interactive QKD protocol:

Theorem 2 (Informal). *Assuming the hardness of the LWE problem (or any other assumption that implies the existence of a post-quantum NIKE), there exists a non-interactive QKD protocol that offers everlasting security when Alice and Bob agree on the same key.*

Thus, we identify a natural and meaningful setting under which truly non-interactive QKD is possible to achieve with everlasting security, which was not known prior to our work. At the quantum level, our protocol only uses EPR pairs, and Alice and Bob measure their state as soon as they receive each other's message. This makes our protocol a plausible candidate for experimental validation, using existing or near-term quantum hardware.

We furthermore propose how to achieve the standard notion of everlasting security by a two-round simultaneous-message protocol that builds on top of our non-interactive protocol and has essentially the same complexity. In particular, our two-round protocol still only uses EPR pairs – in contrast to [19] which used entangled states of $\text{poly}(\lambda)$ many qubits. However, while the protocol of [19] uses only two messages in total and only assumes the existence of post-quantum one-way functions, our new two-round protocol uses four messages in total and requires the existence of a post-quantum NIKE, which is considered a stronger assumption. The question of the existence of a non-interactive QKD scheme (with two simultaneous messages, one from Alice and one from Bob) that achieves the standard notion of everlasting security, as posed in [19], remains open.

No-go Result. While traditional QKD protocols can achieve security by sending single-qubit states, our non-interactive protocol requires Alice to create EPR pairs and store one qubit of each pair until she receives Bob's message. While experimentally more challenging, we show that this to some extent unavoidable:

Theorem 3 (Informal). *A perfectly-correct non-interactive QKD protocol can only be everlastingly secure if it uses entanglement.*

We prove this result by exhibiting an attack that does not disturb the quantum states and allows the attacker to learn the key with constant probability.

1.2 Technical Outline

Non-Interactive QKD and Weak Everlasting Security. Before explaining our approach, let us make the scenario more concrete. We consider a setting where Alice and Bob exchange a single round of simultaneous messages, each consisting of a classical and quantum part. While all classical messages are delivered honestly, to model the presence of an authenticated classical channel, the quantum channel is fully untrusted: the attacker can apply an arbitrary quantum polynomial time (QPT) channel to manipulate the quantum messages (and entangle them with his own register) before they get delivered to Alice and Bob. Once the protocol is completed, i.e., Alice and Bob have derived their local key K_A and K_B , the attacker becomes computationally unbounded and can perform arbitrary computations in order to try to guess the key. We say that the attacker succeeds if their guess is correct and furthermore $K_A = K_B$ (Alice and Bob agree on the same key). We define *weak everlasting security* to mean that attackers succeed only with negligible probability.

The Protocol Blueprint. The template for our protocol is quite natural: We combine the celebrated QKD protocol of [1] with a *classical* post-quantum non-interactive key exchange (NIKE), where the key is used to select the secret basis:

- *Alice:* Samples a key pair using the classical NIKE protocol, and prepares n EPR pairs $|\text{EPR}\rangle^{\otimes n} = \left(\frac{|00\rangle + |11\rangle}{\sqrt{2}}\right)^{\otimes n}$, then she sends her classical public key, along with the second qubit of each EPR pair, to Bob.
- *Bob:* Samples a key pair using the classical NIKE protocol and sends his public key to Alice.
- *Outputs:* Alice uses her private key and Bob’s public key to derive a classical shared key $\theta_A \in \{0, 1\}^n$. Then she measures her qubits in the θ_A -basis: she measures her j -th qubit in the standard basis if $\theta_{A,j} = 0$ and otherwise in the Hadamard basis. Alice sets $K_A \in \{0, 1\}^n$ to be the bitstring containing the measurement outcomes.
Bob proceeds identically, by using his private key and Alice’s public key to derive a classical shared key θ_B and obtaining K_B as the measurement outcomes of the θ_B -basis measurement on his qubits.

Correctness follows from correctness of the NIKE, since if Alice and Bob agree on the same basis $\theta_A = \theta_B$, then they measure their EPR pairs in the same basis, resulting in the same outcomes.

However, proving security is much less obvious. One standard approach would be to appeal to a *monogamy of entanglement* game in the spirit of [25]. We will

elaborate more on this later, but for the moment it suffices to say that known statements are *information-theoretic*, i.e., they crucially use the assumption that even computationally-unbounded adversaries have no information about the basis θ . In our setting this is rather not true: Because of classical NIKE protocol is only computationally secure, the basis choice is only computationally hidden (that is, hidden from efficient quantum adversaries), but not information-theoretically so. To use the computational security of the NIKE, we therefore need a computational argument, i.e., an *efficient* reduction. However, simple reduction strategies do not seem to work either: we cannot just switch the basis θ to a uniform string and appeal to the security of the NIKE protocol, because in the second stage the adversary's power is *unbounded*. Therefore, running the entire adversary as part of a reduction would take the reduction unbounded time, making the security guarantees of the classical NIKE protocol not applicable. Therefore, while our strategy ought to appeal to the computational security of the NIKE, it has to do so in an indirect manner.

Computational Monogamy of Entanglement. We formalize our solution in a more abstract scenario, by defining and analyzing a computational variant of the monogamy-of-entanglement game of [25].

We assume the existence of an efficiently-sampleable distribution $\mathcal{Z}(1^\lambda)$ supported on pairs $(p, \theta) \in \mathcal{P}_\lambda \times \{0, 1\}^{n(\lambda)}$ for some polynomial $n = n(\lambda)$. We require that the following distributions are computationally indistinguishable:

$$((p, \theta) : (p, \theta) \leftarrow \mathcal{Z}(1^\lambda)) \approx_c ((p, \theta^*) : (p, \cdot) \leftarrow \mathcal{Z}(1^\lambda); \theta^* \leftarrow \{0, 1\}^n). \quad (1)$$

The game proceeds as follows:

1. *Sampling Phase:* Alice samples $(p, \theta) \leftarrow \mathcal{Z}(1^\lambda)$ and reveals p to Bob and Charlie.
2. *Efficient Preparation Phase:* Alice, Bob, and Charlie jointly apply a QPT algorithm (with input p) to create a shared quantum state between their registers A, B, C . Registers A and B should consist of $n(\lambda)$ qubits, while C can be arbitrary.
3. *Question Phase:* Alice measures register A in the θ -basis to obtain an outcome K_A . She then reveals θ to Bob and Charlie.
4. *Semi-Honest Answer Phase:* Bob measures register B in the θ -basis to obtain an outcome K_B , while Charlie can apply an arbitrary (possibly inefficient) measurement of register C to obtain an outcome K_C .

The players win the game if $K_A = K_B = K_C$.

The key differences to the original monogamy-of-entanglement game of [25] are as follows: Most significantly for us, in our game Bob and Charlie have some information P about θ *before* creating their shared entangled state, which is not the case in [25]. On the other hand, we require the shared state to be efficiently preparable, and we also assume that Bob's measurement in the answer phase is performed honestly, whereas in [25] is an arbitrary POVM.

Note that this game is a good model for the non-interactive QKD protocol described above: Charlie essentially plays the role of the attacker; in the preparation phase, Alice creates n EPR pairs, and Charlie applies an arbitrary efficient quantum channel to create systems B and C .

To prove a bound on the success probability in the above game, we consider the following thought experiment: Let ρ_{AB} be the joint state of Alice and Bob, right before the question phase. We split the state into n/s blocks, each of size s (we have some freedom in the choice of parameters, but for this overview it suffices to take $s = \sqrt{n}$). Then we imagine applying the binary POVM $\{M_{AB}^{(0)}, M_{AB}^{(1)}\}$ given by

$$M_{AB}^{(1)} = \left(I - |\text{EPR}\rangle\langle\text{EPR}|^{\otimes s} \right)^{\otimes \frac{n}{s}}, \quad M_{AB}^{(0)} = I - M_{AB}^{(1)}.$$

If the measurement outcome is 0, then, *roughly speaking*, we project the state ρ_{AB} onto a state that has *at least* s EPR pairs shared between Alice and Bob. Indeed we can prove that in this case, no matter what Charlie does, his probability of guessing Alice and Bob's outcomes (assuming they agree) is bounded by $\tilde{O}(2^{-s}) = \tilde{O}(2^{-\sqrt{n}})$.

To complete the proof, we need to bound the probability that the game is won if the above-described POVM returns outcome 0. In fact, we can show something stronger: In this case the probability that Alice and Bob agree is negligible (this is stronger because $K_A = K_B$ is a necessary but not sufficient condition for winning the game). To see this, let us assume for a moment that Alice and Bob perform measurements in a basis θ^* sampled uniformly at random and independently from p . In this case, the probability that Alice and Bob agree is given by

$$\text{Tr} \left(\mathbb{E}_{\theta^* \in \{0,1\}^n} \left(\sum_{x \in \{0,1\}^n} \theta^* |xx\rangle\langle xx|_{\theta^*} \right) (I - (|\text{EPR}\rangle\langle\text{EPR}|)^{\otimes s})^{\otimes n/s} \rho_{AB}^{(p)} \right),$$

where $|x\rangle_{\theta}$ denotes the basis states in the θ -basis. A direct calculation shows that this probability can be bounded by $2^{-n/s} = 2^{-\sqrt{n}}$, independently of the quantum state. In the actual experiment Alice and Bob measure according to θ , which is correlated with p . However, the probability of agreement cannot differ from the case treated above, as otherwise we could efficiently distinguish (p, θ) from (p, θ^*) , in contradiction to [Eq. \(1\)](#). This is the point where we finally appeal to the computational indistinguishability of the two distributions. Crucially, this reduction only uses the efficiently prepared state of Alice and Bob, while Charlie's later unbounded computation does not enter the picture.

This concludes the analysis of the monogamy-of-entanglement game ([Theorem 1](#)). It is not hard to obtain from this desired security of the non-interactive QKD protocol ([Theorem 2](#)).

Achieving Everlasting Security in Two Rounds. In order to obtain a QKD protocol with the standard notion of everlasting security (indistinguishability also

in case of disagreement), we propose adding another round of simultaneous messages, where Alice and Bob test the equality of their key. To achieve this without leaking too much information we consider a standard technique: instead of sending K_A and K_B in the plain, Alice and Bob send and compare hashes of their respective keys. With overwhelming probability, this test fails if $K_A \neq K_B$. Finally, to turn search security (the key is hard to guess) to indistinguishability from random we take a quantum-proof randomness extractor, seeded by the XOR of two seeds sampled independently by Alice and Bob.

Entanglement is Necessary. We prove our impossibility result ([Theorem 3](#)) by showing that if there is no entanglement, the key shared by Alice and Bob in an honest run of the protocol is a function of the classical randomness held by Alice and Bob. In particular, this implies that the honest measurements of the protocol are non-destructive: they do not collapse the quantum messages! An attack can then proceed as follows. Eve intercepts the message by Alice, simulates polynomially many possible runs of Bob, and computes simulated key for each run. Similarly, Eve intercepts the message by Bob, simulates polynomially many possible runs of Alice, and computes the simulated key that would be output in each run. After collecting this data, Eve forwards Alice's message to Bob and vice-versa, who continue the protocol. Because the measurements are non-destructive, from the perspective of Alice and Bob they are in an honest run of the protocol. On the other hand, the data collected by Eve allows her to later guess classical randomness such that the resulting key matches the key of Alice and Bob with constant probability.

1.3 Open Problems

As already mentioned above, the question of a non-interactive QKD satisfying the standard definition of everlasting security remains open from *any* computational assumption. We suspect that new ideas are needed to construct such a protocol (or to rule out its existence). Another interesting open problem is to exhibit two-round protocols with a positive key rate. At a more fundamental level, a fascinating direction is to strengthen our computational monogamy of entanglement result: It is conceivable that a bound can be proven even without restricting Bob to measure its state in the θ -basis, instead allowing him to apply an arbitrary POVM. Both the setting of a polynomial-time POVM and the setting of a computationally unbounded one are open, although we expect the latter to be difficult to prove given known techniques, since a polynomial-time reduction would not even be able to run Bob's algorithm.

2 Preliminaries

Throughout this work, we denote the security parameter by λ . We denote by 1^λ the all-ones string of length λ . We say that a function f is negligible in the

security parameter λ if $f(\lambda) = \lambda^{-\omega(1)}$ or, equivalently, $f(\lambda) = 2^{-\omega(\log \lambda)}$; often such a function is simply denoted negl .

