Bit-string oblivious transfer based on quantum state computational distinguishability

A. Souto
a.souto@math.ist.utl.pt

P. Mateus
pmat@math.ist.utl.pt

P. Adão
pedro.adao@ist.utl.pt

N. Paunković
npaunkovic@math.ist.utl.pt

SQIG - Instituto de Telecominicações
Instituto Superior Técnico, Universidade de Lisboa

Abstract

Oblivious transfer protocol is a basic building block in cryptography and is used to transfer information from a sender to a receiver in such a way that, at the end of the protocol, the sender does not know if the receiver got the message or not.

Since Shor's quantum algorithm appeared, the security of most of classical cryptographic schemes has been compromised, as they rely on the fact that factoring is unfeasible. To overcome this, quantum mechanics has been used intensively in the past decades, and alternatives resistant to quantum attacks have been developed in order to fulfill the (potential) lack of security of a significant number of classical schemes.

In this paper, we present a quantum computationally secure protocol for bit-string oblivious transfer between two parties, under the assumption of quantum hardness of state distinguishability and the constraint of performing at most few-qubit measurements (leaving open the question of general attacks performed on all qubits involved). The protocol is feasible, in the sense that it is implementable in polynomial time.

1 Introduction

An *oblivious transfer* protocol involves two parties, a sender (Alice) and a receiver (Bob). It consists of two phases: the transferring phase and the opening phase. The goal of the sender is to send a message (in general, a bit-string)

during the transferring phase, that will not be known to the receiver until the opening phase, during which the sender reveals the message with probability 1/2. The goal of the receiver is that, upon opening the message, the sender is oblivious to the fact whether the message was successfully transferred or not. Although not explicitly stated in the original argument, it is usually assumed that the receiver knows, at the end of the protocol, if he got the correct message (see for example [12]).

In classical cryptography, the first oblivious transfer scheme was proposed by Rabin [37] and is based on the same assumptions as the RSA cryptographic system. In Rabin's scheme, the sender sends a message to the receiver that is able to decrypt it properly with probability 1/2. At the end of the protocol, the sender remains oblivious to whether or not the receiver got the correct message. Later, Even, Goldreich, and Lempel [15] formally presented the idea of *1-out-of-2 oblivious transfer*. In 1-out-of-2 oblivious transfer the sender has two messages to send such that: the receiver gets only one of the two with equal probability; the sender is oblivious to which message was received. It is clear that from a 1-out-of-2 oblivious transfer protocol, by choosing one of the message at random, it is possible to construct an oblivious transfer protocol. Furthermore, it is possible to reduce 1-out-of-2 oblivious transfer protocol, where the message is a bit-string, to a single-bit 1-out-of-2 oblivious transfer protocol, first shown in [6] (see also [13, 7]). Finally, Crépeau showed that Rabin's oblivious transfer is equivalent to 1-out-of-2 oblivious transfer [12]). This way, a single-bit oblivious transfer becomes a cryptographic primitive for all different flavors of oblivious transfer protocols, in *classical setting*. Moreover, oblivious transfer is a particularly important primitive as from $O(n)$ instances of a 1-out-of-2 oblivious transfer protocol one can construct a bit-commitment scheme, using the technique presented in [4].

In the last decades quantum computation has played a crucial role in the development of cryptographic analysis. The breakthrough of quantum computation in the realm of cryptography is due to Shor's factoring algorithm [41]. This algorithm compromises the security of most common public key cryptographic schemes as factoring becomes feasible with a quantum computer. Since today's technology is evolving to be able to deal with a larger number of qubits, a possibility of having affordable and reliable quantum computers in the future arises, compromising the secrecy of communications and transactions.

The first results in the field of quantum cryptography were made already back in 1969 by Wiesner, when he introduced the notions of quantum multiplexing and quantum money. The former was essentially a 1-out-of-2 oblivious transfer protocol which was introduced more than a decade later [15] within

the scope of classical cryptography. Unfortunately, his ideas remained largely unknown to the general scientific community as he managed to publish his work only in 1983 [44]. Subsequently, based on similar ideas to those of Wiesner, Bennet and Brassard developed their famous BB84 cryptographic protocol for key distribution [3] , which was shown to be unconditionally secure [29, 42, 34, 39], in contrast to only computationally secure classical cryptography.

