Hybrid Quantum Cryptography from Communication Complexity

Francesco Mazzoncini, Balthazar Bauer, Peter Brown, Romain Alléaume

Hybrid Quantum Cryptography from Communication Complexity

Francesco Mazzoncini[1], Balthazar Bauer[2], Peter Brown[1], and Romain Alléaume[1]

[1]Télécom Paris-LTCI, Institut Polytechnique de Paris, 19 Place Marguerite Perey, 91120 Palaiseau, France
[2]LMV, Université de Versailles – Saint-Quentin-en-Yvelines, 55 Avenue de Paris, 78646 Versailles, France

We introduce an explicit construction for a key distribution protocol in the Quantum Computational Timelock (QCT) security model, where one assumes that computationally secure encryption may only be broken after a time much longer than the coherence time of available quantum memories. Taking advantage of the QCT assumptions, we build a key distribution protocol called HM-QCT from the Hidden Matching problem for which there exists an exponential gap in one-way communication complexity between classical and quantum strategies.

We establish that the security of HM-QCT against arbitrary i.i.d. attacks can be reduced to the difficulty of solving the underlying Hidden Matching problem with classical information. Legitimate users, on the other hand, can use quantum communication, which gives them the possibility of sending multiple copies of the same quantum state while retaining an information advantage. This leads to an everlasting secure key distribution scheme over n bosonic modes. Such a level of security is unattainable with purely classical techniques. Remarkably, the scheme remains secure with up to $\mathcal{O}(\frac{\sqrt{n}}{\log(n)})$ input photons for each channel use, extending the functionalities and potentially outperforming QKD rates by several orders of magnitudes.

1 Introduction

1.1 Quantum Cryptography

Quantum cryptography has been largely defined [1] as a novel form of cryptography that would not rely on computational hardness assumptions but on quantum means, and in particular quantum communications, to achieve information-theoretic security. Encoding classical information redundantly, on multiple copies of the same quantum state, could be highly beneficial from an engineering viewpoint, allowing for higher rates and better resilience to loss. However, this is a problem for the security of many quantum cryptography protocols as it would allow the adversary to gain more information about the underlying state than if just a single copy is sent. This limitation translates into a mean photon number that is typically upper bounded by 1 in QKD protocols, and more generally into the existence of a fundamental rate-loss trade-off that severely limits the distances over which we can perform QKD [2].

In this work, we explore a new approach to quantum cryptography, by considering a hybrid security model. In particular, we unlock the possibility of sending multiple copies

of the same state to perform key establishment with *everlasting security* [3] with performances that go beyond standard QKD. We specifically consider a cryptographic protocol built on top of the Hidden Matching quantum communication complexity problem [4, 5], for which there exists an exponential gap between classical and quantum strategies. We prove its security by establishing a reduction to the classical strategies for this communication complexity problem, effectively connecting the field of communication complexity and quantum cryptography.

1.2 QCT Security model

A novel security model called *Quantum Computational Time-lock (QCT)* was introduced in [6], building a bridge between the often disparate worlds of classical and quantum cryptography. The model is based on two nested assumptions. The first one is that Alice and Bob can use a t_{comp}-secure encryption scheme.

Definition 1.1 (t_{comp}-secure encryption scheme)**.** *An encryption scheme* $(Gen; Enc; Dec)$ *is said to be* t_{comp}*-secure if it is computationally secure with respect to any unauthorized attacker Eve for a time at least* t_{comp}*, after a ciphertext is exchanged on the classical channel,*

The second assumption is that an adversary Eve cannot reliably store a quantum state during a time larger than t_{comp} i.e. that she has access to what we call a (t_{comp}, δ)-noisy quantum memory, defined as follows.

Definition 1.2 ((t_{comp}, δ)-noisy quantum memory)**.** *A* (t_{comp}, δ)*-noisy quantum memory is a Markovian time-dependent quantum memory* Φ_t *such that at time* t_{comp}*:*

$$\|\Phi_{t_{comp}} - \mathcal{F}\|_\diamond \leq \delta \ , \tag{1}$$

where $\mathcal{F}(\rho) \coloneqq \frac{\mathrm{Tr}[\rho]}{d_{out}} \mathbb{1}_{d_{out}}$, $\|\cdot\|_\diamond$ *is the diamond norm [7] and* d_{out} *is the dimension of the output of the quantum memory.*

In other words, a (t_{comp}, δ)-noisy quantum memory is a quantum memory that is hard to distinguish (parametrized by a parameter δ) from a completely mixing channel $\mathcal{F}$, when it stores a quantum state for a time t_{comp} or longer. One can note that assuming that the coherence time of available quantum memories is much shorter than t_{comp} corresponds to taking $\delta \ll 1$.

1.2.1 Validity of QCT model

The validity of the QCT model is solidly grounded in practice when one considers existing and prospective quantum storage capabilities [8] and puts them in perspective with an extremely conservative lower bound on the time t_{comp} for which current encryption schemes would be considered secure, such as $t_{comp} \geq 10^5\, s \sim 1$ day. Moreover, it is interesting to understand that although the QCT assumptions set some limits to the scaling of quantum error-corrected quantum memory, it does not rule out the possibility of having useful quantum computers. Extrapolating for instance on [9] we see that 20 million noisy (with physical gate error 10^{-3}) qubits would be sufficient to factor a RSA 2048 key, using 10^4 logical qubits. However, considering the same resources, and the same number of logical qubits, they could be stored during only few hours. This would hence not rule out the conservative QCT assumptions mentioned above. We should also stress that the QCT approach enables us to build key establishment schemes that offer everlasting security. This

means that the secret keys can be provably secure against an adversary who is computationally unbounded after quantum storage decoherence, where the decoherence time to be considered is the one technologically available at the time of protocol execution. In particular, security holds against any future progress of the attacker's computational and quantum storage capabilities.

1.3 Our work

1.3.1 Sketch of the protocol

In our work we introduce an explicit construction for a new key distribution protocol called Hidden-Matching Quantum Computational Timelock (HM-QCT). It is built on top of a computational problem with a boolean output, called β-Partial Matching (βPM) [4], for which $\Omega(\sqrt{n})$ bits of communication from Alice to Bob are required, against only $\mathcal{O}(\log(n))$ qubits, with n the length of input x. In each round of the HM-QCT protocol Alice generates both inputs x and y and shares the latter with Bob using a computationally secure encryption scheme. Alice and Bob can then solve the βPM protocol with a quantum strategy to extract a bit, sending m copies of the same n-dimensional quantum state. See Figure 1 for a pictorial representation. Finally, by performing standard classical post-processing to their string of bits, they can distill a secure key.

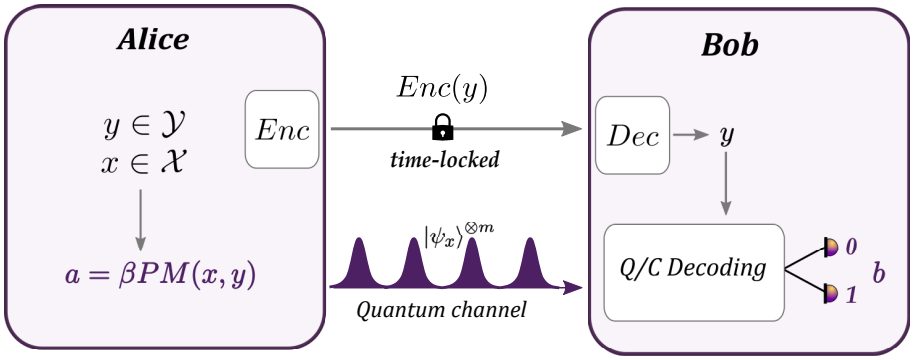

Figure 1: One round of the HM-QCT protocol

1.3.2 Advantages over standard QKD

Our results illustrate that the QCT hybrid security model constitutes a promising route to enhance the capabilities and effectiveness of quantum cryptography, while retaining some core advantage against classical cryptography: the possibility of providing everlasting security. In particular, our protocol offers the following benefits:

- **Boosted key rates:** Security can be achieved while sending up to $\mathcal{O}(\frac{\sqrt{n}}{\log(n)})$ photons per channel use, overcoming the standard limit of one photon per channel use. As detailed in Section 3, the HM-QCT protocol, based on the βPM problem, can be implemented with 2 single-mode threshold detectors, and performance can hence be benchmarked with 2-output-mode protocols. The fact that security can be achieved with many photons per channel use leads to asymptotic achievable secret key rates that can be boosted by a factor $\mathcal{O}(\frac{\sqrt{n}}{\log(n)})$ with respect to BB84 QKD. As illustrated on Figure 5, HM-QCT could moreover overcome the fundamental secret key capacity [2].

- **Improved functionalities:** A fascinating advantage of enabling multiple copies per channel use is the potential to consistently hit the classical capacity of one bit per channel use over relatively short distances, as illustrated in Figure 5 — a feat unseen in standard QKD. Moreover, multiple photons not only offer improved efficiency but also enable multicast key distribution with up to $\mathcal{O}(\frac{\sqrt{n}}{\log(n)})$ authorized Bobs simultaneously.

- **Security with untrusted detectors**: Eve's information can be upper bounded by only considering the state that Alice inputs and does not require (as in QKD) any information about Bob measurement results, as discussed in Section 3.3. Consequently, the implementation of Bob's measurement device is not required to be trusted, a property analog to measurement-device independent security.

Moreover, the security proof that we have established for a key distribution scheme based on the βPM problem could also be applied to any one-way communication complexity problem with a boolean output. The results obtained in this article hence also pave the way to the study of other communication complexity problems with larger gaps between classical and quantum strategies, which would lead to even greater performances.

1.3.3 Technical contributions

One of the main technical achievements has been to reduce Eve's general i.i.d. attack strategy, represented in Figure 4, to a strategy where she has no access to any quantum storage at the cost of an additive linear term in the noise parameter δ, as formally proved in Theorem 3.1. Since this result is solely based on the fact that an eavesdropper has access to a noisy memory in Definition 1.2, Theorem 3.1 could be of independent interest for other protocols that exploit noisy storage.