For a finite set S , we write $x \leftarrow S$ to denote that x is sampled uniformly at random from S , and for a probability distribution $\mathbb{P}$, we write $x \leftarrow \mathbb{P}$ to denote that x is sampled according to $\mathbb{P}$. Unless stated otherwise, all random variables and probability distributions are finitely supported, that is, take values in finite sets. We denote by $[n]$ the set $\{1, \dots, n\}$. We write I for identity matrices or operators, and Tr for the trace of a matrix or operator. A unitary operator U is one that satisfies $UU^\dagger = U^\dagger U = I$, and a Hermitian operator H is one such that $H^\dagger = H$.

2.1 Quantum Information

In this section, we provide a brief overview of quantum information. For a more detailed introduction, see [22, 26]. A (*quantum*) *register* A consisting of n qubits is associated with the Hilbert space $\mathcal{H}_A = (\mathbb{C}^2)^{\otimes n}$. Given two registers A and B , we denote the composite register by AB . The corresponding Hilbert space is given by the tensor product $\mathcal{H}_{AB} = \mathcal{H}_A \otimes \mathcal{H}_B$.

Quantum States. The (*quantum*) *state* of a register A is described by a density operator ρ_A on $\mathcal{H}_A$, which is a positive semi-definite Hermitian operator with trace equal to one. A state is called *pure* if it has rank one. Thus, pure quantum states can be represented by unit vectors $|\psi\rangle_A \in \mathcal{H}_A$, with $\rho_A = |\psi\rangle\langle\psi|_A$. For a quantum state ρ_{AB} on $\mathcal{H}_{AB}$, we denote $\rho_A = \text{Tr}_B(\rho_{AB}) \in \mathcal{H}_A$ the reduced state of ρ_{AB} on A .

The quantum formalism allows treating classical and quantum information on the same footing. For example, if X is a random variable with outcomes in some set $\mathcal{X}$, its probability distribution can be described by the *classical* quantum state $\rho_X = \sum_{x \in \mathcal{X}} p_x |x\rangle\langle x|$, where $p_x = \Pr(X = x)$. For the uniform distribution, this called the *maximally mixed state* $\tau_X = \frac{1}{|\mathcal{X}|} \sum_{x \in \mathcal{X}} |x\rangle\langle x|$. More generally, if we have a random variable X and a quantum register E such that E is in state $\rho_E^{(x)}$ conditional on $X = x$, this can be described by a *classical-quantum (cq) state* $\rho_{XE} = \sum_x p_x |x\rangle\langle x| \otimes \rho_E^{(x)}$. In the above, subscripts indicate the registers (we only omit them when the context is clear).

For a quantum state ρ_{AB} on two registers A and B , we often denote by $\rho_A = \text{tr}_B[\rho_{AB}]$ for the reduced state of register A . Dually, if M_A is an operator (typically a unitary, a projection, or a POVM element, see below) on register A , we extend it implicitly by the identity to an operator $M_A \otimes I_B$. These notations are compatible: we have $\text{tr}[M_A \rho_{AB}] = \text{tr}[M_A \text{tr}_B[\rho_{AB}]] = \text{tr}[M_A \rho_A]$.

Quantum Channels and Measurements. A (*quantum*) *channel* $\mathcal{F}$ is a completely positive trace-preserving (CPTP) map from a register A to a register B . In other words, given any density matrix ρ_A , the channel $\mathcal{F}$ produces $\mathcal{F}(\rho_A) = \sigma_B$, which is another state on register B , and the same applies when $\mathcal{F}$ is applied to the A -register of a quantum state ρ_{AC} , resulting in the quantum state $\sigma_{BC} =$

$(\mathcal{F} \otimes \mathcal{I})(\rho_{AC})$, where $\mathcal{I}$ denotes the identity channel. For any unitary operator U , there is a quantum channel $\mathcal{U}$ that maps any input state ρ to the output state $\mathcal{U}(\rho) := U\rho U^\dagger$.

A *projective measurement* is defined by a set of projectors $\{\Pi_j\}_j$ such that $\sum_j \Pi_j = I$. A projector Π is a Hermitian operator such that $\Pi^2 = \Pi$, that is, an orthogonal projection. Given a state ρ , the measurement yields outcome j with probability $p_j = \text{Tr}(\Pi_j \rho)$, upon which the state changes to $\Pi_j \rho \Pi_j / p_j$. A basis measurement is one where $\Pi_j = |e_j\rangle\langle e_j|$ and the $\{|e_j\rangle\}$ (necessarily) form an orthonormal basis.

A *positive operator-valued measure (POVM)* is a generalization of a projective measurement. A POVM is defined by a set of positive semi-definite operators $\{E_j\}_j$ such that $\sum_j E_j = I$ (that is, the E_j no longer need to be projections). As before, given a quantum state ρ , the probability of obtaining outcome j when performing the measurement is given by $p(j) = \text{Tr}(E_j \rho)$, but the state after the measurement is no longer uniquely specified. Indeed, while any POVM measurement can be realized by a projective measurement on a larger Hilbert space (by Naimark's dilation theorem), different realizations can lead to different post-measurement states. A *binary POVM* is one that has two outcomes 0 and 1. Binary POVMs, are in one-to-one correspondence with quantum channels that output a single bit (i.e., the output state is a mixture of $|0\rangle\langle 0|$ and $|1\rangle\langle 1|$ for any input state).

Lemma 4 (Operator Union Bound). *Let $P_1, \dots, P_t$ be PSD operators such that $I - P_i$ is also PSD for all $i \in [t]$. Then:*

$$I - \bigotimes_{i=1}^t P_i \leq \sum_{i=1}^t \left(I^{\otimes(i-1)} \otimes (I - P_i) \otimes I^{\otimes(t-i)} \right)$$

Proof. For $t = 1$, the statement is trivially true. We now prove this by induction on k , so let us assume that the statement is true for some value k . We will prove it also holds for $k + 1$:

$$\begin{aligned} I - \bigotimes_{i=1}^{k+1} P_i &= I - \left(\bigotimes_{i=1}^k P_i \right) \otimes P_{k+1} \\ &= \left(I - \bigotimes_{i=1}^k P_i \right) \otimes I + \left(\bigotimes_{i=1}^k P_i \right) \otimes (I - P_{k+1}) \\ &\leq \left(I - \bigotimes_{i=1}^k P_i \right) \otimes I + I^{\otimes k} \otimes (I - P_{k+1}) \\ &\leq \sum_{i=1}^k \left(I^{\otimes(i-1)} \otimes (I - P_i) \otimes I^{\otimes(k-i)} \right) \otimes I + I^{\otimes k} \otimes (I - P_{k+1}) \\ &= \sum_{i=1}^k \left(I^{\otimes(i-1)} \otimes (I - P_i) \otimes I^{\otimes(k+1-i)} \right). \end{aligned}$$

The last inequality is by the induction hypothesis. $\square$

Computational Basis, Hadamard Basis, and Bell Basis. For a single qubit, the *computational basis* is denoted by $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, while the *Hadamard basis* is given by $|+\rangle = H|0\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}$ and $|-\rangle = H|1\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}$. Here, $H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ is the Hadamard unitary. Note that $|0\rangle, |1\rangle$ is an eigenbasis of the Pauli Z -operator, while $|+\rangle, |-\rangle$ is an eigenbasis of the Pauli X -operator. These operators are the unitaries defined by $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, and they are also Hermitian, so that $X^2 = Z^2 = I$.

For more than one qubit, we can choose either basis for each qubit:

Definition 5 (θ -Basis States). We denote, for $x, \theta \in \{0, 1\}^n$,

$$|x\rangle_\theta = H^\theta |x\rangle, \quad \text{where} \quad |x\rangle = |x_1\rangle \otimes \cdots \otimes |x_n\rangle \quad \text{and} \quad H^\theta = H^{\theta_1} \otimes \cdots \otimes H^{\theta_n},$$

where we use the notation $H^1 = H$ and $H^0 = I$, with I the identity matrix. The basis $\{|x\rangle_\theta\}_{x \in \{0,1\}^n}$ is called the θ -basis.

Thus θ labels the basis choice and x the state with respect to the chosen basis. For example, $|01\rangle_{10} = H|0\rangle \otimes |1\rangle = |+\rangle \otimes |1\rangle$.

For two qubits, we not only have the product bases discussed earlier but also an important basis known as the *Bell basis*. It consists of the four maximally entangled *Bell states*:

$$\begin{aligned} |\phi^+\rangle &= |\text{EPR}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), & |\psi^+\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle), \\ |\phi^-\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle), & |\psi^-\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle). \end{aligned}$$

The Bell states form a joint eigenbasis of the two-qubit Pauli operators $X \otimes X$ and $Z \otimes Z$, and they are uniquely characterized by the corresponding eigenvalues. In particular, $(X \otimes X)|\phi^+\rangle = (Z \otimes Z)|\phi^+\rangle = |\text{EPR}\rangle$. It follows that if one measures both qubits of an EPR pair in the standard basis, or both in the Hadamard basis, then the outcomes always coincide. Furthermore:

Lemma 6 (Support of EPR Pairs). Let $\theta \in \{0, 1\}$ and $P_\theta = \sum_{x=0}^1 \theta |xx\rangle\langle xx|_\theta$, with $|xx\rangle_\theta := |x\rangle_\theta |x\rangle_\theta$. Then,

$$P_\theta |\phi^+\rangle = |\phi^+\rangle.$$

Proof. Because the EPR pair is invariant under Hadamard gates on both qubits, $(H \otimes H)|\phi^+\rangle = |\phi^+\rangle$, we have that $|\phi^+\rangle = \frac{1}{\sqrt{2}} \sum_{x=0}^1 |xx\rangle_\theta$ for any $\theta \in \{0, 1\}$. $\square$

Statistical and Computational Distinguishability. The *trace distance* between two states ρ and σ is defined as:

$$\text{Td}(\rho, \sigma) = \frac{1}{2} \|\rho - \sigma\|_1 = \frac{1}{2} \text{Tr} \left(\sqrt{(\rho - \sigma)^\dagger (\rho - \sigma)} \right).$$

The operational meaning of the trace distance is that $\frac{1}{2}(1 + \text{Td}(\rho, \sigma))$ is the maximal probability that two states ρ and σ can be distinguished by any (not necessarily efficient) quantum channel or POVM. That is,

$$\text{Td}(\rho, \sigma) = \max_{\mathcal{A}} |\Pr(\mathcal{A}(\rho) = 1) - \Pr(\mathcal{A}(\sigma) = 1)|,$$

where the maximum is over arbitrary quantum channels $\mathcal{A}$ that output a single bit. Thus, the trace distance generalizes the statistical (total variation) distance from probability theory. We will also use the trace distance for *subnormalized states*, that is, positive semi-definite operators with trace at most one (these generalize sub-probability distributions in probability theory).

We will also consider computational indistinguishability. To this end, recall that a *nonuniform QPT algorithm* $\mathcal{A} = \{\mathcal{A}_\lambda\}$ consists of a family of quantum channels that can be implemented by polynomial-size quantum circuits that get quantum states of a polynomial number of qubits as advice. We call $\mathcal{A}$ a *nonuniform QPT distinguisher* if the channels output a single bit.

Definition 7 (Computational Indistinguishability). *We say that two families of states $\{\rho_\lambda\}, \{\sigma_\lambda\}$ are computationally indistinguishable, denoted $\{\rho_\lambda\} \approx_c \{\sigma_\lambda\}$, if for every nonuniform QPT distinguisher $\mathcal{A} = \{\mathcal{A}_\lambda\}$ there exists a negligible function negl such that the following holds for all λ :*

$$|\Pr(\mathcal{A}_\lambda(\rho_\lambda) = 1) - \Pr(\mathcal{A}_\lambda(\sigma_\lambda) = 1)| \leq \text{negl}(\lambda). \quad (2)$$

The two families are called strongly computationally indistinguishable, denoted $\{\rho_\lambda\} \approx_{sc} \{\sigma_\lambda\}$, if there exists a single negligible function negl such that for every nonuniform QPT distinguisher $\mathcal{A} = \{\mathcal{A}_\lambda\}$ there exists λ_0 such that Eq. (2) holds for all $\lambda \geq \lambda_0$.

The latter, stronger notion is also a natural one [10]. It applies, e.g., when more concrete bounds on the advantage of adversaries are considered. See also the discussion below Definition 15.