Following the success of quantum cryptography, a significant effort was put in developing other quantum security protocols that would outperform their classical counterparts. Unfortunately, a number of no-go results showed the impossibility of having some of important security primitives unconditionally secure even in the quantum setting (nevertheless some, such as quantum contract signing, have been shown to be unconditionally secure [36]). First, Lo and Chau [27, 30], and independently Mayers [33], showed the impossibility of designing an unconditionally secure quantum bit commitment protocol, unless relativistic effects are used (see [20, 22, 5]). This resulted in the development of various practically secure quantum bit commitment protocols using noisy and bounded memories [43, 40, 24, 35, 5, 31].

Subsequently, Lo showed the same no-go result for a broad class of two-party security protocols, called "one-sided two-party computations" [28]. As an immediate corollary to this result follows the impossibility of an unconditionally secure quantum 1-out-of-2 oblivious transfer, in particular transfer of single bits. Note that in the classical setting, due to the above mentioned reduction of a bit commitment to a 1-out-of-2 oblivious transfer, the impossibility of having a secure bit commitment would imply the impossibility of having a secure single-bit 1-out-of-2 oblivious transfer as well. In the quantum realm the situation is more subtle and complicated, and classical reductions may not be valid anymore.

Namely, classical reduction schemes are typically based on a number of executions of one ("more basic") protocol, to achieve another ("more complex") one, where the "simpler" protocol is treated as a black box. In quantum mechanics such assumption is generally not valid, as the parties involved in the protocol are in principle allowed to perform joint measurements on different "black boxes", thus compromising the classical reduction schemes. Indeed, although secure quantum single-bit 1-out-of-2 oblivious transfer was shown to be impossible, a secure quantum single-bit oblivious transfer is possible [18]. This result showed that the two "flavors" of oblivious transfer protocols are no longer equivalent in quantum domain, as further elaborated in [17]. The reason for this is precisely in the fact that the above mentioned Crépeau's reduction scheme [12] uses many instances of oblivious transfer protocol in order to construct a 1-out-of-2 protocol, thus making it vulnerable to so-called "coherent

attacks" (joint measurements). Hence, other cryptographic protocols based on multiple usage of simpler protocols (as black boxes) have to be reanalyzed when quantum counterparts are considered. In particular, the use of oblivious transfer as a building block for more complex cryptographic protocols [6, 23, 16, 32, 11], and in designing secure multiparty computation schemes, as suggested in recent papers [25, 26]. A possible approach towards rigorous security framework for complex protocols based on the above mentioned primitives could be taken along the lines presented in [2, 38], where the so-called universal composability of quantum key distribution-based schemes was considered.

Further, Kent showed that, although unconditionally secure quantum bit commitment in not possible, a secure quantum bit-string protocol is [21], thus showing explicitly the insecurity of classical reduction schemes from a single-bit to a bit-string protocols (see also a discussion on a slightly different version of a bit-string commitment [8], as well as a quantum bit-string generation protocol [1]). Thus, although there exists an unconditionally secure quantum single-bit oblivious transfer, a question of a quantum bit-string counterpart stays open.

In this paper we present a polynomial time quantum bit-string oblivious transfer protocol based on a presumed polynomial hard problem even for a quantum computer,[1] the *Quantum State Computational Distinguishability with Fully Flipped Permutations*, denoted by $\mathbb{QSCD}_{ff}$, presented in [19]. We prove the protocol's security against at most few-qubit coherent attacks, leaving open the question of most general multi-qubit measurements. To our best knowledge, this is the first proposal of a concrete quantum realization of a bit-string oblivious transfer protocol based on a presumably quantum hard problem. $\mathbb{QSCD}_{ff}$ is the standard problem of quantum state distinguishability, applied to two particular quantum states: $\otimes_{i=1}^{k(n)} \frac{1}{\sqrt{2}}(|\sigma_i\rangle + |\sigma_i \circ \pi\rangle)$ and $\otimes_{i=1}^{k(n)} \frac{1}{\sqrt{2}}(|\sigma_i\rangle - |\sigma_i \circ \pi\rangle)$, where $\sigma_i \in \mathbb{S}_n, \pi \in \mathbb{K}_n$ are permutations ($\mathbb{K}_n$ is the set of all permutation in $\mathbb{S}_n$ of order 2, such that $\pi(i) \neq i$ for all i), and k is some polynomial, such that for each state the array of σ_i-s is chosen at random. In the same paper, the authors discuss how one can explore the indistinguishability of these quantum states in the scope of cryptography and propose a cryptographic public key scheme that, under the hardness assumption of $\mathbb{QSCD}_{ff}$, is secure against polynomial quantum adversaries using π as a trapdoor.