Once we reduce to an eavesdropper with no quantum memory, a central result of our work is the exploitation of the communication gap between quantum and classical strategies to build a secure key distribution protocol. In particular, the security reduction to the communication complexity of the βPM problem cannot be done directly. First, since Alice is sending m copies of the same n-dimensional quantum state, the amount of information that she is leaking to Eve about the input x is at most $m\log(n)$ bits thanks to the Holevo bound. This simply reduces the security proof to the study of the *information complexity* [10] of the classical βPM problem, a quantity which describes the amount information exchanged about the input needed to reliably solve the complexity problem.

Through mapping communication complexity to information complexity in the one-way setting in Lemma 2.1, we demonstrated in Theorem 3.2 that Eve's one-round guessing probability is safely bounded away from 1 when Alice sends $\mathcal{O}\left(\frac{\sqrt{n}}{\log(n)}\right)$ copies of the quantum state.

1.4 Previous work

Communication complexity [11] is a model of computation where two parties, Alice with input x and Bob with input y, collaborate to compute with high probability the value of $f(x,y)$, where f is a function (or relation) defining the computational problem that the players have to solve. An exponential separation in the required amount of communication between quantum and classical strategies has been already shown experimentally [12] and then used to build a private quantum money scheme [13]. However, to the best of our knowledge, ours is the first explicit quantum key distribution protocol that guarantees security based on this exponential separation.

On the other hand, it is not the first time that someone relies on physical limitations of the quantum storage capabilities to extend the functionality of QKD. In the quantum bounded-storage model, for example, by limiting the amount of quantum information that an eavesdropper can store and process, QKD protocols can be designed to allow for higher error rates compared to the standard model with unbounded adversaries [14]. An additional way to provide high resilience to noise, either caused by a malevolent Eve or simply environmental, is to perform QKD with high dimensional quantum states [15] in the standard security model. However, both these frameworks are still highly susceptible to loss, since their security is limited to send only one photon per channel use.

Another example is also the theoretical framework of Quantum Data Locking (QDL) [16], where the security of communication schemes is based on the even stricter assumption that quantum storage fully decoheres (i.e. $\delta = 0$) after some finite time. Existing work on QDL is either restricted to single-photon encoding [16, 17], with limitations in terms of loss-tolerance, or resorts to constructions based on random coding arguments [18] for which practical decoding measurements with current technologies are not possible.

Security models with limitations in the accuracy of the storage of quantum states do not solely focus on key distribution schemes. The noisy-storage model [19, 20] is indeed a well-known security model, which generalizes the quantum bounded-storage model. It has been used to prove security of two-party protocols such as oblivious transfer [21] and bit commitment [22], for which full unconditional security is impossible [23, 24]. Experimental demonstrations of these protocols were moreover performed, with typical hardware used in key distribution protocols, both for discrete [25, 26] and continuous variable protocols [27]. However, unlike the QCT model, both QDL and the noisy-storage model do not rely on any computational assumptions, but they force the adversary to store the quantum states by intentionally delaying the classical post-processing. While this solution is enough to prove security, it has clear setbacks in the speed of the key exchange which is an important practical consideration.

2 Preliminaries

2.1 General notation

We reserve capital letters for random variables and distributions, calligraphic letters for sets, and lowercase letters for elements of sets. Let $\mathcal{S}$ be a set. We use $\Delta(\mathcal{S})$ to denote the family of all probability distributions on $\mathcal{S}$. We use $\mathcal{D}(\mathcal{H})$, $\mathcal{L}(\mathcal{H})$ and $\mathcal{P}(\mathcal{H})$ to denote the space of density operators, square linear operators and positive operators, respectively, acting on a finite dimensional Hilbert space $\mathcal{H}$. Moreover, we will use extensively the notation $d_{[.]} \coloneqq \dim[\mathcal{H}_{[.]}]$. The trace norm on $\mathcal{L}(\mathcal{H})$ is defined as $\|\sigma\|_1 \coloneqq \mathrm{Tr}\sqrt{\sigma\sigma^\dagger}$.

Consider a classical random variable A with distribution P_A on some set $\mathcal{A}$. Since we are going to treat classical and quantum variables with the same formalism, it is useful to view A as a particular case of a quantum system. We shall identify the classical values $a \in \mathcal{A}$ with some fixed orthonormal basis $|a\rangle$ on some Hilbert space $\mathcal{H}_\mathcal{A}$. The random variable A can then be identified with the quantum state $\rho_A = \sum_{a\in\mathcal{A}} P_A(a) \, |a\rangle\langle a|$. We can extend this representation to hybrid settings where the state ρ_a of a quantum system $\mathcal{H}_Q$ depends on the value of a of a classical random variable A. Such a state is called a *classical-quantum state*, or simply *cq-state*, and takes the form $\rho_{AQ} = \sum_{a\in\mathcal{A}} P_A(a) \, |a\rangle\langle a| \otimes \rho_a$.

2.2 Classical and quantum information theory

We need to define some notions of classical and quantum information theory. First, we quantify the amount of information shared between two random variables A and B with distribution $P_{AB} \in \Delta(\mathcal{A}\times\mathcal{B})$ and marginal distributions P_A and P_B respectively. We call $I(A:B) \coloneqq H(A) - H(A|B)$, the *mutual information*, where $H(A) \coloneqq -\sum_a P_A(a)\log(P_A(a))$ is the *Shannon entropy* and $H(A|B) \coloneqq -\sum_{a,b} P_{AB}(a,b)\log\left(\frac{P_{AB}(a,b)}{P_A(a)}\right)$ is the conditional entropy.

Given any cq-state ρ_{AQ}, another useful quantity in quantum cryptography is the probability of guessing the random variable A for an adversary holding a quantum system Q, given by $P_{\text{guess}}(A|Q) \coloneqq \max_\Pi \sum_a P_A(a)\text{Tr}[\Pi(a)\rho_a]$, where we maximize over all POVMs $\Pi : A \to \mathcal{P}(\mathcal{H}_Q)$. Finally, we can define a conditional entropy, called the *min-entropy*, given by $H_{\min}(A|Q) \coloneqq -\log(P_{\text{guess}}(A|Q))$.

Now we introduce the generalization of Shannon entropy for quantum states, called the *von Neumann entropy*. The von Neumann entropy of $\rho \in \mathcal{D}(\mathcal{H}_A)$ is $H(A)_\rho \coloneqq -\text{Tr}[\rho\log(\rho)]$. One can notice that by considering a classical state we recover back the Shannon entropy. For a bipartite state $\rho_{AE} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_E)$, we use the notation ρ_E for $\text{Tr}_A[\rho_{AE}]$ and define the *conditional von Neumann entropy* of system A given system E when the joint system is in the state ρ_{AE} by $H(A|E)_\rho \coloneqq H(AE)_\rho - H(E)_\rho$. We can finally define the *quantum mutual information* as $I(A:B) \coloneqq H(A)_\rho - H(A|B)_\rho$.

2.3 One-way Communication and Information Complexity

Communication complexity is a computation model introduced by Yao [11]. It involves two players, Alice and Bob, who receive inputs: Alice receives x from set $\mathcal{X}$ and Bob receives y from set $\mathcal{Y}$. Their objective is to compute the value of $f(x,y)$ with high probability using allowed communication methods (classical or quantum). In this article, we focus on one-way settings, where only Alice can send messages to Bob. The message sent by Alice to Bob is called the *transcript*, and Bob's final guess of $f(x,y)$ is called the *output*. In the public-coin model, they share a random string r, while in the private-coin model, they have private random strings r_A and r_B. We start by defining the *communication cost* of a protocol and the *one-way distributional complexity* in the public-coin setting.

Definition 2.1 (Communication Cost)**.** *The communication cost of a public coin protocol π, denoted by $CC(\pi)$, is the maximum number of bits that can be transmitted in any run of the protocol.*

Definition 2.2 (One-way distributional complexity)**.** *For a function $f : \mathcal{X}\times\mathcal{Y} \to \mathcal{Z}$, a distribution $\mu \in \Delta(\mathcal{X}\times\mathcal{Y})$ and a parameter $\epsilon > 0$, we define the one-way distributional complexity $D^1_\mu(f,\epsilon)$ as the communication cost of the cheapest one-way deterministic protocol for computing f on inputs sampled according to μ with error ϵ, i.e.*

$$D^1_\mu(f,\epsilon) \coloneqq \min_{\pi:\, P_{(X,Y)}[\pi_{out}(x,y),\neq f(x,y)]\leq\epsilon} CC(\pi)\,, \tag{2}$$

where $\pi_{out}(x,y)$ describes Bob's output.

We also consider different relevant quantities that apply an information-theoretic formalism to computational settings.

Definition 2.3 (External Information Cost)**.** *Fix a one-way private-coin communication protocol π on inputs $\mathcal{X}\times\mathcal{Y}$ and a distribution $\mu \in \Delta(\mathcal{X}\times\mathcal{Y})$. The one-way external*

information cost of π with respect to μ, denoted by $IC^1_\mu(\pi)$ is defined as

$$IC^1_\mu(\pi) \coloneqq I(\Pi : X) \ , \tag{3}$$

where $\Pi = \Pi(X, R_A)$ describes the transcript of the protocol.

Intuitively, the external information cost captures how much information an external viewer who does not know the inputs learns about X. Similarly to the communication version, we can define the information complexity of a problem as the infimum over all possible protocols.

Definition 2.4 (One-way external information complexity)**.** *Let π be a one-way private-coin protocol on inputs $\mathcal{X} \times \mathcal{Y}$ and $\mu \in \Delta(\mathcal{X} \times \mathcal{Y})$. The one-way external information complexity of f with error tolerance ϵ is defined as the infimum of the one-way external information cost over all private-coin protocols π for computing f that achieve an error no larger than ϵ with respect to μ:*

$$IC^1_\mu(f, \epsilon) \coloneqq \inf_{\pi:\, P_{(X,Y),R_A,R_B}[\pi_{out}(x,y,r_A,r_B) \neq f(x,y)] \leq \epsilon} IC^1_\mu(\pi) \ , \tag{4}$$

where $\pi_{out}(x, y, r_A, r_B)$ describes Bob's output.

In this case we only considered a private-coin model, since one can see that any public randomness can be simulated by a private-coin model: Alice can send to Bob a portion of r_A together with the private-coin transcript. Now they can use this portion as shared randomness r. However, while this extra step increases the communication cost, it doesn't affect the external information cost.