Finally, we note that a (*uniform*) *QPT algorithm* is defined as above but the quantum circuit family is uniformly generated and there is no advice. There are also interactive definitions of both uniform and nonuniform QPT algorithms.

Min-Entropy and Quantum-Proof Extractors. The conditional min-entropy of quantum states is defined as follows [15].

Definition 8 (Conditional Min-Entropy). *Let ρ_{AB} be a quantum state. The min-entropy of A conditioned on B is defined by*

$$H_{\min}(A|B)_\rho := -\inf_{\sigma_B} D_\infty(\rho_{AB} \parallel I_A \otimes \sigma_B),$$

where the infimum is taken over all density operators σ_B on subsystem B , and where

$$D_\infty(\alpha \parallel \beta) := \inf\{\lambda \in \mathbb{R} : \alpha \leq 2^\lambda \beta\}.$$

In the case that the first system is classical, the following theorem states that the conditional min-entropy can be interpreted as a guessing probability [15].

Theorem 9 (Min-Entropy of classical-quantum states). *Consider a classical-quantum state $\rho_{XB} = \sum_x p_x |x\rangle\langle x| \otimes \rho_B^{(x)}$. Then,*

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

where

$$p_{\text{guess}}(X|B)_\rho := \max_{\{E_B^{(x)}\}} \sum_x p_x \text{Tr}\left(E_B^{(x)} \rho_B^{(x)}\right) = \max_{\{E_B^{(x)}\}} \text{Tr}\left(\rho_{XB} \sum_x |x\rangle\langle x|_X \otimes E_B^{(x)}\right).$$

is the maximal probability of obtaining X using an arbitrary POVM $\{E_B^{(x)}\}_x$ on B .

The conditional min-entropy satisfies the following chain rule [27, Lemma 11]:

Theorem 10 (Chain Rule). *Let ρ_{ABZ} be a tripartite state that is classical on Z . Then,*

$$H_{\min}(A|BZ)_\rho \geq H_{\min}(A|B)_\rho - \log |Z|,$$

where $|Z|$ is the dimension of system Z (that is, the size of the underlying classical alphabet).

Next, we recall the following definition of (quantum-proof) randomness extractor.

Definition 11 (Extractor). *A PPT algorithm $\text{Ext}: \mathcal{S} \times \mathcal{X} \rightarrow \{0, 1\}^\ell$ is called a seeded strong average-case (k, ε) -extractor if the following holds: for any cq-state $\rho_{XB} = \sum_x p_x |x\rangle\langle x| \otimes \rho_B^{(x)}$ such that $H_{\min}(X|B) \geq k$, we have*

$$\text{Td}(\rho_{YSB}, \tau_Y \otimes \rho_{SB}) \leq \varepsilon,$$

where

$$\rho_{YSB} = \frac{1}{|S|} \sum_{s \in \mathcal{S}} \sum_{x \in \mathcal{X}} p_x |\text{Ext}(s, x)\rangle\langle \text{Ext}(s, x)| \otimes |s\rangle\langle s| \otimes \rho_B^{(x)}$$

describes the joint state of the result of the extraction (Y), the seed (S), and the quantum side information (B), and where we recall that τ_Y denotes the maximally mixed state on Y .

We recall the definition of universal hash functions.

Definition 12 (Universal Hash Family). *A family $\mathbb{H} = \{h: [N] \rightarrow [M]\}$ of functions is a universal hash if for every $x, y \in [N]$ such that $x \neq y$, it holds that*

$$\Pr_{h \leftarrow \mathbb{H}}(h(x) = h(y)) = \frac{1}{M}.$$

It is well-known that *efficient* constructions of universal hash families exist [3]. Moreover, randomness extractors can be constructed from universal hash families [7,23,14].

Lemma 13 (Generalized Leftover Hash Lemma). *Let $\mathbb{H} = \{h: [N] \rightarrow \{0,1\}^\ell\}$ be a universal hash family. Then, $\text{Hash}: \mathbb{H} \times [N] \rightarrow \{0,1\}^\ell$ defined by $\text{Hash}(h, x) = h(x)$ is a seeded strong average-case (k, ε) -extractor for any $k \geq \ell + 2 \log(1/\varepsilon)$.*

We also rely on the computational notion of a collision-resistant hash function, which we define next. As in the definition of strong computational indistinguishability (Definition 7) we assume that there exists a single negligible function that applies to all QPT adversaries.

Definition 14 (Collision-Resistant Hash Function). *A family $\{\mathbb{H}_\lambda\}$ of function families is called a collision-resistant hash function if there exists a negligible function negl such that the following holds: for every QPT adversary $\mathcal{A}$ there exists λ_0 such that, for all $\lambda \geq \lambda_0$, we have*

$$\Pr_{h \leftarrow \mathbb{H}_\lambda, (x,y) \leftarrow \mathcal{A}(h)} (x \neq y \text{ and } h(x) = h(y)) \leq \text{negl}(\lambda).$$

2.2 Post-Quantum Non-Interactive Key Exchange

Following [4,5,8,9], we formally define a post-quantum non-interactive key exchange protocol (that is, one that is computationally secure against quantum adversaries).

Definition 15 (Post-Quantum Non-Interactive Key Exchange). *A post-quantum non-interactive key exchange (NIKE) protocol is defined as a tuple $\text{NIKE} = (\text{Stp}, \text{Gen}, \text{SdK})$ of the following algorithms, with an identity space $\text{IDS} \subseteq \{0,1\}^{n(\lambda)}$ and a shared key space $\text{SKS} \subseteq \{0,1\}^{n(\lambda)}$ for a polynomially bounded $n(\lambda)$:*

- $\text{pp} \leftarrow \text{Stp}(1^\lambda)$: Given the security parameter encoded in unary, 1^λ , the PPT algorithm Stp returns public system parameters pp .
- $(\text{sk}_A, \text{pk}_A) \leftarrow \text{Gen}(\text{pp}, A)$: Given the public parameters pp and an identity $A \in \text{IDS}$, the PPT algorithm Gen returns a secret-public key pair $(\text{sk}_A, \text{pk}_A)$.
- $K \leftarrow \text{SdK}(A, \text{pk}_A, B, \text{sk}_B)$: Given an identity $A \in \text{IDS}$ and a corresponding public key pk_A , along with another identity $B \in \text{IDS}$ and corresponding secret key sk_B , SdK should be a deterministic PPT algorithm that returns a shared key $K \in \text{SKS}$, or an abort symbol $\perp$. If $A = B$ then SdK always returns $\perp$.

We always assume the following two properties:

- **Correctness:** There exists a negligible function negl such that for all $A, B \in \text{IDS}$, it holds that

$$\Pr(\text{SdK}(A, \text{pk}_A, B, \text{sk}_B) \neq \text{SdK}(B, \text{pk}_B, A, \text{sk}_A)) = \text{negl}(\lambda),$$

where $\text{pp} \leftarrow \text{Stp}(1^\lambda)$, $(\text{sk}_A, \text{pk}_A) \leftarrow \text{Gen}(\text{pp}, A)$, and $(\text{sk}_B, \text{pk}_B) \leftarrow \text{Gen}(\text{pp}, B)$.

– Post-Quantum Security: *For all $A, B \in \text{IDS}$, we have*

$$(\text{pp}, \text{pk}_A, \text{pk}_B, \text{SdK}(A, \text{pk}_A, B, \text{sk}_B)) \approx_{sc} (\text{pp}, \text{pk}_A, \text{pk}_B, K^*) \quad (3)$$

where $\text{pp} \leftarrow \text{Stp}(1^\lambda)$, $(\text{sk}_A, \text{pk}_A) \leftarrow \text{Gen}(\text{pp}, A)$, $(\text{sk}_B, \text{pk}_B) \leftarrow \text{Gen}(\text{pp}, B)$, and $K^* \leftarrow \text{SKS}$.

Post-quantum NIKE protocols can be constructed assuming the hardness of the standard learning with errors problem [9] or from computational problems in isogenies over elliptic curves [5]. The stronger definition of computational indistinguishability used in Eq. (3) (see Definition 7 for the precise definition of $\approx_{sc}$) requires making concrete assumptions on the runtime of the best attacker against the underlying hard problem. This is not unique to our settings and it is in fact required by essentially any application that considers concrete security estimates for the NIKE. We refer the reader to [9,17] for concrete bounds on lattice-based NIKE and to [2] for isogeny-based schemes.

We remark that one can also consider a stronger definition of security [4], where the adversary is given access to a key derivation oracle, for both honestly generated keys. Since the above weaker definitions will suffice for us, we refrain from defining the stronger variant.

3 Computational Monogamy of Entanglement

In this section we propose and analyze a computational variant of the monogamy of entanglement game of [25].

3.1 Definition of Computational Monogamy-of-Entanglement Game

We assume the existence of a distribution $\mathcal{Z}$ on $\{0, 1\}^{q(\lambda)} \times \{0, 1\}^{n(\lambda)}$, parameterized by a security parameter λ , where $q(\lambda)$ and $n(\lambda)$ are polynomially bounded, and $n(\lambda) = \omega(\log^2 \lambda)$. The distribution should be samplable by a QPT algorithm, which we denote by $(p, \theta) \leftarrow \mathcal{Z}(1^\lambda)$ and we require one of the following computational indistinguishability assumptions (Definition 7):

$$((p, \theta) : (p, \theta) \leftarrow \mathcal{Z}(1^\lambda)) \approx_{sc} ((p, \theta^*) : (p, \cdot) \leftarrow \mathcal{Z}(1^\lambda); \theta^* \leftarrow \{0, 1\}^n) \quad (4)$$

or

$$((p, \theta) : (p, \theta) \leftarrow \mathcal{Z}(1^\lambda)) \approx_c ((p, \theta^*) : (p, \cdot) \leftarrow \mathcal{Z}(1^\lambda); \theta^* \leftarrow \{0, 1\}^n). \quad (5)$$

In the game that we are about to define, p models public parameters revealed to the players before they have to agree on a joint quantum state, while the value θ is only revealed afterwards.

Definition 16 (Computational Monogamy-of-Entanglement Game).

Given a distribution $\mathcal{Z}$ as above, we define the following computational monogamy-of-entanglement game between Alice and a pair of “adversaries” Bob and Charlie. It is parametrized by a security parameter λ and consists of four phases:

1. Sampling Phase: Alice samples $(p, \theta) \leftarrow \mathcal{Z}(1^\lambda)$ and reveals p to Bob and Charlie.
2. Efficient Preparation Phase: Alice, Bob, and Charlie jointly apply a QPT algorithm (which may depend p but not on θ) to create a shared quantum state between their registers A, B, C . Registers A and B should consist of $n(\lambda)$ qubits, while C can be arbitrary.
3. Question Phase: Alice measures register A in the θ -basis to obtain an outcome K_A . She then reveals θ to Bob and Charlie.
4. Semi-Honest Answer Phase: Bob measures register B in the θ -basis to obtain an outcome K_B , while Charlie can apply an arbitrary (possibly inefficient) measurement of register C to obtain an outcome K_C .

The players win the game if $K_A = K_B = K_C$.

Thus a *strategy* for the above game consists of a QPT algorithm that on input p outputs a state $\rho_{ABC}^{(p)}$ (the result of the preparation phase), along with a family of (possibly inefficient) POVMs $\{Q_C^{(k_E|p, \theta)}\}_{k_E}$ that correspond to Charlie's measurement for a given value of p and θ . Without loss of generality we may assume that this POVM does not explicitly depend on p , i.e., $Q_C^{(k_E|p, \theta)} = Q_C^{(k_E|\theta)}$ (indeed, p can always be stored in C during the preparation phase). Then the winning probability of the game is given by

$$p_{\text{win}} = \Pr(K_A = K_B = K_C) = \mathbb{E}_{(p, \theta) \leftarrow \mathcal{Z}(1^\lambda)} \sum_k \text{Tr} \left((\theta |kk\rangle\langle kk|_\theta \otimes Q_C^{(k|\theta)}) \rho_{ABC}^{(p)} \right). \quad (6)$$

3.2 Bound on the Min-Entropy and the Winning Probability

We now analyze the winning probability of the above game. We first prove a slightly stronger statement – an explicit bound on the min-entropy of $K_A = K_B$ if the two keys agree (which is a necessary condition in order to win the game) given Charlie's quantum system – and then deduce a bound on the winning probability as a corollary.

Theorem 17. *Let $\mathcal{Z}$ be any distribution satisfying Eq. (4) with a negligible function $\eta(\lambda)$. For any QPT algorithm modeling the preparation phase, let us run the computational monogamy-of-entanglement game until right before Charlie's measurement. If $K_A \neq K_B$, sample $K \leftarrow \{0, 1\}^{n(\lambda)}$ independently and uniformly at random, else set $K := K_A = K_B$. Let $\rho_{KC\Theta}$ denote the resulting cq-state describing the random variables K and θ and Charlie's register C . Then, there exists λ_0 such that, for all $\lambda \geq \lambda_0$,*

$$H_{\min}(K|C)_\rho \geq H_{\min}(K|C\Theta)_\rho \geq t(\lambda) := -\log \left(\tilde{O} \left(2^{-\frac{1}{2}} \sqrt{n(\lambda)} \right) + \eta(\lambda) \right).$$

In particular, $H_{\min}(K|C)_\rho = \omega(\log \lambda)$.

Proof. For notational simplicity we assume that $n(\lambda)$ is a square. The first inequality is known as the data-processing inequality for the min-entropy and is

easy to see in the cq case. Thus we need only to prove the second inequality. In view of [Theorem 9](#), this means that we wish to prove that there exists λ_0 such that, for all $\lambda \geq \lambda_0$ and for every POVM $\{E_{C\Theta}^{(k)}\}$, we have

$$\text{Tr} \left(\rho_{KC\Theta} \sum_k |k\rangle\langle k|_K \otimes E_{C\Theta}^{(k)} \right) \leq \frac{1}{2^{t(\lambda)}}. \quad (7)$$

Because the state ρ is classical on register Θ , we may assume that $E_{C\Theta}^{(k)} = \sum_\theta E_C^{(k|\theta)} \otimes |\theta\rangle\langle\theta|_\Theta$, where $\{E_C^{(k|\theta)}\}_k$ is a POVM for every fixed value of θ .

Let $\rho_{ABC}^{(p)}$ denote the joint quantum state of Alice, Bob, and Charlie right before the question phase of the game, for a fixed value of p , and let $\rho_{KC}^{(p,\theta)}$ denote the cq-state defined as in the statement of the theorem, but for fixed values of p and θ . Then, $\rho_{KC\Theta} = \mathbb{E}_{(p,\theta) \leftarrow \mathcal{Z}(1^\lambda)} (\rho_{KC}^{(p,\theta)} \otimes |\theta\rangle\langle\theta|_\Theta)$, so that

$$\text{Tr} \left(\rho_{KC\Theta} \sum_k |k\rangle\langle k|_K \otimes E_{C\Theta}^{(k)} \right) = \mathbb{E}_{(p,\theta) \leftarrow \mathcal{Z}(1^\lambda)} \text{Tr} \left(\rho_{KC}^{(p,\theta)} \sum_k |k\rangle\langle k|_K \otimes E_C^{(k|\theta)} \right) \quad (8)$$

Moreover, we have

$$\begin{aligned} \rho_{KC}^{(p,\theta)} &= \sum_k |k\rangle\langle k|_K \otimes \text{Tr}_{AB} \left((\theta|kk\rangle\langle kk|_\theta \otimes I_C) \rho_{ABC}^{(p)} \right) \\ &\quad + \tau_K \otimes \text{Tr}_{AB} \left(\left(\sum_{k_A \neq k_B} \theta |k_A k_B\rangle\langle k_A k_B|_\theta \otimes I_C \right) \rho_{ABC}^{(p)} \right), \end{aligned} \quad (9)$$

where τ_K denotes the maximally mixed state on K and $|k_A k_B\rangle_\theta := |k_A\rangle_\theta |k_B\rangle_\theta$. Choose any function $s(\lambda)$ such that $s(\lambda) = \omega(\log \lambda)$ and $n(\lambda)/s(\lambda) = \omega(\log \lambda)$, with both $s(\lambda)$ and $n(\lambda)/s(\lambda)$ integers. Then we can define the projections

$$M_{AB}^{(1)} = \left(I - |\phi^+\rangle\langle\phi^+|^{\otimes s(\lambda)} \right)^{\otimes \frac{n(\lambda)}{s(\lambda)}} \quad \text{and} \quad M_{AB}^{(0)} = I - M_{AB}^{(1)} \quad (10)$$

(where $|\phi^+\rangle$ is a single EPR pair shared between Alice and Bob), using which we further decompose the right-hand side of [Eq. \(9\)](#) into three terms:

$$\begin{aligned} \rho_{KC}^{(p,\theta)} &= \sum_k |k\rangle\langle k|_K \otimes \text{Tr}_{AB} \left((\theta|kk\rangle\langle kk|_\theta M_{AB}^{(0)} \otimes I_C) \rho_{ABC}^{(p)} \right) \\ &\quad + \sum_k |k\rangle\langle k|_K \otimes \text{Tr}_{AB} \left((\theta|kk\rangle\langle kk|_\theta M_{AB}^{(1)} \otimes I_C) \rho_{ABC}^{(p)} \right) \\ &\quad + \tau_K \otimes \text{Tr}_{AB} \left(\left(\sum_{k_A \neq k_B} \theta |k_A k_B\rangle\langle k_A k_B|_\theta \otimes I_C \right) \rho_{ABC}^{(p)} \right), \end{aligned} \quad (11)$$

Thus,

$$\text{Tr} \left(\rho_{KC}^{(p,\theta)} \sum_k |k\rangle\langle k|_K \otimes E_C^{(k|\theta)} \right) = \sum_k \text{Tr} \left((\theta|kk\rangle\langle kk|_\theta M_{AB}^{(0)} \otimes E_C^{(k|\theta)}) \rho_{ABC}^{(p)} \right)$$

$$\begin{aligned}
& + \sum_k \text{Tr} \left((\theta |kk\rangle\langle kk|_\theta M_{AB}^{(1)} \otimes E_C^{(k|\theta)}) \rho_{ABC}^{(p)} \right) \\
& + \frac{1}{2^{n(\lambda)}} \text{Tr} \left(\left(\sum_{k_A \neq k_B} \theta |k_A k_B\rangle\langle k_A k_B|_\theta \otimes I_C \right) \rho_{ABC}^{(p)} \right) \\
& \leq \sqrt{\frac{n(\lambda)/s(\lambda)}{2^{s(\lambda)}}} + \sum_k \text{Tr} \left(\theta |kk\rangle\langle kk|_\theta M_{AB}^{(1)} \rho_{AB}^{(p)} \right) + \frac{1}{2^{n(\lambda)}},
\end{aligned}$$

where we bound the first term using [Lemma 21](#) below, for the middle term we use $E_C^{(k|\theta)} \leq I_C$, and for the last term $\sum_{k_A \neq k_B} \theta |k_A k_B\rangle\langle k_A k_B|_\theta \leq I_{AB}$. Taking the expectation as in [Eq. \(8\)](#), we find that

$$\begin{aligned}
\text{Tr} \left(\rho_{K C \Theta} \sum_k |k\rangle\langle k|_K \otimes E_{C\Theta}^{(k)} \right) &= \mathbb{E}_{(p,\theta) \leftarrow \mathcal{Z}(1^\lambda)} \left(\sum_k \text{Tr} \left(\theta |kk\rangle\langle kk|_\theta M_{AB}^{(1)} \rho_{AB}^{(p)} \right) \right) \\
&+ \sqrt{\frac{n(\lambda)/s(\lambda)}{2^{s(\lambda)}}} + \frac{1}{2^{n(\lambda)}}, \tag{12}
\end{aligned}$$

In [Lemma 23](#) below we show that

$$\mathbb{E}_{(p,\cdot) \leftarrow \mathcal{Z}(1^\lambda); \theta^* \leftarrow \{0,1\}^{n(\lambda)}} \left(\sum_k \text{Tr} \left(\theta^* |kk\rangle\langle kk|_{\theta^*} M_{AB}^{(1)} \rho_{AB}^{(p)} \right) \right) \leq \frac{1}{2^{n(\lambda)/s(\lambda)}}. \tag{13}$$

We claim that the computational indistinguishability in [Eq. \(4\)](#) implies that there exists λ_0 , depending only on the QPT algorithm modeling the preparation phase, such that, for all $\lambda \geq \lambda_0$,

$$\left| \mathbb{E}_{(p,\theta) \leftarrow \mathcal{Z}(1^\lambda)} \left(\sum_k \text{Tr} \left(\theta |kk\rangle\langle kk|_\theta M_{AB}^{(1)} \rho_{AB}^{(p)} \right) \right) - \mathbb{E}_{(p,\cdot) \leftarrow \mathcal{Z}(1^\lambda); \theta^* \leftarrow \{0,1\}^{n(\lambda)}} \left(\sum_k \text{Tr} \left(\theta^* |kk\rangle\langle kk|_{\theta^*} M_{AB}^{(1)} \rho_{AB}^{(p)} \right) \right) \right| \leq \eta(\lambda). \tag{14}$$

Indeed we can define a reduction as follows: On input (p, θ) , simulate the efficient preparation phase (phase 2) to obtain the state $\rho_{AB}^{(p)}$ of Alice and Bob's qubits. Next, apply the efficient projective measurement $\{M_{AB,0}, M_{AB,1}\}$ defined in [Eq. \(10\)](#). If the outcome is "0", output an arbitrary. If the outcome is "1", measure Alice and Bob's qubits in the θ -basis and return "1" if and only if the measurement outcomes agree. Note that the reduction so defined is efficient (the possibly inefficient POVM is not used in the reduction). Moreover, the bias of this reduction is precisely the left-hand side of [Eq. \(14\)](#).⁹ Thus, [Eq. \(14\)](#) must hold, for otherwise we would obtain a contradiction to the computational indistinguishability assumption in [Eq. \(4\)](#), and λ_0 only depends on the preparation

⁹ Note that, for every fixed θ , the projections $\sum_k \theta |kk\rangle\langle kk|_\theta$ and $M_{AB}^{(1)}$ commute. This follows from [Lemma 6](#).

phase. Combining Eqs. (12) to (14), and choosing $s(\lambda) = \sqrt{n(\lambda)}$, we obtain the upper bound (7): we have, for all $\lambda \geq \lambda_0$,

$$\text{Tr} \left(\rho_{KC\Theta} \sum_k |k\rangle\langle k|_K \otimes E_{C\Theta}^{(k)} \right) \leq \frac{1}{2^{n(\lambda)/s(\lambda)}} + \eta(\lambda) + \sqrt{\frac{n(\lambda)/s(\lambda)}{2^{s(\lambda)}}} + \frac{1}{2^{n(\lambda)}} \leq 2^{-t(\lambda)}.$$

Because λ_0 does not depend on the choice of POVM $\{E_{C\Theta}^{(k)}\}$, it follows that $p_{\text{guess}}(K|C\Theta)_\rho \leq 2^{-t(\lambda)}$. Using Theorem 9, we conclude that

$$H_{\min}(K|C\Theta)_\rho = -\log p_{\text{guess}}(K|C\Theta)_\rho \geq t(\lambda). \quad \square$$

Corollary 18. *Let $\mathcal{Z}$ be any distribution satisfying Eq. (4) with a negligible function $\eta(\lambda)$. Then, for any strategy for the computational monogamy-of-entanglement game, there is λ_0 such that, for all $\lambda \geq \lambda_0$, the winning probability is bounded by $\tilde{O}(2^{-\frac{1}{2}\sqrt{n(\lambda)}}) + \eta(\lambda)$. In particular, the winning probability is negligible.*

Proof. Let $\rho_{ABC}^{(p)}$ denote the joint quantum state of Alice, Bob, and Charlie right before the question phase of the game, for a fixed value of p . For a fixed value of p and θ , the joint state of the random variables K_A, K_B and Charlie's register C right before Charlie's measurement is given by

$$\rho_{K_A K_B C}^{(p, \theta)} = \sum_{k_A, k_B} |k_A k_B\rangle\langle k_A k_B|_{K_A K_B} \otimes \sigma_C^{(p, \theta, k_A k_B)},$$

where

$$\sigma_C^{(p, \theta, k_A k_B)} = \text{Tr}_{AB} \left((\theta |k_A k_B\rangle\langle k_A k_B|_\theta \otimes I_C) \rho_{ABC}^{(p)} \right),$$

with $|k_A k_B\rangle_\theta := |k_A\rangle_\theta |k_B\rangle_\theta$. Let $\{Q_C^{(k_E|\theta)}\}_{k_E}$ denote the POVM applied by Charlie in the answer phase for a given value of θ (as discussed below Definition 16 we may assume without loss of generality that this POVM does not depend explicitly on p). Then the winning probability is given by Eq. (6):

$$\begin{aligned} p_{\text{win}} &= \mathbb{E}_{(p, \theta) \leftarrow \mathcal{Z}(1^\lambda)} \sum_k \text{Tr} \left((\theta |kk\rangle\langle kk|_\theta \otimes E_C^{(k|\theta)}) \rho_{ABC}^{(p)} \right) \\ &= \mathbb{E}_{(p, \theta) \leftarrow \mathcal{Z}(1^\lambda)} \sum_k \text{Tr} \left(\sigma_C^{(p, \theta, kk)} E_C^{(k|\theta)} \right). \end{aligned}$$