2.3.1 From distributional to information complexity

In [28], the authors demonstrated that it is possible to compress each message of a protocol to approximately its contribution to the external information cost plus some additional constant term. While the authors focused only on the scaling laws, we carefully derived all the specific constants for the compression scheme. We refer to the Appendix A for a description of how to derive the theorem from [29].

Theorem 2.1 (Message compression)**.** *Consider a message M sent by Alice, who holds X. M is extracted from a conditional probability distribution $P_{M|X}$. Alice and Bob can use public randomness to simulate[1] sending M by sending an expected number of bits upper bounded by $I(X : M) + 1.262 \log(1 + I(X : M)) + 11.6$. The simulation is one round (i.e. only Alice has to send information) and without error.*

Finally, one can then map the one-way distributional communication complexity to the external information complexity in a one-way setting, exploiting the message compression in Theorem 2.1, obtaining the result in [28, Lemma V.3] with explicit constants.

Lemma 2.1 (Mapping to information complexity)**.** *Let $\epsilon, \delta_2 > 0$, $\mu \in \Delta(\mathcal{X} \times \mathcal{Y})$ and $f : \mathcal{X} \times \mathcal{Y} \to \mathcal{Z}$. Then*

$$IC^1_\mu(f, \epsilon) \geq \frac{\delta_2}{2} D^1_\mu(f, \epsilon + \delta_2) - 6 \ .$$

[1] Instead of sending directly M, Alice and Bob can use their shared randomness to decrease the number of bits Alice has to send, while Bob can still retrieve completely the message M.

Proof. Let f be a function, $\mu \in \Delta(\mathcal{X} \times \mathcal{Y})$ be a joint probability distribution over the inputs of f, and π a one-way private-coin protocol which computes f with error upper bounded by ϵ such that

$$IC^1_\mu(\pi) \leq IC^1_\mu(f, \epsilon) + 0.05 \,. \tag{5}$$

We use Theorem 2.1 to deduce a new one-way public-coin protocol π' such that the average size of the transcript is upper bounded by

$$\mathbb{E}(|\Pi'|) \leq I(\Pi : X) + 1.262 \log(1 + I(\Pi : X))) + 11.6$$

and the error probability is at most ϵ. Then we apply the inequality $1.262 \log(1 + x) \leq x + 0.3$ for any $x \geq 0$ to deduce

$$\begin{aligned}\mathbb{E}(|\Pi'|) \leq & I(\Pi : X) + 1.262 \log(1 + I(\Pi : X))) + 11.6 \\ \leq & 2I(\Pi : X) + 11.9 \\ \leq & 2IC^1_\mu(f, \epsilon) + 12 \,,\end{aligned}$$

where in the last inequality we used (5). By using Markov's inequality, we can create a new protocol π'' which is identical to π' except when the transcript Π'' has size greater than $\frac{1}{\delta_2}\mathbb{E}(|\Pi'|)$, then the protocol simply aborts. By suitably fixing the public randomness, one can a deterministic protocol which has probability to fail upper bounded by $\epsilon + \delta_2$ and a communication cost at most $\frac{2IC^1_\mu(f,\epsilon)+12}{\delta_2}$. The lemma then follows from Definition 2.2 (see Eq. (2)).

□

2.4 β-Partial Matching problem

In this subsection we shall present the quantum communication complexity problem that we want to use to build a key distribution protocol. Let $n \in \mathbb{N}$. We use the notation $[n] = \{1, ..., n\}$. In the following n will be assumed to be even. A *matching* M is a set of pairs $(a, b) \in [n]^2$, such that no two pairs contain the same index, where, each index is called a *vertex* and a pair of vertices is called an *edge*. For example if $n = 4$ then the set of edges $\{(1, 2), (3, 4)\}$ or $\{(2, 3)\}$ are valid matchings whereas $\{(1, 2), (2, 3)\}$ are not. See Figure 2 for a pictorial representation.

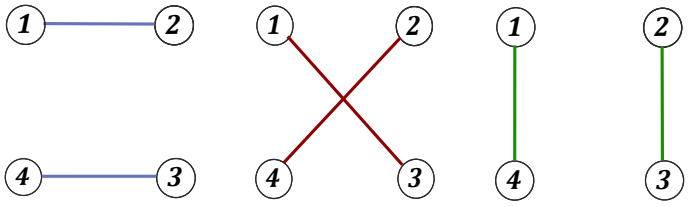

Figure 2: Illustration of a set of perfect matchings for size $n = 4$. For example, considering $x = 1001$, $\omega = 11$, for the first perfect matching in blue we have $Mx = \begin{bmatrix} x_1 \oplus x_2 = 1 \\ x_3 \oplus x_4 = 1 \end{bmatrix}$, resulting in $a = 0$.

We say M is a β-*matching* if in addition $|M| = \beta n$. The βPM problem is built around a β-matching M, that constitutes part of the input given to Bob. M consists of a sequence of βn disjoint edges $(i_1, j_1)...(i_{\beta n}, j_{\beta n})$ over $[n]$. We will call $\mathcal{M}_{\beta n}$ the set of all β-matchings on n bits: if $\beta = \frac{1}{2}$ the matching is called *perfect* and if $\beta < \frac{1}{2}$ the matching is called *partial*. M can be represented as a $\beta n \times n$ matrix with only a single one in each column

and two ones per row, namely at position i_l and j_l for the l-th row of matrix M. Let $x \in \{0,1\}^n$, applying the matching M to x leads to the βn-bit string $v = v_1, ..., v_l, ..., v_{\beta n}$ where $v_l = x_{i_l} \oplus x_{j_l}$. Finally, we call $a^{\beta n}$ a vector of dimension βn with value a in each component. Using the notation above, we can finally define the βPM problem:

Alice's input: $x \in \{0,1\}^n$.
Bob's input: $M \in \mathcal{M}_{\beta n}$ and $\omega \in \{0,1\}^{\beta n}$.
Promise P: given a bit $a \in \{0,1\}$, then $\omega = Mx \oplus a^{\beta n}$.
Communication Model: Classical or Quantum one-way communication between Alice and Bob.
Goal: Bob outputs $b = a$ with high probability.

We shall call for clarity $\mathcal{X} \coloneqq \{0,1\}^n$, $y \coloneqq (M, \omega)$ and $\mathcal{Y} \coloneqq \mathcal{M}_{\beta n} \times \{0,1\}^{\beta n}$. Moreover, we define the (partial) function $\beta PM : \mathcal{X} \times \mathcal{Y} \to \{0,1\}$ as the function that randomly picks an element from the vector $Mx \oplus \omega$.

Input distribution: we call $\mu \in \Delta(\mathcal{X} \times \mathcal{Y})$ the input probability distribution uniform over $x \in \{0,1\}^n$ and $M \in \mathcal{M}_{\beta n}$. The inputs x and M together determine the βn-bit string $v = Mx$. To complete the input distribution, with probability $1/2$ we set $\omega = v$ and with probability $1/2$ we set $\omega = \bar{v}$.

Finally, one can derive from [4] the prefactors of the scaling law for the one-way distributional complexity of the βPM protocol.

Theorem 2.2. *Let $\beta \in (0, 1/4]$, $\forall \epsilon \in (0, \frac{1}{2}]$. Then*

$$D^1_\mu(\beta PM, \epsilon) \geq k(\epsilon)\sqrt{n} + d(\epsilon) \ , \tag{6}$$

where

$$k(\epsilon) = \frac{4\gamma}{25\sqrt{\beta}}\Big(\frac{1}{2} - \epsilon\Big)^2 \quad \textit{and} \quad d(\epsilon) = 2\log\Big(\frac{1}{2} - \epsilon\Big) + 2(\log(2) - \log(5)) \ , \tag{7}$$

with $\gamma = \frac{1}{8e}$.

Proof. A complete description of how to derive this theorem from [4] is given in Appendix C. □

3 Key Establishment Protocol

3.1 Security model and definitions

Considering the novelty of our hybrid security model, the assumptions on the resources of an adversary and the security properties that can be achieved in this model must be described thoroughly.

In the QCT construction, authorized parties, Alice and Bob, are assumed to be connected via a noiseless and authentical classical channel and an insecure quantum channel. An adversary, Eve, is assumed to have full access to the input of Alice and Bob's communication channels. Every classical (quantum) message communicated between Alice and Bob over the classical (quantum) channel can be wiretapped by Eve and stored in classical (quantum) memory. With this pessimistic setting for Eve's channel, we are in a similar set-up as strong data locking [16, 30] wherein an adversary Eve receives direct inputs from Alice. As stated in Section 1.2, the QCT model is based on two main assumptions on the power of an eavesdropper: a computational assumption (see Definition 1.1) and a noisy-storage assumption (see Definition 1.2).

We start by stating the type of computational assumption needed to prove security in our scheme. What Alice and Bob need is a *semantically secure* symmetric encryption scheme against adaptive chosen-ciphertext attacks (CCA2) for a time at least t_{comp}. Semantic security means that it is computationally unfeasible for an eavesdropper to learn any partial information about a plaintext from the corresponding ciphertext (see [31] for a formal definition.) This implies that the encrypted message $Enc_k(m)$ is (computationally) indistinguishable from a completely random string until at least a time t_{comp}. Furthermore, the security against adaptive chosen-ciphertext attacks ensures another required property: *non-malleability* [31]. In simple terms, an encryption scheme is called non-malleable if one cannot feasibly manipulate a given ciphertext in such a way that it produces another ciphertext, which, when decrypted, yields a plaintext related to the original. Finally, the desired security for the hybrid key distribution protocol is based on the *trace distance criterion* [32], a standard criterion to prove information-theoretic security for quantum key distribution.

3.2 Protocol description

Now that we have introduced all the crucial ingredients, we can present and analyze our protocol. The main building block for our construction is an explicit quantum communication protocol that solves the βPM problem by simply sending a constant number of n-dimensional quantum states [4].