On the other hand, the state $\rho_{KC\Theta}$ in the statement of Theorem 17 is given by

$$\rho_{KC\Theta} = \mathbb{E}_{(p, \theta) \leftarrow \mathcal{Z}(1^\lambda)} \left(\sum_k |k\rangle\langle k|_K \otimes \sigma_C^{(p, \theta, kk)} \otimes |\theta\rangle\langle\theta|_\Theta + \tau_K \otimes \sum_{k_A \neq k_B} \sigma_C^{(p, \theta, k_A k_B)} \otimes |\theta\rangle\langle\theta|_\Theta \right),$$

where τ_K is the maximally mixed state. Defining the POVM $E_{C\Theta}^{(k)} := \sum_\theta E_C^{(k|\theta)} \otimes |\theta\rangle\langle\theta|_\Theta$, we see that

$$p_{\text{win}} \leq \text{tr} \left(\rho_{KC\Theta} \left(\sum_k |k\rangle\langle k|_K \otimes E_{C\Theta}^{(k)} \right) \right) \leq p_{\text{guess}}(K|C\Theta)_\rho = 2^{-H_{\min}(K|C\Theta)_\rho},$$

where the last step is due to Theorem 9. Thus Theorem 17 implies the claim. $\square$

For the standard notion of computational indistinguishability, an easy adaption of these proofs yield the following variants of [Theorem 17](#) and [Corollary 18](#).

Theorem 19. *Let $\mathcal{Z}$ be any parameterized distribution satisfying [Eq. \(5\)](#). For any QPT algorithm modeling the preparation phase, let us run the computational monogamy-of-entanglement game until right before Charlie's measurement. If $K_A \neq K_B$, sample $K \leftarrow \{0, 1\}^{n(\lambda)}$ independently and uniformly at random, else set $K := K_A = K_B$. Let $\rho_{KC\Theta}$ denote the resulting cq-state describing the random variables K and θ and Charlie's register C . Then there exists a function $t(\lambda) = \omega(\log \lambda)$ such that the following holds for all λ :*

$$H_{\min}(K|C)_\rho \geq H_{\min}(K|C\Theta)_\rho \geq t(\lambda).$$

The proof proceeds as the one of [Theorem 17](#) – the only difference is that the negligible function $\eta(\lambda)$ in [Eq. \(14\)](#) may now depend on the preparation phase, rather than just on the computational indistinguishability assumption.

Corollary 20. *Let $\mathcal{Z}$ be any parameterized distribution satisfying [Eq. \(5\)](#). Then, for any strategy for the computational monogamy-of-entanglement game, the winning probability is a negligible function of λ .*

3.3 Technical Lemmas

We now state and prove the technical lemmas used in the proof of [Theorems 17](#) and [19](#).

Lemma 21. *Let ρ_{ABE} be a quantum state, where A and B are n -qubit registers, let $\{Q_E^{(x)}\}_{x \in \{0,1\}^n}$ be a POVM, and let s be a divisor of n . Then the following holds for any fixed $\theta \in \{0, 1\}^n$:*

$$\text{Tr} \left(\left(\sum_{x \in \{0,1\}^n} \theta |xx\rangle\langle xx|_\theta \otimes Q_E^{(x)} \right) \left(I - \left(I - |\phi^+\rangle\langle\phi^+|^{\otimes s} \right)_{AB}^{\otimes(n/s)} \right) \rho_{ABE} \right) \leq \sqrt{\frac{n/s}{2^s}},$$

where $|xx\rangle_\theta := |x\rangle_\theta |x\rangle_\theta$.

Proof. By Naimark's theorem, any POVM $\{Q_E^{(x)}\}$ can be implemented by an isometry $V_{E \rightarrow E'F}$, where E' is an n -qubit system and F another quantum system, followed by a measurement of E' in the standard basis. Thus we may assume without loss of generality that E is an n -qubit register and $Q_E^{(x)} = |x\rangle\langle x|_E$. To prove the claim, it suffices to bound the operator norm of

$$\sum_{x \in \{0,1\}^n} \theta |xx\rangle\langle xx|_\theta \left(I - \left(I - |\phi^+\rangle\langle\phi^+|^{\otimes s} \right)_{AB}^{\otimes(n/s)} \right) \otimes |x\rangle\langle x|_E$$

Because this is an operator controlled on E , this norm is the maximum operator norm of

$$M_x := \theta |xx\rangle\langle xx|_\theta \left(I - \left(I - |\phi^+\rangle\langle\phi^+|^{\otimes s} \right)_{AB}^{\otimes(n/s)} \right)$$

for $x \in \{0, 1\}^n$. By Lemma 4, we have

$$\begin{aligned} P &:= \left(I - \left(I - |\phi^+\rangle\langle\phi^+|^{\otimes s} \right)_{AB}^{\otimes(n/s)} \right) \\ &\leq |\phi^+\rangle\langle\phi^+|^{\otimes s} \otimes I \otimes \cdots \otimes I + \cdots + I \otimes \cdots \otimes I \otimes |\phi^+\rangle\langle\phi^+|^{\otimes s}. \end{aligned}$$

Using that P is a projection, we have

$$\|M_x\|^2 = \|M_x M_x^\dagger\| = \theta \langle xx | P | xx \rangle_\theta \leq \sum_{j=1}^{n/s} \theta_j \langle x_j x_j | |\phi^+\rangle\langle\phi^+|^{\otimes s} | x_j x_j \rangle_{\theta_j} = \frac{n/s}{2^s},$$

where $x_j, \theta_j \in \{0, 1\}^s$ denotes the j -th substring of x and θ , respectively, of length s . $\square$

Lemma 22. *We have:*

$$\begin{aligned} \mathbb{E}_{\theta \leftarrow \{0,1\}^n} \sum_{x \in \{0,1\}^n} \theta |xx\rangle\langle xx|_\theta &\equiv \left(\mathbb{E}_{\theta \leftarrow \{0,1\}} \sum_{x \in \{0,1\}} \theta |xx\rangle\langle xx|_\theta \right)^{\otimes n} \\ &= \left(|\phi^+\rangle\langle\phi^+| + \frac{1}{2} |\phi^-\rangle\langle\phi^-| + \frac{1}{2} |\psi^+\rangle\langle\psi^+| \right)^{\otimes n}, \end{aligned} \quad (15)$$

where $|xx\rangle_\theta := |x\rangle_\theta |x\rangle_\theta$ and we use $\equiv$ to indicate that the equality holds up to the natural reordering of the systems.

Proof. We prove the lemma for $n = 1$, and the general result follows since both the left-hand side and the right-hand side of Eq. (15) are the n -th tensor power of it. To this end we use:

$$|0\rangle\langle 0| = \frac{I + Z}{2}, \quad |1\rangle\langle 1| = \frac{I - Z}{2}, \quad |+\rangle\langle +| = \frac{I + X}{2}, \quad |-\rangle\langle -| = \frac{I - X}{2}.$$

Thus:

$$\begin{aligned} \mathbb{E}_{\theta \leftarrow \{0,1\}} \sum_{x \in \{0,1\}} \theta |xx\rangle\langle xx|_\theta &= \frac{1}{2} (|00\rangle\langle 00| + |11\rangle\langle 11| + |++\rangle\langle ++| + |--\rangle\langle --|) \\ &= \frac{1}{8} ((I + Z)^{\otimes 2} + (I - Z)^{\otimes 2} + (I + X)^{\otimes 2} + (I - X)^{\otimes 2}) \\ &= \frac{1}{4} (I \otimes I + Z \otimes Z + I \otimes I + X \otimes X) \\ &= |\phi^+\rangle\langle\phi^+| + \frac{1}{2} |\phi^-\rangle\langle\phi^-| + \frac{1}{2} |\psi^+\rangle\langle\psi^+|, \end{aligned}$$

In the last step we used that

$$\begin{aligned} \frac{1}{2} (I \otimes I + Z \otimes Z) &= |\phi^+\rangle\langle\phi^+| + |\phi^-\rangle\langle\phi^-|, \\ \frac{1}{2} (I \otimes I + X \otimes X) &= |\phi^+\rangle\langle\phi^+| + |\psi^+\rangle\langle\psi^+|, \end{aligned}$$

which holds because $Z \otimes Z$ acts by $+1$ on the Bell states $|\phi^\pm\rangle$ and by -1 on the Bell states $|\psi^\pm\rangle$, and similarly for $X \otimes X$. This concludes the proof. $\square$

Lemma 23. *Let ρ_{AB} be a quantum state on n -qubit registers A and B , and let s be a divisor of n . Then:*

$$\mathbb{E}_{\theta \leftarrow \{0,1\}^n} \text{Tr} \left(\sum_{x \in \{0,1\}^n} \theta |xx\rangle\langle xx|_{\theta} \left(I - |\phi^+\rangle\langle\phi^+|^{\otimes s} \right)^{\otimes (n/s)} \rho_{AB} \right) \leq \frac{1}{2^{n/s}},$$

where $|xx\rangle_{\theta} := |x\rangle_{\theta} |x\rangle_{\theta}$.

Proof. By Lemma 22, we can rewrite

$$\mathbb{E}_{\theta \in \{0,1\}^n} \sum_{x \in \{0,1\}^n} \theta |xx\rangle\langle xx|_{\theta} = \left(|\phi^+\rangle\langle\phi^+| + \frac{1}{2} |\phi^-\rangle\langle\phi^-| + \frac{1}{2} |\psi^+\rangle\langle\psi^+| \right)^{\otimes n},$$

and therefore

$$\begin{aligned} \mathbb{E}_{\theta \leftarrow \{0,1\}^n} \sum_{x \in \{0,1\}^n} \theta |xx\rangle\langle xx|_{\theta} \left(I - |\phi^+\rangle\langle\phi^+|^{\otimes s} \right)^{\otimes (n/s)} \\ = \left(|\phi^+\rangle\langle\phi^+| + \frac{1}{2} |\phi^-\rangle\langle\phi^-| + \frac{1}{2} |\psi^+\rangle\langle\psi^+| \right)^{\otimes n} \left(I - |\phi^+\rangle\langle\phi^+|^{\otimes s} \right)^{\otimes (n/s)} \\ = \left(\left(|\phi^+\rangle\langle\phi^+| + \frac{1}{2} |\phi^-\rangle\langle\phi^-| + \frac{1}{2} |\psi^+\rangle\langle\psi^+| \right)^{\otimes s} - |\phi^+\rangle\langle\phi^+|^{\otimes s} \right)^{\otimes (n/s)} \\ \leq \frac{1}{2^{n/s}} I. \end{aligned}$$

To see the latter inequality, note that $P_0 := |\phi^+\rangle\langle\phi^+|$ and $P_1 = |\phi^-\rangle\langle\phi^-| + |\psi^+\rangle\langle\psi^+|$ are projectors with orthogonal range, and hence

$$(P_0 + \frac{1}{2}P_1)^{\otimes s} - P_0^{\otimes s} = \sum_{0 \neq x \in \{0,1\}^s} \frac{1}{2^{|x|}} P_{x_1} \otimes \cdots \otimes P_{x_s} \leq \frac{1}{2} \sum_{0 \neq x \in \{0,1\}^s} P_{x_1} \otimes \cdots \otimes P_{x_s} \leq \frac{1}{2} I.$$

Therefore,

$$\text{Tr} \left(\mathbb{E}_{\theta \leftarrow \{0,1\}^n} \sum_{x \in \{0,1\}^n} \theta |xx\rangle\langle xx|_{\theta} \left(I - |\phi^+\rangle\langle\phi^+|^{\otimes s} \right)^{\otimes (n/s)} \rho_{AB} \right) \leq \frac{1}{2^{n/s}} \text{Tr}(\rho_{AB}) = \frac{1}{2^{n/s}},$$

concluding our proof. $\square$

4 Quantum Key Distribution Protocols

We first construct our non-interactive QKD protocol and establish a weak form of everlasting security (Section 4.1). We then show how to convert this protocol into a two-round protocol to achieve the standard definition of everlasting security (Section 4.2).