3.2.1 βPM quantum protocol

Alice sends a uniform superposition of her bits to Bob:

$$|\psi_x\rangle = \frac{1}{\sqrt{n}} \sum_{i=1}^{n} (-1)^{x_i} |i\rangle \ . \tag{8}$$

Bob completes his βn edges to a perfect matching in an arbitrary way and measures with the corresponding set of $n/2$ rank 2 projectors, where for an edge (a, b) the projector is $P = |a\rangle\langle a| + |b\rangle\langle b|$. With probability 2β he will receive an output corresponding to one of the edges (i_l, j_l) from his input β-matching M. The state then collapses to $\frac{1}{\sqrt{2}}((-1)^{x_{i_l}} |i_l\rangle + (-1)^{x_{j_l}} |j_l\rangle$, from which Bob can obtain the bit $v_l = x_{i_l} \oplus x_{j_l}$ using a measurement containing projectors $\{|+\rangle\langle +|, |-\rangle\langle -|\}$, where $|+\rangle = (|i_l\rangle + |j_l\rangle)/\sqrt{2}$ and $|-\rangle = (|i_l\rangle - |j_l\rangle)/\sqrt{2}$, and immediately retrieve the bit a. With probability $1 - 2\beta$, instead, he will receive an output that doesn't correspond to any edge of the β-matching M: in this case, he immediately outputs $b = \perp$, aborting the protocol. One important point is that Bob can perform his measurement with only two single photon detectors, since he can pre-route, in accordance with $(M; \omega)$ the output of the n beamsplitters. See Figure 3 for a pictorial representation.

In practice the quantum channel and detectors will be subject to loss and errors. What Alice and Bob can implement is a practical version of the βPM protocol, described in detail in Appendix B, where they compensate for the loss by sending several copies of the same state $|\psi_x\rangle$.

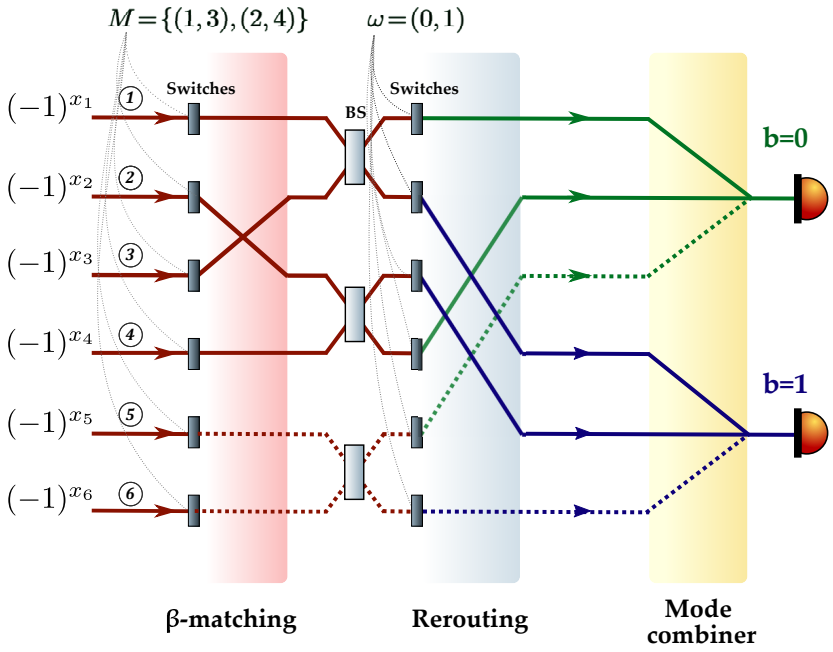

Figure 3: Illustration of a possible implementation of Bob's decoding with $n = 6$ spatial modes and $\beta = 1/3$. In the β-matching part Bob uses his knowledge of M to control each switch and direct each mode to the corresponding beam splitter (BS). The modes with dotted lines are blocked instead, since they don't correspond to any vertex of the partial matching. Then, in the rerouting part, he reorders the modes based on ω. Finally, thanks to a mode combiner, he directs the first (second) half of the modes to the first (second) detector.

3.2.2 HM-QCT key distribution scheme

Now that we have described the main building block, we are ready to present our hybrid key distribution protocol.

HM-QCT Protocol

Parameters:

- dimension n of the problem
- number of copies m
- number of rounds l.

1. **Data Generation:**
   - Alice generates and stores $\vec{x} = (x_1, ...x_l)$ and $\vec{y} = (y_1, ...y_l)$ from the probability distribution $\mu^l \in \Delta^l(\mathcal{X} \times \mathcal{Y})$. She then computes and stores the string $\vec{a} = (a_1, ..., a_l)$, where $a_j = \beta PM(x_j, y_j)$.

2. **QCT exchange**
   - Alice and Bob run Gen and obtain a shared secret k.
   - Alice sends $Enc_k(\vec{y})$ to Bob.
   - Bob decrypts $Enc_k(\vec{y})$ using Dec_k, obtaining $\vec{y}$.

3. **Quantum communication**
   - for $i = 1$; $i \leq l$; $i++$

– Alice and Bob run the βPM quantum protocol, with input x_i and y_i. Bob stores the output b_i.

4. **Sifting:**
   - Alice and Bob discard all rounds with $b_i = \perp$.

5. **Classical post processing:**
   - Parameter estimation: Alice and Bob estimate the quantum bit error rate (QBER) i.e. the error rate of a conclusive round, by revealing a part of their string.
   - Alice and Bob perform *error correction* [33] followed by *privacy amplification* [34] to distill a secret key.

Remark 3.1. The correctness of our protocol is ensured by the correctness of the βPM protocol together with an extra step of error correction to deal with noise and loss present in practical scenarios.

3.3 Security Analysis

3.3.1 Achievable key rate in the i.i.d. setting

We now focus on how to derive an achievable key rate within our model. In this article we shall analyze the security of our key distribution protocol in the i.i.d.∼setting, i.e. a restricted case where the adversary Eve performs the same strategy independently on every round. In this setting, we can consider, without loss of generality, the most general attack from Eve on a single round of the protocol. It consists of immediately applying an encoding operation $\mathcal{E} : \mathcal{L}((\mathbb{C}^n)^{\otimes m}) \to \mathcal{L}(\mathcal{H}_Z \otimes \mathcal{H}_{Q_{in}})$ statistically independent of y due to the semantic security of the encryption scheme, before storing the quantum state on her (t_{comp}, δ)-noisy quantum memory $\Phi_{t_{comp}} : \mathcal{L}(\mathcal{H}_{Q_{in}}) \to \mathcal{L}(\mathcal{H}_{Q_{out}})$, following a similar strategy of [27]. Moreover, the non-malleability of the classical encryption scheme prevents Eve from running any homomorphic strategy, i.e. a quantum operation depending also on $Enc_k(y)$, which could eventually leak sensitive information. The encoding $\mathcal{E}$ also includes a classical outcome Z that can, for instance, result from measuring part of the copies. Moreover, we consider that after the time t_{comp}, Eve is given the encrypted secret y, i.e. that Enc can be fully decrypted after t_{comp}, which is the most favorable case for Eve.

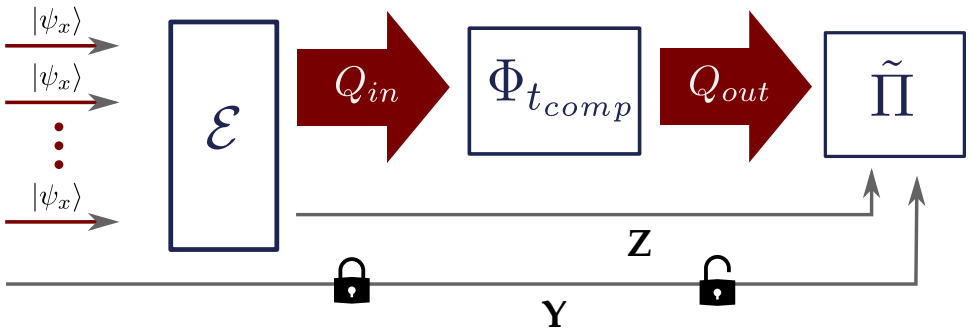

Figure 4: General form of an attack of Eve. It consists in an encoding $\mathcal{E}$ that maps (conditioned on some classical outcome Z) the m copies of Alice's quantum state to the memory input Q_{in}. At time t_{comp}, when she unlocks the secret Y, she decodes the key bit by performing the measurement $\tilde{\Pi}$ on Q_{out} using both the secret Y and the classical outcome Z.

One should note that this general strategy also includes the limit strategies where Eve either simply stores the quantum input[2] $|\psi_x\rangle^{\otimes m}$, since we have never given any bound on the dimension of our memory, or the case where she measures all the copies immediately. Moreover, any strategy that consists of performing any general measurement at times different from 0 and t_{comp}, even if surely suboptimal, can be described by this general strategy. As a consequence of this setting, at the end of each round Alice and Bob have access to a realization of correlated classical random variables A and B, respectively, whereas the adversary Eve holds the quantum system $E = YZQ_{out}$. The final joint state for each round between Alice and Eve will therefore have the form

$$\rho_{AYZ\Phi_{t_{comp}}(Q_{in})} = \sum_{x,y,a} \mu(x,y)\delta_{\beta PM(x,y),a} \\ |a\rangle\langle a| \otimes |y\rangle\langle y| \otimes (\mathbb{1}_{d_{\mathcal{Z}}} \otimes \Phi_{t_{comp}})(\mathcal{E}(\rho_x)) \ . \tag{9}$$

At this point Eve performs the POVM $\tilde{\Pi} : \{0,1\} \to \mathcal{P}(\mathcal{H}_{\mathcal{Y}} \otimes \mathcal{H}_{\mathcal{Z}} \otimes \mathcal{H}_{Q_{out}})$ on the output of the quantum memory to guess the bit a, making use of y and the classical string z. Finally, we can lower bound the achievable key rate under this general i.i.d. attack, depicted on Figure 4. Since the min-entropy lower-bounds the von Neumann entropy, we can lower bound the Devetak-Winter bound [36] and obtain the following achievable key rate

$$R \geq (1 - P(\text{abort}))(H_{min}(A|E) - H_2(\text{QBER})) \ , \tag{10}$$

where $H_{min}(A|E) = -\log(P_{\text{guess}}(A|YZ\Phi_{t_{comp}}(Q_{\text{in}})))$, H_2 is the binary Shannon entropy, and $P(\text{abort})$ is the probability that a round of the protocol is inconclusive. In Appendix B we have evaluated $P(\text{abort})$ and QBER as a function of the number of copies sent m in a practical scenario.

3.3.2 Bounding $P_{\text{guess}}(A|YZ\Phi_{t_{comp}}(Q_{\text{in}}))$

We now compute a lower bound for the achievable key rate in Eq. (10). In particular here we focus on computing $H_{min}(A|E)$. We evaluate Eve's guessing probability $P_{\text{guess}}(A|YZ\Phi_{t_{comp}}(Q_{\text{in}}))$ in two steps. First we want to bound it with respect to a restricted strategy where she never uses a noisy quantum memory, but she performs immediately a joint measurement on the m copies. We call such a strategy an *immediate measurement strategy*. The second step consists instead in deriving a bound on the guessing probability of this restricted strategy by exploiting the communication complexity gap between quantum and classical strategies for the βPM protocol.

3.3.3 Reduction to immediate measurement

In this restricted scenario, following a standard post-measurement information strategy [37], Eve performs an immediate measurement $\mathcal{Z} : \mathcal{L}((\mathbb{C}^n)^{\otimes m}) \to \mathcal{L}(\mathcal{H}_{\mathcal{Z}})$ on the input state $\rho_x := (|\psi_x\rangle\langle\psi_x|)^{\otimes m}$ and obtains a classical outcome z. At time t_{comp}, she unlocks y and extracts the final guess by performing a classical decoding $\tilde{\Pi}_1$, that can be expressed

[2]Storing all copies simultaneously and measuring once the encrypted message y is unlocked can be viewed a generalized version of the photon number splitting attack (PNS) [35]. In PNS, eavesdroppers store extra photons in their quantum memory until they obtain the basis information, enabling them to execute the appropriate measurement.

as a POVM $\tilde{\Pi}_1 : \{0,1\} \to \mathcal{P}(\mathcal{H}_\mathcal{Y} \otimes \mathcal{H}_\mathcal{Z})$. The guessing probability can therefore be written as

$$P_{\text{guess}}(A|Y\mathcal{Z}(Q)) \coloneqq \max_{\tilde{\Pi}_1} \sum_{x,y,a} \mu(x,y)\delta_{\beta PM(x,y),a} \text{Tr}[\tilde{\Pi}_1(a)(|y\rangle\langle y| \otimes \mathcal{Z}(\rho_x))] \ . \tag{11}$$

To show the security reduction we first prove the following useful (and more general) theorem.

Theorem 3.1. *If $\|\Phi - \mathcal{F}\|_\diamond \leq \delta$, with $\mathcal{F}$ being the completely mixing channel, then for any cqq-state ρ_{AXQ} we have*

$$P_{guess}(A|X\Phi(Q)) \leq P_{guess}(A|X) + \delta \ . \tag{12}$$

Proof. We can bound the guessing probability as follows

$$\begin{aligned} P_{guess}(A|X\Phi(Q)) =& \max_{\Pi} \sum_a p(a)\text{Tr}[\Pi(a)\Phi(\rho_{XQ})] \\ \leq& \max_{\Pi} \sum_a p(a)\Big(\|\Pi(a)\|_\infty \|(\Phi - \mathcal{F})(\rho_{XQ})\|_1 + \text{Tr}[\Pi(a)\mathcal{F}(\rho_{XQ})]\Big) \\ \leq& \delta + \max_{\Pi} \sum_a p(a)\text{Tr}[\Pi(a)\mathcal{F}(\rho_{XQ})] \ , \end{aligned}$$

where we used the notation $\mathcal{N}(\rho_{XQ}) \coloneqq (\mathbb{1}_{d_\mathcal{X}} \otimes \mathcal{N})(\rho_{XQ})$ for any quantum channel $\mathcal{N}$ acting only on Q. In the second line we used the Hölder's inequality, while the last inequality is obtained by noticing that $\|M\|_\infty \leq 1$ for any element of a POVM, the fact that $\sum_a p(a) = 1$, and the fact that $\|(\Phi - \mathcal{F})(\rho_{AX})\|_1 \leq \delta$, since we have $\|\Phi - \mathcal{F}\|_\diamond \leq \delta$. Finally, since $\mathcal{F}$ destroys all the quantum information in the system Q, we directly have $\max_\Pi \sum_a p(a)\text{Tr}[\Pi(a)\mathcal{F}(\rho_{XQ})] = P_{guess}(A|X)$ which concludes the proof. □

Now from Theorem 3.1 we simply have that for any encoding attack

$$\begin{aligned} P_{\text{guess}}(A|YZ\Phi_{t_{comp}}(Q_{\text{in}})) \leq& P_{guess}(A|YZ) + \delta \\ \leq& \max_{\mathcal{Z}} P_{\text{guess}}(A|Y\mathcal{Z}(Q)) + \delta \ , \end{aligned} \tag{13}$$

where we maximized over all possible Eve's immediate measurements $\mathcal{Z}$. Hence, considering $\delta \ll 1$, we have successfully reduced any general attack strategy to an immediate joint measurement on the m multiple copies.

3.3.4 Exploiting the complexity gap

To finally estimate an upper bound to Eve's guessing probability we still have to study this restricted scenario. Our approach for a full proof follows the idea that extracting a bit of the key with an immediate measurement strategy is as hard as solving the classical βPM problem. In particular, Eve cannot do better than what one would get for the βPM problem by sending $m\log(n)$ bits of information about the input x, where $m\log(n)$ bits is the maximum classical information one can extract from m copies of a n-dimensional quantum state thanks to the Holevo bound.

Lemma 3.1. *$\forall \epsilon \in (0, \frac{1}{2})$ if an immediate measurement strategy with $P_{guess}(A|Y\mathcal{Z}(Q)) \geq 1 - \epsilon$ exists, then Alice has sent m copies of the quantum state (8), with*

$$m \geq \frac{IC^1_\mu(\beta PM, \epsilon)}{\lceil \log(n) \rceil} \ .$$

Proof. Let's suppose there exists an immediate measurement strategy with $P_{\text{guess}}(A|Y\mathcal{Z}(Q))$ at most $1-\epsilon$, then we can transform this strategy into a classical protocol to solve the βPM problem. The transformation is straightforward, Alice generates m copies of the quantum state (8), then she immediately performs the measurement $\mathcal{Z}$ and sends the classical output z to Bob who, after performing the final POVM $\tilde{\Pi}_1$ on z and y, will output the correct answer with probability at least $1-\epsilon$. Note that the string z is the transcript of the protocol. Since from Holevo's bound we know that $I(X;Z) \leq m\lceil\log(n)\rceil$, by definition of $IC^1_\mu(\beta PM, \epsilon)$ we have

$$m \geq \frac{IC^1_\mu(\beta PM, \epsilon)}{\lceil\log(n)\rceil}$$

that concludes the proof. □

Finally, thanks to the complexity gap between classical and quantum strategies, Theorem 3.2 ensures that Eve's guessing probability is safely bounded far from 1 as long as Alice is sending $\mathcal{O}(\frac{\sqrt{n}}{\log(n)})$ copies of the quantum state.

Theorem 3.2. *Let us suppose $n \geq 4$. For any encoding attack Eve's guessing probability is bounded by*

$$P_{guess}(A|YZ\Phi_{t_{comp}}(Q_{in})) \leq \frac{1}{2} + 2\left(\sqrt[3]{-q} + \sqrt{\frac{p}{3}}\right) + \delta, \tag{14}$$

with

$$q = \frac{-50}{\sqrt{n}} e\sqrt{\beta}((m+1)\lceil\log(n)\rceil + \ln(4) + 6)$$
$$p = \frac{-50}{\sqrt{n}} e\sqrt{\beta}\Big(\log\left(\frac{5}{2}\right) - \ln(4)\Big).$$

Proof. The proof is given in Appendix E. □

Remark 3.2. From Theorem 3.2 we can effectively establish a bound on the min-entropy $H_{\min}(A|E)$. Notably, this bound is independent of Bob's measurements, ensuring security in a measurement-device-independent manner.

3.3.5 Everlasting secure key expansion

The security analysis shows that, within the QCT model, we can simplify the scenario to one where Eve's interaction (measurement) on the quantum state occurs right at the beginning, at $t = 0$. The security analysis after t_{comp}, then purely relies on information-theory principles. Hence the resulting key rates are valid against an adversary with unbounded computational power after t_{comp}, i.e. our schemes have everlasting security [3]. We note that everlasting secure key establishment cannot be attained with cryptographic protocols relying solely on classical communication, even with computational assumptions. Classical communication can be copied, making harvesting attacks (store now, attack later) a significant vulnerability.

Furthermore, to ensure the effectiveness of our hybrid key distribution scheme, the rate of secure key generation must exceed the rate of key consumption due to the need for a pre-shared key. One way to achieve this is by employing a block cipher in the QCT exchange described in Section 3.2, where Alice divides the message $\vec{y}$ into fixed-size blocks. As a block cipher can encrypt an exponential number of blocks in the key size, the rate of pre-shared key consumption grows logarithmically with the number of protocol rounds, while the final key size increases linearly, ensuring secure key expansion.

3.4 Key rate from best-known protocol

Theorem 3.2 is a significant result, derived from a lower bound of the one-way information complexity of the βPM problem, but this bound may not be tight. In fact, the error $\epsilon_{BKP}(d)$ from the best-known classical protocol with a communication cost d, analyzed in Appendix D, is quite larger than what one would get from the lower bound. Nevertheless, one can consider an optimistic scenario where the actual one-way information complexity for any error ϵ is equal to the information cost of the best-known protocol[3]. In this context, by combining Theorem 3.1 and Lemma 3.1 we have $P_{\text{guess}}(A|YZ\Phi_{t_{comp}}(Q_{\text{in}})) \leq 1 - \epsilon_{BKP}(m\lceil\log(n)\rceil) + \delta$.