4.1 Non-Interactive Protocol with Weak Everlasting Security

We now present a quantum key distribution protocol that is *non-interactive*, i.e., it consists of a single round of simultaneous messages between Alice and Bob. Our construction assumes the existence of a post-quantum non-interactive key exchange (NIKE) protocol and upgrades it to a non-interactive quantum key distribution protocol that satisfies a weak version of everlasting security, which we will define below.

Definition 24 (Non-Interactive QKD Protocol). *Let $\text{NIKE} = (\text{Stp}, \text{Gen}, \text{SdK})$ be a post-quantum secure NIKE protocol (Definition 15), with key space $\{0, 1\}^{n(\lambda)}$, where $n(\lambda)$ grows polynomially in the security parameter λ . We define the following non-interactive QKD protocol with the same key space $\text{SKS} = \{0, 1\}^{n(\lambda)}$:*

1. Setup: Run $\text{pp} \leftarrow \text{Stp}(1^\lambda)$. We assume that pp are given as input to all parties.
2. Alice: Run $(\text{sk}_A, \text{pk}_A) \leftarrow \text{Gen}(\text{pp}, A)$ and prepare $n(\lambda)$ EPR pairs. Send the classical bitstring pk_A to Bob, along with one qubit of each EPR pair.
Bob: Sample $(\text{sk}_B, \text{pk}_B) \leftarrow \text{Gen}(\text{pp}, B)$ and send the classical bitstring pk_B to Alice.
3. Output: Alice computes $\theta_A \leftarrow \text{SdK}(B, \text{pk}_B, A, \text{sk}_A)$ and measures her remaining $n(\lambda)$ qubits in the θ_A -basis to obtain $K_A \in \{0, 1\}^{n(\lambda)}$. Similarly, Bob computes $\theta_B \leftarrow \text{SdK}(A, \text{pk}_A, B, \text{sk}_B)$ and measures his $n(\lambda)$ qubits in the θ_B -basis to obtain $K_B \in \{0, 1\}^{n(\lambda)}$.

This defines a QKD protocol that is non-interactive: There is a single round of communication, consisting of one message from Alice to Bob and one from Bob to Alice, with the two messages not depending on each other. Moreover, the correctness of protocol is immediate: by the correctness of the NIKE protocol, it holds that $\text{SdK}(B, \text{pk}_B, A, \text{sk}_A) = \text{SdK}(A, \text{pk}_A, B, \text{sk}_B)$ with overwhelming probability – and in this case, Alice and Bob measure their EPR pairs in the same basis ($\theta_A = \theta_B$), hence they obtain the same outcome $K_A = K_B$.

However, it is easy to see that the protocol does *not* satisfy the standard notion of everlasting security. Indeed, the QPT adversary can keep the $n(\lambda)$ qubits that Alice sends to Bob and instead output one qubit each of $n(\lambda)$ fresh EPR pairs, and also store the public keys pk_A, pk_B . Since the post-quantum NIKE is only computationally secure, this information suffices to (inefficiently) learn $\theta_A = \theta_B$. Then K_A can be obtained by suitable basis measurements on the qubits that were sent by Alice and kept by the adversary, and K_B can be obtained on the remaining qubits kept by the adversary. Interestingly, for this attack it holds that $K_A = K_B$ only with negligible probability (since K_A and K_B are now independent and uniformly random). This is no accident. Indeed we will now show that the protocol still satisfies a form of everlasting security provided $K_A = K_B$. We now give a formal definition tailored to the protocol defined in Definition 24:

Definition 25 (Weak Everlasting Security). *Consider the following experiment involving Alice, Bob, and an adversary described by a non-uniform QPT algorithm:*

- I. We run step 1 of [Definition 24](#) and also give $\mathbf{pp}$ as an input to the adversary.
- II. We run step 2 of [Definition 24](#), but instead of delivering the two messages, we first send them to the adversary, who returns a register B (and keeps an internal register E). Modify Alice's message to consist of the quantum register B , along with the original classical bitstring, and deliver it to Bob. Deliver Bob's message unchanged as it only consists of a classical bitstring.
- III. We proceed by running step 3 of [Definition 24](#). Let K_A, K_B denote Alice's and Bob's output, respectively. If $K_A \neq K_B$, we set K to be a uniformly random bitstring in $\{0, 1\}^{n(\lambda)}$. Otherwise, we set $K := K_A = K_B$. Let ρ_{KE} be the classical-quantum joint state of K and the adversary's internal register E .

We say that the protocol satisfies weak everlasting security if there exists a function $t(\lambda) = \omega(\log(\lambda))$ such that following holds: for every QPT adversary, there exists λ_0 such that, for all $\lambda \geq \lambda_0$,

$$H_{\min}(K|E)_\rho \geq t(\lambda). \quad (16)$$

Using our computational monogamy of entanglement result, we now show that the QKD protocol indeed satisfies this weaker notion of everlasting security.

Theorem 26. *The non-interactive QKD protocol ([Definition 24](#)) is correct and satisfies weak everlasting security ([Definition 25](#)).*

Proof. We already established correctness in the discussion above, so it remains to prove security. We can write the cq-state in [Definition 25](#) as $\rho_{KE} = \mathbb{E}_{\theta_A, \theta_B} \rho_{KE}^{(\theta_A, \theta_B)}$, where $\rho_{KE}^{(\theta_A, \theta_B)}$ is the cq-state conditioned on fixed values of θ_A and θ_B and the average is over the marginal distribution of (θ_A, θ_B) . To establish the bound on the min-entropy, we wish to compare ρ_{KE} to the cq-state arising in the computational monogamy-of-entanglement theorem ([Theorem 17](#)). Let $\mathcal{Z}(1^\lambda)$ denote the joint distribution of (p, θ_A) sampled by the following efficient algorithm:

1. Sample $\mathbf{pp} \leftarrow \text{Setup}(1^\lambda)$, $(\text{sk}_A, \text{pk}_A) \leftarrow \text{Gen}(\mathbf{pp}, A)$, and $(\text{sk}_B, \text{pk}_B) \leftarrow \text{Gen}(\mathbf{pp}, B)$.
2. Output $p := (\mathbf{pp}, \text{pk}_A, \text{pk}_B)$ and $\theta_A := \text{SdK}(B, \text{pk}_B, A, \text{sk}_A)$.

The post-quantum security of the NIKE in [Eq. \(3\)](#) implies the computational indistinguishability for the computational monogamy-of-entanglement game in [Eq. \(4\)](#). Now suppose that Eve plays the role of Charlie ($C = E$) and let $\rho_{ABC}^{(p)}$ denote the state of Alice, Bob, and Charlie after steps I and II of [Definition 25](#) (which are efficient). This constitutes an efficient preparation phase for the computational monogamy-of-entanglement game. Because in the game both Alice and Bob use the same measurement basis θ_A , the cq-state described in [Theorem 17](#) is given by $\tilde{\rho}_{KE} := \mathbb{E}_{\theta_A} \rho_{KE}^{(\theta_A, \theta_A)}$. Thus [Theorem 17](#) implies that there exists λ_0 such that, for all $\lambda \geq \lambda_0$, we have

$$H_{\min}(K|E)_{\tilde{\rho}} \geq t(\lambda)$$

or, equivalently,

$$p_{\text{guess}}(K|E)_{\tilde{\rho}} \leq 2^{-t(\lambda)},$$

where $t(\lambda) = \omega(\log \lambda)$ is a function that is independent of the adversary. Note that $2^{-t(\lambda)}$ is negligible. By the correctness of the NIKE protocol, $\text{Td}(\rho_{KE}, \tilde{\rho}_{KE}) \leq \text{P}(\theta_A \neq \theta_B)$ is also a negligible function independent of the adversary. Hence the above also holds for ρ , concluding the proof. $\square$

One can obtain an explicit min-entropy bound in Eq. (16) by using the formula in Theorem 17 along with a bound on the correctness of the post-quantum secure NIKE used in the construction. E.g., if the security of the post-quantum NIKE holds with a negligible function $2^{-\Omega(\sqrt{n}(\lambda))}$ and correctness holds with a failure probability of $2^{-\Omega(\sqrt{n}(\lambda))}$, then we have $H_{\min}(K|E) = \Omega(\sqrt{n}(\lambda))$.

We remark that if in the post-quantum security of the NIKE (Eq. (3) in Definition 15) we replace the strong computational indistinguishability $\approx_{sc}$ by $\approx_c$ (Definition 7), then weak everlasting security still holds with the right-hand side of Eq. (16) given by a function $t = \omega(\log \lambda)$ that can now depend on the adversary. This is still a meaningful notion of security. However, we need the stronger notion to construct the two-round protocol that we describe next.

4.2 Two-Round Protocol with Everlasting Security

We now describe a two-round simultaneous-message protocol to achieve the standard definition of everlasting security. This protocol builds on the one-round protocol constructed in Section 4.1 which satisfies weak everlasting security. We use a collision-resistant hash function to verify that $K_A = K_B$ in the second round of communication, and a seeded randomness extractor for privacy amplification.

Definition 27 (Two-Round QKD Protocol). *Let NIQKD be the non-interactive QKD protocol of Definition 24, with key space $\{0, 1\}^{n(\lambda)}$ and min-entropy bound (16) given by $t(\lambda) = \omega(\log \lambda)$. Let $m(\lambda) := \Theta(t(\lambda))$, and choose a collision-resistant hash function $\mathbb{H}_\lambda = \{h : [2^{n(\lambda)}] \rightarrow [2^{m(\lambda)}]\}$ (Definition 14), as well as a seeded strong average-case $(\Theta(m(\lambda)), 2^{-\Theta(m(\lambda))})$ -extractor $\text{Ext} : \mathcal{S}_\lambda \times \{0, 1\}^{n(\lambda)} \rightarrow \{0, 1\}^{m(\lambda)}$ (Definition 11). We first define a two-round sub-protocol:*

1. Setup and Round 1: Alice and Bob run NIQKD to obtain $K_A, K_B \in \{0, 1\}^{n(\lambda)}$.
2. Round 2: Alice samples $\text{seed}_A \leftarrow \mathcal{S}_\lambda$, $h_A \leftarrow \mathbb{H}_\lambda$ and sends $(\text{seed}_A, h_A, h_A(K_A))$ to Bob. Bob samples $h_B \leftarrow \mathbb{H}_\lambda$ and sends $(h_B, h_B(K_B))$ to Alice.
3. Output: Alice returns K_A if $h_B(K_A) = h_B(K_B)$, and otherwise $\perp$. Bob returns K_B if $h_A(K_A) = h_A(K_B)$, and otherwise $\perp$.

We now present our two-round QKD protocol with key space $\text{SKS} = \{0, 1\}^{m(\lambda)}$.¹⁰

- Parallel Sub-Protocol Runs: Alice and Bob run two parallel (independent) instances of the above sub-protocol, once as above and once the roles of the two parties swapped. Denote by (K_A^0, K_A^1) the outputs of Alice and by (K_B^0, K_B^1) the outputs of Bob for the two sub-protocol runs. Moreover, denote by seed_A and seed_B the seeds sampled in the two sub-protocol runs.

¹⁰ This protocol applies the extractor to a concatenation of the two ‘subkeys’ in a fixed order. To obtain a fully symmetrical protocol, Alice and Bob can in the first round sample and exchange random bits $b_A, b_B \leftarrow \{0, 1\}$, and in the second round use $b = b_A \oplus b_B$ to decide whether to apply the extractor to $K^0 \| K^1$ or $K^1 \| K^0$, respectively.

- Output: If $K_A^0 \neq \perp$ and $K_A^1 \neq \perp$, Alice outputs

$$K_A^* = \text{Ext}(\text{seed}_A \oplus \text{seed}_B, K_A^0 \| K_A^1),$$

and otherwise $\perp$. Likewise, if $K_B^0 \neq \perp$ and $K_B^1 \neq \perp$, Bob outputs

$$K_B^* = \text{Ext}(\text{seed}_A \oplus \text{seed}_B, K_B^0 \| K_B^1),$$

and otherwise $\perp$.