Consequently, in Figure 5 we plot the achievable key rate from (10), considering the best-known classical protocol, and performing numerical optimization on the number of copies m. Since our protocol is implemented using two detection modes, effectively sending

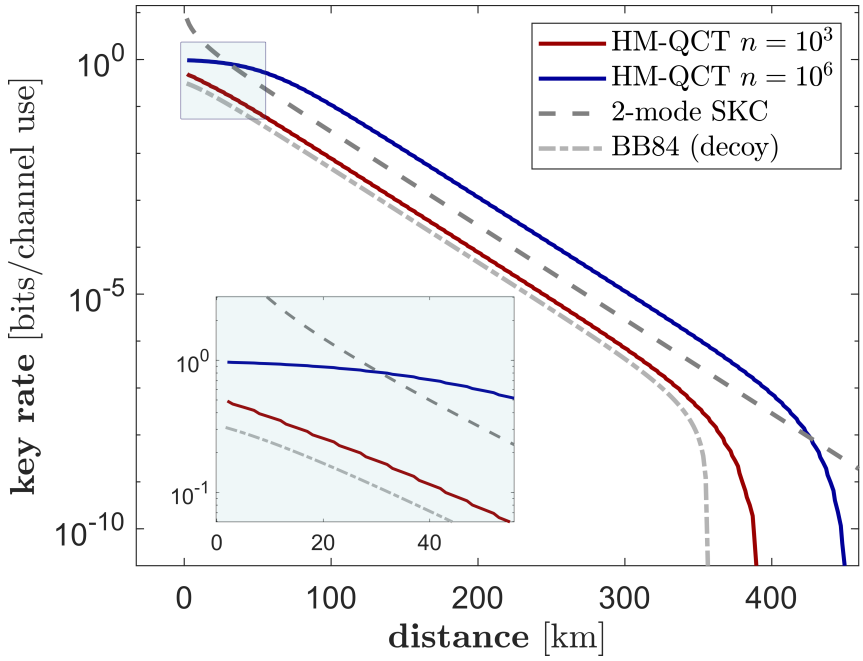

Figure 5: Key rate comparison between the upper bound for the HM-QCT protocol with $\delta = 10^{-4}$ and $\beta = \frac{1}{4}$, the BB84 protocol with decoy states [38] and the 2-mode Secret Key Capacity (SKC) [2], The plot for the HM-QCT protocol is derived under a practical implementation, as detailed in Appendix B. For both the HM-QCT protocol and the BB84 protocol with decoy states, we used the same detector specifications. These detectors are state-of-the-art SNSPDs, as detailed in [39], characterized by a dark count probability of $P_{\text{dark}} = 10^{-8}$ and a detection efficiency of $\eta_{\text{det}} = 65\%$.

at most one bit per channel use, we benchmark it with two standard key rate limits: the BB84 protocol with decoy states [38] and the more general limit for 2-mode optical key distribution [2]. From the plot we note that we can overcome the former with only a thousand modes. Notably, an experimental implementation of a variant of the quantum βPM protocol has already been performed with a similar number of modes [12]. We also observe that by increasing the number of modes n we can provide a key rate of almost one bit per channel use for short distances since at least one photon always reaches the detectors. At longer distances, the key rate scaling is similar to the 2-mode QKD limit,

[3]In other words, assuming that future developments on finding tighter lower bounds will show that the current best-known classical protocol is the optimal protocol.

decaying exponentially with distance, since Bob receives on average less than one photon per channel use. Ultimately, the protocol is constrained at very long distances by detector dark counts, drastically restricting the achievable key rate.

References

[1] Charles H. Bennett and Gilles Brassard. "Quantum cryptography: Public key distribution and coin tossing". Theoretical Computer Science **560**, 7–11 (2014).

[2] Stefano Pirandola, Riccardo Laurenza, Carlo Ottaviani, and Leonardo Banchi. "Fundamental limits of repeaterless quantum communications". Nature Communications **8**, 15043 (2017).

[3] Dominique Unruh. "Everlasting Multi-party Computation". In Ran Canetti and Juan A. Garay, editors, Advances in Cryptology – CRYPTO 2013. Pages 380–397. Lecture Notes in Computer ScienceBerlin, Heidelberg (2013). Springer.

[4] Dmitry Gavinsky, Julia Kempe, Iordanis Kerenidis, Ran Raz, and Ronald de Wolf. "Exponential separations for one-way quantum communication complexity, with applications to cryptography". In Proceedings of the Thirty-Ninth Annual ACM Symposium on Theory of Computing. Pages 516–525. STOC '07New York, NY, USA (2007). Association for Computing Machinery.

[5] Ziv Bar-Yossef, T.s Jayram, and Iordanis Kerenidis. "Exponential separation of quantum and classical one-way communication complexity". In Electronic Colloquium on Computational Complexity (ECCC). Pages 128–137. (2004).

[6] Nilesh Vyas and Romain Alleaume. "Everlasting Secure Key Agreement with performance beyond QKD in a Quantum Computational Hybrid security model" (2020). arxiv:2004.10173.

[7] John Watrous. "The Theory of Quantum Information". Cambridge University Press. (2018). 1 edition.

[8] Khabat Heshami, Duncan G. England, Peter C. Humphreys, Philip J. Bustard, Victor M. Acosta, Joshua Nunn, and Benjamin J. Sussman. "Quantum memories: Emerging applications and recent advances". Journal of Modern Optics **63**, 2005–2028 (2016).

[9] Craig Gidney and Martin Ekerå. "How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits". Quantum **5**, 433 (2021).

[10] Mark Braverman and Anup Rao. "Information Equals Amortized Communication" (2011). arxiv:1106.3595.

[11] Andrew Chi-Chih Yao. "Some complexity questions related to distributive computing(Preliminary Report)". In Proceedings of the Eleventh Annual ACM Symposium on Theory of Computing. Pages 209–213. STOC '79New York, NY, USA (1979). Association for Computing Machinery.

[12] Niraj Kumar, Iordanis Kerenidis, and Eleni Diamanti. "Experimental demonstration of quantum advantage for one-way communication complexity surpassing best-known classical protocol". Nature Communications **10**, 4152 (2019).

[13] Niraj Kumar. "Practically Feasible Robust Quantum Money with Classical Verification". Cryptography **3**, 26 (2019).

[14] Ivan B. Damgård, Serge Fehr, Renato Renner, Louis Salvail, and Christian Schaffner. "A Tight High-Order Entropic Quantum Uncertainty Relation with Applications". In Alfred Menezes, editor, Advances in Cryptology - CRYPTO 2007. Pages 360–378. Lecture Notes in Computer ScienceBerlin, Heidelberg (2007). Springer.

[15] Daniele Cozzolino, Beatrice Da Lio, Davide Bacco, and Leif Katsuo Oxenløwe. "High-Dimensional Quantum Communication: Benefits, Progress, and Future Challenges". Advanced Quantum Technologies **2**, 1900038 (2019).

[16] Cosmo Lupo and Seth Lloyd. "Quantum-Locked Key Distribution at Nearly the Classical Capacity Rate". Physical Review Letters **113**, 160502 (2014).

[17] Daniel J. Lum, John C. Howell, M. S. Allman, Thomas Gerrits, Varun B. Verma, Sae Woo Nam, Cosmo Lupo, and Seth Lloyd. "Quantum enigma machine: Experimentally demonstrating quantum data locking". Physical Review A **94**, 022315 (2016).

[18] Cosmo Lupo and Seth Lloyd. "Continuous-variable quantum enigma machines for long-distance key distribution". Physical Review A **92**, 062312 (2015).

[19] Stephanie Wehner, Christian Schaffner, and Barbara Terhal. "Cryptography from Noisy Storage". Physical Review Letters **100**, 220502 (2008). arxiv:0711.2895.

[20] Robert Koenig, Stephanie Wehner, and Juerg Wullschleger. "Unconditional security from noisy quantum storage". IEEE Transactions on Information Theory **58**, 1962–1984 (2012). arxiv:0906.1030.

[21] Manuel B. Santos, Paulo Mateus, and Armando N. Pinto. "Quantum oblivious transfer: A short review". Entropy **24**, 945 (2022). arxiv:2206.03313.

[22] Álvaro J. Almeida, Ricardo Loura, Nikola Paunković, Nuno A. Silva, Nelson J. Muga, Paulo Mateus, Paulo S. André, and Armando N. Pinto. "A brief review on quantum bit commitment". In Second International Conference on Applications of Optics and Photonics. Volume 9286, pages 189–196. SPIE (2014).

[23] Hoi-Kwong Lo and H. F. Chau. "Why quantum bit commitment and ideal quantum coin tossing are impossible". Physica D: Nonlinear Phenomena **120**, 177–187 (1998).

[24] Harry Buhrman, Matthias Christandl, and Christian Schaffner. "Complete Insecurity of Quantum Protocols for Classical Two-Party Computation". Physical Review Letters **109**, 160501 (2012).

[25] Nelly Huei Ying Ng, Siddarth K. Joshi, Chia Chen Ming, Christian Kurtsiefer, and Stephanie Wehner. "Experimental implementation of bit commitment in the noisy-storage model". Nature Communications **3**, 1326 (2012).

[26] C. Erven, N. Ng, N. Gigov, R. Laflamme, S. Wehner, and G. Weihs. "An experimental implementation of oblivious transfer in the noisy storage model". Nature Communications **5**, 3418 (2014).

[27] Fabian Furrer, Tobias Gehring, Christian Schaffner, Christoph Pacher, Roman Schnabel, and Stephanie Wehner. "Continuous-variable protocol for oblivious transfer in the noisy-storage model". Nature Communications **9**, 1450 (2018).

[28] Prahladh Harsha, Rahul Jain, David McAllester, and Jaikumar Radhakrishnan. "The Communication Complexity of Correlation". IEEE Transactions on Information Theory **56**, 438–449 (2010).

[29] Anup Rao and Amir Yehudayoff. "Communication Complexity: And Applications". Cambridge University Press. Cambridge (2020).

[30] Cosmo Lupo and Seth Lloyd. "Quantum data locking for high-rate private communication". New Journal of Physics **17**, 033022 (2015).

[31] Jonathan Katz and Yehuda Lindell. "Introduction to Modern Cryptography". Chapman & Hall/CRC. (2014). 2 edition.

[32] Renato Renner. "Security of quantum key distribution". International Journal of Quantum Information **06**, 1–127 (2008).

[33] Gilles Brassard and Louis Salvail. "Secret-Key Reconciliation by Public Discussion". In Tor Helleseth, editor, Advances in Cryptology — EUROCRYPT '93. Pages 410–423. Lecture Notes in Computer ScienceBerlin, Heidelberg (1994). Springer.

[34] C. H. Bennett, G. Brassard, C. Crépeau, and U. Maurer. "Generalized privacy amplification". IEEE Trans. Inf. Theory (1995).

[35] Norbert Lütkenhaus and Mika Jahma. "Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack". New Journal of Physics **4**, 44 (2002).

[36] Igor Devetak and Andreas Winter. "Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum states. Proc. R. Soc. Lond. A 461, 207-235". Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences**461** (2003).

[37] Deepthi Gopal and Stephanie Wehner. "Using post-measurement information in state discrimination". Physical Review A **82**, 022326 (2010). arxiv:1003.0716.

[38] Hoi-Kwong Lo, Xiongfeng Ma, and Kai Chen. "Decoy State Quantum Key Distribution". Physical Review Letters **94**, 230504 (2005).

[39] Wei Li, Likang Zhang, Hao Tan, Yichen Lu, Sheng-Kai Liao, Jia Huang, Hao Li, Zhen Wang, Hao-Kun Mao, Bingze Yan, Qiong Li, Yang Liu, Qiang Zhang, Cheng-Zhi Peng, Lixing You, Feihu Xu, and Jian-Wei Pan. "High-rate quantum key distribution exceeding 110 Mb s–1". Nature Photonics **17**, 416–421 (2023).

A Derivation of Theorem 2.1

For the sake of completeness, in this section we show how to derive Theorem 2.1, which is an analog result to Corrollary 7.7 in [29] with a concrete constant. First we need to define a one-way compression scheme to transmit integers in an optimal way.

Lemma A.1 (Compression scheme)**.** *Let z be an integer. There exists a one-way protocol that allows Alice to communicate z to Bob using at most* $\log(z) + 1.262\log(\log(z)) + 6.3$ *bits.*

Proof. The protocol consists of two phases. In the first phase Alice sends $y := \lceil \log(z) \rceil$ in base 3 using the two-bit letters $00, 01, 10$. Alice then sends the bits 11 to indicate to Bob that the first phase is complete. In the second phase Alice sends the binary representation of z to Bob. Note that because Bob knows $\lceil \log(z) \rceil$, he knows when the protocol stops.

In the first phase of the protocol Alice sends $\lceil \log_3(\lceil \log(z) \rceil) \rceil$ two-bit letters plus an addition two bits to complete the phase. Thus the total number of bits can be bounded as

$$\begin{aligned}
&2\lceil \log_3(\lceil \log(z) \rceil) \rceil + 2 \leq 2\log_3(\lceil \log(z) \rceil) + 4 \\
=&2\log_3(2)\log(\lceil \log(z) \rceil) + 4 \leq 2 \cdot 0.631 \cdot \log(\lceil \log(z) \rceil) + 4 \\
=&1.262\log(\lceil \log(z) \rceil) + 4 \leq 1.262\log(\log(z) + 1) + 4 \\
\leq&1.262\log(\log(z)) + 5.3\,,
\end{aligned}$$

where in the last inequality we used the fact that $\log(x+1) \leq \log(x) + 1$ for $x \geq 1$. In the second step Alice only needs to send $\lceil \log(z) \rceil \leq \log(z) + 1$ bits. By combining the upper bounds we obtain the claimed result. □

Then, we can use Claim 7.9 of [29], and replace the Claim 7.8 by our Lemma A.1 to complete the derivation.

B Practical quantum protocol

In this section, we analyze a practical quantum protocol for the βPM problem. Alice sends m copies of the quantum state $|\psi_x\rangle$ in Eq. (8) to Bob. Bob performs a measurement form the ideal protocol where there are three possible outcomes: he aborts the protocol with probability $P(\text{abort})$ if the measurement result is inconclusive ($b = \perp$), otherwise, he outputs $b = a$ with probability $(1 - P(\text{abort}))(1 - \text{QBER})$ or $b \neq a$ with probability $(1 - P(\text{abort}))\text{QBER}$.

Given a dimension n and a number of copies m, the physical implementation of the protocol determines the QBER and the abort probability $P(\text{abort})$. In the following we will analyze these quantities for a physical implementation based on photonics, where each copy of the quantum state is encoded in a photon with n optical modes, and where Bob's outcome decision-making process relies on detecting photons using two detectors.

B.1 QBER and P(abort) derivation

Consider a lossy channel, with T the transmittance of the channel, defined as $T = 10^{-0.02L}$, where L is the length of the quantum channel expressed in kilometers. Let η_{det} be the detector efficiency and P_{dark} the dark-count probability per detector. We will assume that the error rate is dominated by dark counts and that clicks due to signals and due to dark counts are independent. In this analysis we will not consider photon counting

detectors. Now let us consider the probability of a photon sent by Alice being detected: it will be transmitted with probability T due to loss in the transmission channel; once it has successfully reached Bob's measurement apparatus, there is a probability 2β of addressing one of the modes described by the partial matching; finally, once it is rerouted to one of the two detectors, it will be detected only with probability η_{det}. Combining all these steps, the final probability for a photon to be detected is $\tilde{T} \coloneqq 2\beta\eta_{det}T$. Since each photon is independent, the probability that there is at least one click due to the signal is $P_s = 1 - (1 - \tilde{T})^m$. Moreover, the probability of getting zero clicks is the probability of having at the same time no clicks from dark counts and no clicks due to the actual signal, i.e. $(1 - P_{dark})^2(1 - P_s)$. On the other hand, the probability of getting a click in both detectors at the same time is $P_{dark}^2 + P_{dark}(1 - P_{dark})P_s$. We now assume that Bob aborts the protocol every time he has 0 clicks or clicks in both detectors, obtaining

$$P(\text{abort}) = P_{dark} + (1 - 3P_{dark} + 2P_{dark}^2)(1 - \tilde{T})^m \ . \tag{15}$$

Now we have that the QBER is the probability of giving a wrong answer after the sifting, i.e.

$$\text{QBER} = \frac{P(B \neq A \wedge B \neq \perp)}{1 - P(\text{abort})} \ , \tag{16}$$

with $P(B \neq A \wedge B \neq \perp) = P_{dark}(1 - P_{dark})(1 - P_s)$, obtaining eventually by direct calculation

$$\text{QBER} = \frac{P_{dark} - P_{dark}^2}{1 - P_{dark} - (1 - 3P_{dark} + 2P_{dark}^2)(1 - \tilde{T})^m}(1 - \tilde{T})^m \ . \tag{17}$$

Finally, we have evaluated the P(abort)[4] and QBER as a function of the number of copies sent m.

C Derivation of Theorem 2.2

In [4] the authors prove that, given $\beta \in (0, 1/4]$[5] and $\epsilon_1 \in (0, 1/2)$, for any deterministic protocol π for the β-partial Matching Problem that has a communication cost at most $\gamma\epsilon_1\sqrt{n/\beta} + \log(\epsilon_1)$, with γ a positive constant which we will determine afterwards, the probability of success with respect to the distribution μ is upper bounded by $\frac{1}{2} + \frac{5}{2}\sqrt{\epsilon_1}$. To make the correspondance with Theorem 2, we can write ϵ_1 in terms of the error probability ϵ by noticing that $1 - \epsilon \leq \frac{1}{2} + \frac{5}{2}\sqrt{\epsilon_1}$. This in fact implies $\epsilon_1 \geq \frac{4}{25}\left(\frac{1}{2} - \epsilon\right)^2$. By definition of the distributional complexity we can therefore obtain Theorem 2, where all we need now is to retrieve the desired upper bound for γ.

C.1 About γ

Still from [4], in their analysis they require the value of γ to be small enough to satisfy the following inequalities:

[4] One can notice that even in the case where Alice is sending a large number of copies $P(\text{abort})$ converges to P_{dark} instead of simply 0. This is due to the fact that we didn't considered an implementation with photon counting detectors.

[5] Note that in this work we have used the notation β in place of the α from [4].

$$\frac{\epsilon_1^2}{2} \geq \sum_{\text{even } k=2}^{4c-2} \left(\frac{64e\gamma^2\epsilon_1^2}{k}\right)^{k/2} \tag{18}$$

$$\frac{\epsilon_1^2}{2} \geq \left(8\sqrt{2}e\gamma\epsilon_1\sqrt{\frac{\beta}{n}}\right)^{2c}, \tag{19}$$

with $c \geq 1$. First, let's prove that the bound $\gamma \leq \frac{1}{8e}$ implies Eq. (18). We notice that $\gamma \leq \frac{1}{8e} \leq \sqrt{\frac{1}{96e}}$, resulting in $96e\gamma^2 \leq 1$. Then we obtain the following bound for $\frac{\epsilon_1^2}{2}$:

$$\begin{aligned}
\frac{\epsilon_1^2}{2} &\geq \frac{96e\gamma^2\epsilon_1^2}{2} && \text{(From } 1 \geq 96e\gamma^2\text{)} \\
&\geq \frac{32e\gamma^2\epsilon_1^2}{1-32e\gamma^2} && \text{(Using } 2 \leq 3 - 96e\gamma^2\text{)} \\
&\geq \sum_{k=1}^{\infty}\left(32e\gamma^2\right)^k\epsilon_1^2 && \text{(Given } \sum_{k=1}^{\infty} x^k = \frac{x}{1-x}\text{)} \\
&\geq \sum_{k=1}^{\infty}\left(32e\gamma^2\epsilon_1^2\right)^k && \text{(From } \epsilon_1 < 1\text{)} \\
&\geq \sum_{\text{even } k=2}^{\infty}\left(\frac{64e\gamma^2\epsilon_1^2}{k}\right)^{k/2} && \text{(Using } k > 1\text{)} \\
&\geq \sum_{\text{even } k=2}^{4c-2}\left(\frac{64e\gamma^2\epsilon_1^2}{k}\right)^{k/2}. && \text{(Truncating the sum).}
\end{aligned}$$

To conclude, we demonstrate that $\gamma \leq \frac{1}{8e}$ implies (19). First, we notice that we can rewrite the bound as $\frac{1}{2} \geq \left(4\sqrt{2}e\gamma\right)^2$. Then, as before, we derive the desired upper bound for $\frac{\epsilon_1^2}{2}$:

$$\begin{aligned}
\frac{\epsilon_1^2}{2} &\geq \left(8\sqrt{2}e\gamma\epsilon_1\frac{1}{2}\right)^2 && \text{(From } \frac{1}{2} \geq \left(4\sqrt{2}e\gamma\right)^2\text{)} \\
&\geq \left(8\sqrt{2}e\gamma\epsilon_1\sqrt{\frac{\beta}{n}}\right)^2 && \text{(Using } \epsilon_1 < \frac{1}{2}\text{)} \\
&\geq \left(8\sqrt{2}e\gamma\epsilon_1\sqrt{\frac{\beta}{n}}\right)^{2c}, && \text{(Given } c \geq 1 \text{ and } \beta/n \leq \frac{1}{4}\text{)}.
\end{aligned}$$

D Best-known classical protocol

In this section we analyze the best-known classical protocol for the βPM problem, which has already been sketched in [4].