We consider the following properties:

- *Correctness*: There exists a negligible function negl such that

$$\Pr(K_A^* = K_B^* \neq \perp) \geq 1 - \text{negl}(\lambda).$$

- *Everlasting Security*: Consider the following experiment involving Alice, Bob, and an adversary described by a non-uniform interactive QPT machine:

- I. We run the QPT setup algorithm with input 1^λ to obtain public parameters pp , which are given as input to Alice, Bob, and the adversary.
- II. We then run the interactive protocol but with the following modification: Recall that each message consists of a classical bitstring and a quantum register. Instead of directly delivering the messages, the adversary can intercept them and return modified quantum registers.¹¹ The messages are then delivered with those quantum registers and the original classical bitstrings, which are always left unchanged.

- III. Let K_A^* denote Alice's output, let K_B^* denote Bob's output, and let E denote the internal register of the adversary at the end of the protocol.

We say that the protocol satisfies *everlasting security* if there exists a negligible function negl such that the following holds: for any QPT adversary in the above experiment, there exists λ_0 such that, for all $\lambda \geq \lambda_0$, if we sample $U \leftarrow \{0, 1\}^{m(\lambda)}$ independently and uniformly and put

$$U_A = \begin{cases} \perp & \text{if } K_A^* = \perp \\ U & \text{otherwise} \end{cases} \quad \text{and} \quad U_B = \begin{cases} \perp & \text{if } K_B^* = \perp \\ U & \text{otherwise} \end{cases},$$

then

$$\text{Td}(\rho_{EK_A^*}, \rho_{EU_A}) \leq \text{negl}(\lambda) \quad \text{and} \quad \text{Td}(\rho_{EK_B^*}, \rho_{EU_B}) \leq \text{negl}(\lambda),$$

where $\rho_{EK_A^* K_B^* U_A U_B}$ denotes the classical-quantum state describing the adversary's internal register and the random variables K_A^*, K_B^*, U_A, U_B .

- *Verifiability*: There exists a negligible function negl such that the following holds: for any QPT adversary in the above experiment, there exists λ_0 such that, for all $\lambda \geq \lambda_0$,

$$\Pr(K_A^* \neq K_B^*) \leq \text{negl}(\lambda).$$

¹¹ The adversary is allowed to intercept multiple message at the same time, even across different rounds of the protocol, and also only return a subset of the quantum registers at a time, as long as compatible with the causal order of the protocol.

Note that the classical messages sent by the parties are honestly delivered in the experiment underlying the security definition. This models the presence of (public) authenticated classical channels, which is a necessary assumption for security of key exchange protocols. We refer to [19] for a discussion on this aspect and for other considerations on the above definition.

The correctness of our two-round protocol follows immediately from the correctness of the non-interactive protocol. Next we consider verifiability. Clearly, if $K_A^0 = K_B^0$ and $K_A^1 = K_B^1$, then $K_A^* = K_B^*$. Now suppose that $K_A^0 \neq K_B^0$. Then we must have $h_A^0(K_A^0) = h_A^0(K_B^0)$ or $h_B^0(K_A^0) = h_B^0(K_B^0)$, or both. But this can only happen with negligible probability, for otherwise we would obtain a contradiction to the collision-resistance of the hash function (since the protocol runs in QPT and the keys are sampled honestly). The case that $K_A^1 \neq K_B^1$ works identically. We conclude that $K_A^* = K_B^*$ with overwhelming probability.

We now sketch our argument for everlasting security. Without loss of generality it suffices to consider an attack of the following form. First, the attacker intercepts the simultaneous first-round messages sent by Alice and Bob, and outputs a quantum register that, along with the classical part of Alice's original message, gets delivered to Bob.¹² Next, the attacker receives Bob's second-round message (which is classical) and outputs a quantum register that, along with the classical part of Bob's first-round message, gets delivered to Alice. The attacker records all remaining messages, which are classical and get delivered honestly.

We henceforth concentrate on the first subprotocol and we consider the second subprotocol as part of the adversary, which is possible because the two subprotocols are independent. Then the weak everlasting security of our NI-QKD protocol (Theorem 26) shows that $H_{\min}(K^0|E^0) \geq t(\lambda)$, where K^0 is defined as in the definition of weak everlasting security (in terms of K_A^0 and K_B^0), and E^0 denotes the internal state of the adversary after the first interception. The subsequent message from Bob ($h_B^0, h_B^0(K_B^0)$) contains information about K_B^0 , but using the chain rule for the min-entropy and the structure of the protocol, it follows that $H_{\min}(K^0|E) \geq \Omega(t(\lambda))$, where $E = (E_0, h_B^0, h_B^0(K_B^0))$. Crucially, Alice's seed, seed_A , is chosen independently from K_B^0 (and K_A^0). Thus, if $K_A^0 = K_B^0$, so $K_A^0 = K^0$, the randomness extractor guarantees that K_A^*E and $U_A E$ are negligibly close in trace distance. On the other hand, if $K_A^0 \neq K_B^0$ then $K_A^* = \perp$ with overwhelming probability by the same argument used to prove verifiability, and hence the same holds. Combining these two cases concludes the proof.

5 Entanglement is Necessary for NI-QKD

In this section we prove that any non-interactive QKD protocol where Alice and Bob derive their shared key only from classical randomness cannot be everlastingly secure (Theorem 29). This is in particular the case when the quantum messages sent by Alice and Bob are unentangled with the respective sender's

¹² The case where a message first gets delivered to Alice can be analyzed in exactly the same fashion, thanks to the symmetry of our protocol.

quantum memories. In other words, our result implies that entanglement is required for non-interactive quantum key distribution, and at least one of Alice or Bob must have a quantum memory (Corollary 31). In contrast, multi-round QKD can achieve everlasting security (even unconditional security) by sending unentangled systems from Alice to Bob.

Throughout this section we consider a non-interactive QKD protocol with key space $\text{SKS} = \{0, 1\}^{m(\lambda)}$ that has the following form:

1. Alice efficiently samples (R_A, S_A, ρ_{AM_A}) , where R_A and S_A are $\text{poly}(\lambda)$ -length bitstrings and ρ_{AM_A} is a $\text{poly}(\lambda)$ -qubit state. Bob efficiently samples $(R_B, S_B, \sigma_{BM_B})$, where R_B and S_B are $\text{poly}(\lambda)$ -length bitstrings and σ_{BM_B} is a $\text{poly}(\lambda)$ -qubit state.
2. Alice sends the bitstring S_A and the quantum system M_A to Bob. Simultaneously, Bob sends the bitstring S_B and the quantum system M_B to Alice.
3. Finally, Alice applies an efficient measurement (depending on R_A, S_A, S_B) to quantum systems AM_B to obtain the key $K_A \in \{0, 1\}^{m(\lambda)} \cup \{\perp\}$. Likewise, Bob applies an efficient measurement (depending on R_B, S_A, S_B) to BM_A to obtain $K_B \in \{0, 1\}^{m(\lambda)} \cup \{\perp\}$.

For simplicity we further assume that the protocol is *perfectly correct*. That is, we assume that in the absence of an adversary, $K_A = K_B \neq \perp$ with certainty.

Definition 28 (NI-QKD with classically-derived keys). *We say that a NI-QKD protocol of the form above has classically-derived keys if there is a function f such that $K_A = K_B = f(R_A, R_B, S_A, S_B)$.*

In other words, while quantum information can be used in the protocol, the agreed-upon secret key is a function of the classical randomness sampled by Alice and Bob only (rather than of any quantum randomness produced during the protocol execution). We emphasize that the function f need not be efficient nor does it have to be known to Alice or Bob – it merely needs to exist.

Theorem 29. *No perfectly correct NI-QKD protocol with classically-derived keys can be everlastingly secure. In fact, for any such protocol there exists an attack with an efficient online phase that uses only nondestructive quantum measurements (hence Alice and Bob still output $K_A = K_B \neq \perp$ with certainty) and an unbounded offline phase that outputs $K_A = K_B$ with constant probability.*

Proof. Without loss of generality, we may assume both R_A and R_B consist of the same number $r(\lambda) = \text{poly}(\lambda)$ of bits. We may furthermore assume that R_A includes S_A and R_B includes S_B . Then the function f in Definition 28 will only depend on R_A and R_B , i.e. $K_A = K_B = f(R_A, R_B)$, and the (without loss of generality projective) efficient measurements applied by Alice and Bob to obtain their keys only depend on their local randomness and the classical message sent by the other party. We denote Alice's projective measurements by $\{P_{AM_B}^{(k_A|r_A, s_B)}\}_{k_A \in \{0, 1\}^\lambda \cup \{\perp\}}$ and Bob's projective measurements by $\{Q_{BM_A}^{(k_B|r_B, s_A)}\}_{k_B \in \{0, 1\}^\lambda \cup \{\perp\}}$. Then the condition $K_A = K_B = f(R_A, R_B)$ means

the following: If (R_A, S_A, ρ_{AM_A}) and (R_B, S_B, ρ_{BM_B}) are obtained by Alice and Bob's sampling algorithms, then with probability one we have

$$\text{tr } P_{AM_B}^{(k_A|R_A, S_B)}(\rho_A \otimes \rho_{M_B}) = \delta_{k_A, f(R_A, R_B)}. \quad (17)$$

as well as

$$\text{tr } Q_{BM_A}^{(k_B|R_B, S_A)}(\rho_B \otimes \rho_{M_A}) = \delta_{k_B, f(R_A, R_B)}. \quad (18)$$

In particular, both measurement outcomes are deterministic (conditional on R_A and R_B) and hence these projective measurements do *not* change the measured quantum registers.

With this in mind we consider the following attack:

- In the efficient online phase, Eve intercepts the classical S_A and S_B messages and the M_A and M_B quantum registers sent by Alice and Bob. For $t \in [2r(\lambda)]$:
 - Eve runs Bob's sampling algorithm to obtain $(R_B^{(t)}, \rho_{BM_B}^{(t)})$ and applies Bob's measurement $\{Q_{BM_A}^{(k_B|R_B^{(t)}, S_A)}\}$ on the B register of $\rho^{(t)}$ and the M_A register received from Alice. By Eq. (18), the measurement outcome is $\alpha_t := f(R_A, R_B^{(t)})$, where R_A is the random variable generated by Alice in step 1 of the protocol.
 - Eve runs Alice's sampling algorithm to obtain $(R_A^{(t)}, \rho_{AM_A}^{(t)})$ and applies Alice's measurement $\{P_{AM_B}^{(k_A|R_A^{(t)}, S_B)}\}$ on the A register of $\rho^{(t)}$ and the M_B register received from Bob. By Eq. (17), the measurement outcome is $\beta_t := f(R_A^{(t)}, R_B)$, where R_B is the random variable generated by Bob in step 1 of the protocol.

Finally Eve passes the quantum registers M_A and M_B to Bob and Alice, respectively. The classical messages S_A and S_B are also delivered honestly.

- In the inefficient offline phase, Eve defines sets $\Gamma_A := \{r_A^* : f(r_A^*, R_B^{(t)}) = \alpha_t \forall t \in [2r(\lambda)]\}$ and $\Gamma_B := \{r_B^* : f(R_A^{(t)}, r_B^*) = \beta_t \forall t \in [2r(\lambda)]\}$. First, Eve samples R_A^* from the distribution of R_A *conditional on the event* $R_A \in \Gamma_A$. Then, Eve picks any $R_B^* \in \Gamma_B$, and outputs $f(R_A^*, R_B^*)$.

Note that the quantum registers are passed on unchanged. Therefore, Alice and Bob will still agree on the key $f(R_A, R_B)$ (not equal to $\perp$) with overwhelming probability.