Classical protocol π_{BKP}: Alice and Bob can exploit their public randomness to agree on a subset $\boldsymbol{s} \coloneqq \{j_1, \ldots, j_d\} \in \mathcal{S}$, where $\mathcal{S}$ is the set of all the possible subsets of d indices in $[n]$. Subsequently, Alice transmits the corresponding bit values $x_{\boldsymbol{s}} \coloneqq (x_{j_1}, x_{j_2}, \ldots x_{j_d})$ to Bob. As such, the communication cost of this protocol is d. Consequently, in this protocol, Bob

receives the corresponding $\frac{d(d-1)}{2}$ edges[6]. We call $\sigma(\boldsymbol{s})$ the set of all those edges. Finally, Bob, by knowing ω, can give the right answer whenever he gets at least an edge in the matching M and randomly guesses the bit otherwise.

From our analysis, we find an upper bound of the error probability:

Theorem D.1. *Let d be an integer. An explicit one-way public-coin protocol π_{BKP} exists with a communication cost $CC(\pi_{BKP}) = d$ which solves the n-dimensional βPM protocol with an error probability for any input at most*[7]

$$\epsilon_{BKP}(d) = \sum_{k=0}^{d} \frac{\binom{2\beta n}{k}\binom{n-2\beta n}{d-k}}{2\binom{n}{d}} e^{-\frac{k(k-1)}{4\beta n}} \ . \tag{20}$$

Proof. First, we define $\boldsymbol{s}_M$ as the list of all the vertices in the β-matching M. For example, let $n = 4$ and M be a perfect matching (i.e. $\beta = 1/2$) such that $M = \{(1,2),(3,4)\}$, then $\boldsymbol{s}_M = \{1,2,3,4\}$. We call d_M the number of indices in $\boldsymbol{s}$ that are part of $\boldsymbol{s}_M$, i.e. $d_M \coloneqq |\boldsymbol{s} \cap \boldsymbol{s}_M|$. One can evaluate probability distribution of d_M:

$$P(d_M = k) = \frac{\binom{2\beta n}{k}\binom{n-2\beta n}{d-k}}{\binom{n}{d}} \ , \tag{21}$$

where $\binom{n}{d}$ is the number of ways to pick d indices in $[n]$, $\binom{2\beta n}{k}$ is the number of ways to pick k indices which are part of a β-matching $\boldsymbol{s}_M$ and $\binom{n-2\beta n}{d-k}$ is instead the number of ways to pick $d-k$ indices which are not part of a β-matching M.

We now want to evaluate the probability of Bob not receiving any edge which is part of his β-matching for a known value of d_M. Trivially, whenever Bob doesn't receive any index in $\boldsymbol{s}_M$ then the probability of not receiving any edge which is part of M, i.e. $d_M = 0$, is always equal to 1, otherwise we have

$$\begin{aligned} P(\nexists (i,j) \in \sigma(\boldsymbol{s}) \text{ s.t. } (i,j) \in M | d_M = k) &= \prod_{l=1}^{k} \Big(\frac{2\beta n - 2(l-1)}{2\beta n - (l-1)} \Big) \\ &= \prod_{l'=0}^{k-1} \Big(1 - \frac{l'}{2\beta n - l'} \Big) \\ &\leq \prod_{l'=0}^{k-1} \Big(1 - \frac{l'}{2\beta n} \Big) \\ &\leq e^{-\sum_{l'=0}^{k-1} \frac{l'}{2\beta n}} \\ &\leq e^{-\frac{k(k-1)}{4\beta n}} \ , \end{aligned} \tag{22}$$

where in the first line we used that, after having checked that the first $l-1$ indices in $\boldsymbol{s}_{d_M}$ do not form any edge in M, $2\beta n - 2(l-1)$ is the remaining number of possible indices in $\boldsymbol{s}_M$ that won't form an edge in M when paired with the indices in the already extracted list $\{j'_1, \dots j'_{l-1}\}$, and $2\beta n - (l-1)$ is the total number of remaining indices in $\boldsymbol{s}_M$. In the second line we have simply replaced l with $l' \coloneqq l - 1$. The third line is obtained by noticing that $\frac{a}{x-a} > \frac{a}{x}$ for any x, $a > 0$ with $x > a$. The fourth and fifth lines come from $1 - x < e^{-x}$ and $\sum_{i=0}^{k-1} i = k(k-1)/2$ respectively.

[6] Whenever we say that Bob receives an edge, say (j_1, j_2), it implies that he acquires the bit values assigned to the corresponding vertices, i.e. (x_{j_1}, x_{j_2}).

[7] Note that in (20) we considered $\binom{a}{b} = 0$ whenever $b > a$.

Finally, since Bob, by knowing ω, can give the right answer whenever he gets at least an edge in the matching M and randomly guesses the bit otherwise, the error probability for the best-known protocol is at most

$$\begin{aligned}
&\frac{1}{2}\sum_{k=0}^{d} P(d_M = k) P(\nexists (i,j) \in \sigma(\boldsymbol{s}) \text{ s.t. } (i,j) \in M | d_M = k) \\
&\qquad \leq \frac{1}{2}\sum_{k=0}^{d} P(d_M = k) e^{-\frac{k(k-1)}{4\beta n}} \\
&\qquad \leq \sum_{k=0}^{d} \frac{\binom{2\beta n}{k}\binom{n-2\beta n}{d-k}}{2\binom{n}{d}} e^{-\frac{k(k-1)}{4\beta n}} \ .
\end{aligned}$$

where in the second line we used the fact that d_M cannot be larger than d, Eq. (22) in the third line and (21) in the last line. □

E Proof of Theorem 3.2

We first prove an useful lemma:

Lemma E.1. *$\forall \epsilon \in (0, \frac{1}{2})$, $\forall \delta_2 \in (0, \frac{1}{2} - \epsilon)$ if an encoding attack with $P_{guess}(A|YZ\Phi_{t_{comp}}(Q_{in})) \geq 1 - \epsilon + \delta$ exists, then Alice must have sent m copies of the quantum state (8), with*

$$m \geq \frac{\delta_2 (\frac{1}{50e\sqrt{\beta}} \left(\frac{1}{2} - \epsilon - \delta_2\right)^2 \sqrt{n} + 2\log\left(\frac{1}{2} - \epsilon - \delta_2\right)) - \log(\frac{5}{2})\delta_2 - 6}{\lceil \log(n) \rceil} \ .$$

Proof. Let $\epsilon \in (0, \frac{1}{2})$, $\delta_2 \in (0, \frac{1}{2} - \epsilon)$. Let us suppose there exists an encoding attack with $P_{\text{guess}}(A|YZ\Phi_{t_{comp}}(Q_{\text{in}})) \geq 1 - \epsilon + \delta$. First, by using Theorem 3.1, we deduce $\max_{\mathcal{Z}} P_{\text{guess}}(A|Y\mathcal{Z}(Q)) \geq 1 - \epsilon$. Then we use Lemma 3.1 to deduce $m \geq \frac{IC^1_\mu(\beta PM, \epsilon)}{\lceil \log(n) \rceil}$. Furthermore, from Lemma 2.1 we obtain $m \geq \frac{\frac{\delta_2}{2} D^1_\mu(f, \epsilon + \delta_2) - 6}{\lceil \log(n) \rceil}$. Finally, we conclude the proof by showing that from Theorem 2.2 we have

$$m \geq \frac{\frac{\delta_2}{2}\left(k(\epsilon + \delta_2)\sqrt{n} + d(\epsilon + \delta_2)\right) - 6}{\lceil \log(n) \rceil} \ ,$$

with k and d defined in (7).

□

Now we are ready to prove Theorem 3.2. Let x be equal to $\frac{1}{2} - \epsilon$ and $\delta_2 := \frac{x}{2}$. By contraposition, Lemma E.1 implies that for any encoding attack acting on m copies, with

$$m = \frac{\frac{1}{50e\sqrt{\beta}} \left(\frac{x}{2}\right)^3 \sqrt{n} - \ln(4) - 6 - (\log(\frac{5}{2}) - \ln(4))\frac{x}{2}}{\lceil \log(n) \rceil} - 1 \ , \tag{23}$$

Eve's guessing probability is bounded by $P_{\text{guess}}(A|YZ\Phi_{t_{comp}}(Q_{\text{in}})) < \frac{1}{2} + x + \delta$. We now have to find the real zero of Eq. (23) by using Cardan's method. We first rewrite (23) in in the canonical form

$$z^3 + pz + q = 0 \ , \tag{24}$$

where

$$z = \frac{x}{2}\ , \quad q = \frac{-50}{\sqrt{n}} e\sqrt{\beta}((m+1)\lceil \log(n) \rceil + \ln(4) + 6)\ ,$$
$$p = \frac{-50}{\sqrt{n}} e\sqrt{\beta}\Big(\log\left(\frac{5}{2}\right) - \ln(4)\Big)\ .$$

We now notice that $q < 0$ and, since $\left(\log\left(\frac{5}{2}\right) - \ln(4)\right) < 0$, that $p > 0$. This means that $\Delta \coloneqq -(4p^3 + 27q^2)$ is negative. Therefore, thanks to Cardan's method, the zero of equation (24) expressed in the variable x is:

$$x = 2^{1-\frac{1}{3}}\left(\sqrt[3]{-q + \sqrt{\frac{-\Delta}{27}}} + \sqrt[3]{-q - \sqrt{\frac{-\Delta}{27}}}\right)\ . \tag{25}$$

From Eq. (25), noting the negative second term with $\sqrt[3]{\cdot}$ and the fact that $\sqrt[d]{\cdot}$ is subadditive for any integer d, we deduce that

$$P_{\text{guess}}(A|YZ\Phi_{t_{comp}}(Q_{\text{in}})) \leq \frac{1}{2} + 2\left(\sqrt[3]{-q} + \sqrt{\frac{p}{3}}\right) + \delta\ .$$