To analyze the attack, we define the sets

$$G_A^{(r_A, \{R_B^{(t)}\})} := \left\{ r_A^* \in \{0, 1\}^{r(\lambda)} \mid f(r_A^*, R_B^{(t)}) = f(r_A, R_B^{(t)}) \forall t \in [2r(\lambda)] \right\},$$

$$H_A^{(r_A)} := \left\{ r_A^* \in \{0, 1\}^{r(\lambda)} \mid \Pr_{R_B}(f(r_A^*, R_B) = f(r_A, R_B)) \leq \frac{2}{3} \right\}.$$

For any $r_A \in \{0, 1\}^{r(\lambda)}$ and any $r_A^* \in H_A^{(r_A)}$, we have that

$$\Pr_{\{R_B^{(t)}\}} \left(r_A^* \in G_A^{(r_A, \{R_B^{(t)}\})} \right) = \Pr_{\{R_B^{(t)}\}} \left(f(r_A^*, R_B^{(t)}) = f(r_A, R_B^{(t)}) \forall t \in [2r(\lambda)] \right)$$

$$= \prod_{t=1}^{2r(\lambda)} \Pr_{\{R_B^{(t)}\}} \left(f(r_A^*, R_B^{(t)}) = f(r_A, R_B^{(t)}) \right) \leq \left(\frac{2}{3} \right)^{2r(\lambda)} = \left(\frac{4}{9} \right)^{r(\lambda)}$$

because the $R_B^{(t)}$ are sampled independently and from the same distribution as R_B . As a consequence, we have for any $r_A \in \{0, 1\}^{r(\lambda)}$, using the union bound,

$$\Pr_{\{R_B^{(t)}\}} \left(G_A^{(r_A, \{R_B^{(t)}\})} \cap H_A^{(r_A)} \neq \emptyset \right) \leq \sum_{r_A^* \in H_A^{(r_A)}} \Pr_{\{R_B^{(t)}\}} \left(r_A^* \in G_A^{(r_A, \{R_B^{(t)}\})} \right) \leq \left(\frac{8}{9} \right)^{r(\lambda)}.$$

As the $R_B^{(t)}$ are sampled independently of R_A , the above bound also holds with R_A in place of r_A . Because $R_A^* \in \Gamma_A = G_A^{(R_A, \{R_B^{(t)}\})}$, we obtain

$$\Pr \left(R_A^* \in H_A^{(R_A)} \right) \leq \Pr_{R_A, \{R_B^{(t)}\}} \left(G_A^{(R_A, \{R_B^{(t)}\})} \cap H_A^{(R_A)} \neq \emptyset \right) \leq \left(\frac{8}{9} \right)^{r(\lambda)}. \quad (19)$$

Similarly, if we define for $r_B \in \{0, 1\}^{r(\lambda)}$ the set

$$H_B^{(r_B)} := \left\{ r_B^* \in \{0, 1\}^{r(\lambda)} \mid \Pr_{R_A} (f(R_A, r_B^*) = f(R_A, r_B)) \leq \frac{2}{3} \right\},$$

we obtain with the same argument that

$$\Pr \left(R_B^* \in H_B^{(R_B)} \right) \leq \left(\frac{8}{9} \right)^{r(\lambda)}. \quad (20)$$

Now, on the one hand side, we have

$$\Pr \left(f(R_A^*, R_B) = f(R_A, R_B) \mid R_A^* \notin H_A^{(R_A)} \right) \geq \frac{2}{3}$$

by definition of the set $H_A^{(R_A)}$ and because R_B is sampled independently from R_A and R_A^* . Together with [Eq. \(19\)](#), we obtain

$$\begin{aligned} \Pr(f(R_A^*, R_B) = f(R_A, R_B)) &\geq \Pr \left(f(R_A^*, R_B) = f(R_A, R_B) \mid R_A^* \notin H_A^{(R_A)} \right) - \Pr \left(R_A^* \in H_A^{(R_A)} \right) \\ &\geq \frac{2}{3} - \left(\frac{8}{9} \right)^{r(\lambda)}. \end{aligned} \quad (21)$$

On the other hand, we have

$$\begin{aligned} &\Pr \left(f(R_A^*, R_B^*) = f(R_A^*, R_B) \mid R_B^* \notin H_B^{(R_B)} \right) \\ &= \Pr \left(f(R_A, R_B^*) = f(R_A, R_B) \mid R_B^* \notin H_B^{(R_B)} \right) \geq \frac{2}{3}, \end{aligned}$$

The first equality holds because R_A^* has the same distribution as R_A ,¹³ and either random variable is independent of R_B and R_B^* . Hence we obtain as above, but using Eq. (20), that

$$\Pr(f(R_A^*, R_B^*) = f(R_A^*, R_B)) \geq \frac{2}{3} - \left(\frac{8}{9}\right)^{r(\lambda)}.$$

Together with Eq. (21), we conclude that

$$\Pr(f(R_A^*, R_B^*) = f(R_A, R_B)) \geq \frac{1}{3} - 2 \left(\frac{8}{9}\right)^{r(\lambda)} = \frac{1}{3} - \text{negl}(\lambda),$$

which establishes the desired lower bound on the success probability of the attack. $\square$

As is clear from the statement of the theorem, Eve's attack also works in the weak everlasting security model (Section 4.1).

Lemma 30. *If a perfectly correct NI-QKD protocol of the form described at the beginning of the section is such that both ρ_{AM_A} and ρ_{BM_B} are unentangled with certainty, then the protocol has classically-derived keys in the sense of Definition 28.*

Proof. We may assume that ρ_{AM_A} and ρ_{BM_B} are pure states, hence $\rho_{AM_A} = \rho_A^{(R_A, S_A)} \otimes \rho_{M_A}^{(R_A, S_A)}$ and likewise $\rho_{BM_B} = \rho_B^{(R_B, S_B)} \otimes \rho_{M_B}^{(R_B, S_B)}$. Thus, $\rho_{AM_A} \otimes \rho_{BM_B}$ is also a product state between registers AM_B and BM_A . Because Alice and Bob's keys are obtained by applying measurements (depending on R_A, R_B, S_A, S_B) on registers AM_B and BM_A , respectively, we see that K_A and K_B are conditionally independent given R_A, R_B, S_A, S_B . On the other hand, we have $K_A = K_B$ by perfect correctness. Thus K_A and K_B must be deterministic and equal to each other given R_A, R_B, S_A, S_B . In other words, there exists a function f such that $K_A = K_B = f(R_A, R_B, S_A, S_B)$. $\square$

Corollary 31. *If a perfectly correct NI-QKD protocol is everlastingly secure, at least one of ρ_{AM_A} and ρ_{BM_B} must be entangled. In particular, Alice or Bob need to have a quantum memory.*

Acknowledgments

GM and MW are supported by the European Union (ERC Starting Grant ObfusQation, 101077455 and SYMOPTIC, 101040907). GM, MW and TZ acknowledge Deutsche Forschungsgemeinschaft (DFG, German Research Foundation) under Germany's Excellence Strategy - EXC 2092 CASA - 390781972. MW is also supported by the German Federal Ministry of Research, Technology and Space (QuSol, 13N17173). ABG is supported by ANR JCJC TCS-NISQ ANR-22-CE47-0004.

¹³ This is an instance of the following fact (with $X = R_A$, $Y = \Gamma_A$, $X^* = R_A^*$): Given two random variables X and Y , sample X^* from the distribution $p(\cdot|Y)$, where $p(x|y) = p(x, y)/p(y)$ denotes the conditional distribution of X given Y . Then X^* has the same distribution as X . Indeed, $\sum_y p(y)p(x|y) = p(x)$.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: Public key distribution and coin tossing. In: Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, Dec. 1984. pp. 175–179 (1984)
2. Campos, F., Chavez-Saab, J., Chi-Domínguez, J.J., Meyer, M., Reijnders, K., Rodríguez-Henríquez, F., Schwabe, P., Wiggers, T.: On the practicality of post-quantum TLS using large-parameter CSIDH. *IACR Cryptol. ePrint Arch.* **2023**, 793 (2023)
3. Carter, J.L., Wegman, M.N.: Universal classes of hash functions. In: Proceedings of the ninth annual ACM Symposium on Theory of Computing. pp. 106–112 (1977)
4. Cash, D., Kiltz, E., Shoup, V.: The twin Diffie–Hellman problem and applications. *Journal of Cryptology* **22**, 470–504 (2009)
5. Castryck, W., Lange, T., Martindale, C., Panny, L., Renes, J.: CSIDH: an efficient post-quantum commutative group action. In: Advances in Cryptology–ASIACRYPT 2018: 24th International Conference on the Theory and Application of Cryptology and Information Security, Brisbane, QLD, Australia, December 2–6, 2018, Proceedings, Part III 24. pp. 395–427. Springer (2018)
6. Diffie, W., Hellman, M.E.: New directions in cryptography. In: Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman, pp. 365–390. ACM (2022)
7. Dodis, Y., Reyzin, L., Smith, A.: Fuzzy extractors: How to generate strong keys from biometrics and other noisy data. In: Advances In Cryptology–EUROCRYPT 2004: International Conference On The Theory And Applications Of Cryptographic Techniques, Interlaken, Switzerland, May 2–6, 2004. Proceedings 23. pp. 523–540. Springer (2004)
8. Freire, E.S., Hofheinz, D., Kiltz, E., Paterson, K.G.: Non-interactive key exchange. In: Public-Key Cryptography–PKC 2013: 16th International Conference on Practice and Theory in Public-Key Cryptography, Nara, Japan, February 26–March 1, 2013. Proceedings 16. pp. 254–271. Springer (2013)
9. Gajland, P., de Kock, B., Quaresma, M., Malavolta, G., Schwabe, P.: SWOOSH: Efficient lattice-based non-interactive key exchange. In: 33rd USENIX Security Symposium (USENIX Security 24). pp. 487–504 (2024)
10. Hastad, J., Impagliazzo, R., Levin, L.A., Luby, M.: A pseudorandom generator from any one-way function. *SIAM Journal on Computing* **28**(4), 1364–1396 (1999)
11. Impagliazzo, R.: A personal view of average-case complexity. In: Proceedings of Structure in Complexity Theory. Tenth Annual IEEE Conference. pp. 134–147. IEEE (1995)
12. Impagliazzo, R., Rudich, S.: Limits on the provable consequences of one-way permutations. In: Proceedings of the twenty-first Annual ACM Symposium on Theory of Computing. pp. 44–61 (1989)
13. Jouguet, P., Kunz-Jacques, S., Leverrier, A., Grangier, P., Diamanti, E.: Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photonics* **7**(5), 378–381 (2013)
14. König, R., Renner, R.: Sampling of min-entropy relative to quantum knowledge. *IEEE Transactions on Information Theory* **57**(7), 4760–4787 (2011)
15. König, R., Renner, R., Schaffner, C.: The operational meaning of min-and max-entropy. *IEEE Transactions on Information Theory* **55**(9), 4337–4347 (2009)
16. Korzh, B., Lim, C.C.W., Houlmann, R., Gisin, N., Li, M.J., Nolan, D., Sanguinetti, B., Thew, R., Zbinden, H.: Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nature Photonics* **9**(3), 163–168 (2015)

17. Langrehr, R.: On the multi-user security of LWE-based NIKE. In: Theory of Cryptography Conference. pp. 33–62. Springer (2023)
18. Lo, H.K., Chau, H.F.: Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283**(5410), 2050–2056 (1999)
19. Malavolta, G., Walter, M.: Robust quantum public-key encryption with applications to quantum key distribution. In: Annual International Cryptology Conference. pp. 126–151. Springer (2024)
20. Mayers, D.: Unconditional security in quantum cryptography. *Journal of the ACM (JACM)* **48**(3), 351–406 (2001)
21. Mayers, D., Yao, A.: Quantum cryptography with imperfect apparatus. In: Proceedings 39th Annual Symposium on Foundations of Computer Science (Cat. No. 98CB36280). pp. 503–509. IEEE (1998)
22. Nielsen, M.A., Chuang, I.L.: *Quantum Computation and Quantum Information*. Cambridge University Press (2016)
23. Renner, R.: Security of quantum key distribution. *International Journal of Quantum Information* **6**(01), 1–127 (2008)
24. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. *Physical Review Letters* **85**(2), 441 (2000)
25. Tomamichel, M., Fehr, S., Kaniewski, J., Wehner, S.: A monogamy-of-entanglement game with applications to device-independent quantum cryptography. *New Journal of Physics* **15**(10), 103002 (2013)
26. Watrous, J.: *The Theory of Quantum Information*. Cambridge University Press (2018)
27. Winkler, S., Tomamichel, M., Hengl, S., Renner, R.: Impossibility of growing quantum bit commitments. *Physical Review Letters* **107**(9), 090502 (2011)
28. Yin, J., Cao, Y., Li, Y.H., Liao, S.K., Zhang, L., Ren, J.G., Cai, W.Q., Liu, W.Y., Li, B., Dai, H., et al.: Satellite-based entanglement distribution over 1200 kilometers. *Science* **356**(6343), 1140–1144 (2017)