The rest of this paper is organized as follows: in the next section we present the basic notions, problems, notation and results used in the rest of the paper. We also show the equivalence between a previously known algorithm, used in [19], and a particular orthogonal measurement that is used to prove the security

[1] A problem is polynomially hard if there is no polynomial time algorithm for solving it.

of our protocol, under the assumption that $\mathbb{QSCD}_{ff}$ is polynomially hard for quantum computers. In Section 3 we present our protocol for a bit-string oblivious transfer and analyze its correctness and security. In Section 4 we present the conclusions.

2 Preliminaries

We use a binary alphabet $\Sigma = \{0, 1\}$ and strings of length ℓ, which are elements of Σ^ℓ. The group $\mathbb{S}_n$ is the set of all permutations over the set $\{1, \ldots, n\}$, whose elements we denote by Greek letters $\sigma, \tau, \delta, \ldots$, together with the composition operation $\circ$.[2] In the rest of the paper we assume n to be of the form $2(2m+1)$, for some $m \in \mathbb{N}$.

Example 1 *Consider $n = 6$ and $\sigma \in \mathbb{S}_6$ defined as $\sigma(1) = 2, \sigma(2) = 3, \sigma(3) = 1, \sigma(4) = 5, \sigma(5) = 4$ and $\sigma(6) = 6$. We represent this permutation as $\sigma = (1\ 2\ 3)(4\ 5)$, where $(1\ 2\ 3)$ and $(4\ 5)$ represent the orbits of elements of $\{1, \ldots 6\}$. The orbit of $i \in \{1, \ldots, n\}$ with respect to σ is $(i\ \sigma(i)\ \ldots\ \sigma^j(i))$, where the superscript is the number of times σ is applied to element i, and j is the smallest integer such that $\sigma(\sigma^j(i)) = i$.*

Notice that this representation is not unique, and we can represent this same σ as $(4\ 5)(1\ 2\ 3)$ or $(5\ 4)(2\ 3\ 1)$.

Given a permutation $\sigma \in \mathbb{S}_n$, other than the identity, one can decompose it into a sequence of transpositions, *i.e.*, elementary permutations that only exchange two elements. It is easy to see that such decomposition is not unique, but the number of transpositions, denoted by $\#(\sigma)$, has always the same *parity* and hence one can define the sign of a permutation σ as $sgn(\sigma) = (-1)^{\#(\sigma)}$.

Example 2 *Consider σ as defined in Example 1. Three possible decompositions of σ in terms of transpositions (derived from the three given representations) are $(1\ 3)(1\ 2)(4\ 5)$ and $(4\ 5)(1\ 3)(1\ 2)$ and $(5\ 4)(2\ 1)(2\ 3)$, and all of them have parity 1.*

One can, in fact, show that if a permutation σ generates L orbits of elements from $\{1, \ldots, n\}$ of lengths $\ell_1, \ldots, \ell_L$ then $\#(\sigma) = \sum_{i=1}^{L}(\ell_i - 1)$. In our case, the representation of σ in Example 1 has orbits of length 3 and 2, hence $\#(\sigma) = (3-1)+(2-1) = 3$. The same σ was represented in this example with 3 orbits of length 2, hence $\#(\sigma) = 3 \times (2-1) = 3$.

[2] Formally, each permutation $\sigma \in \mathbb{S}_n$ is a bijective function over $\{1, \ldots, n\}$.

Since $|\mathbb{S}_n| = n!$ one needs $\log(n!) = \sum_{i=1}^{n} \log i \leq n \log n \in O(n \log n)$ bits to represent each $\sigma \in \mathbb{S}_n$. Note that $\mathbb{S}_n$ consists of two sets of equal size: $\mathbb{E}_n$ containing the even permutations (i.e., permutations with sign 1), and its complement $\mathbb{O}_n$ consisting of all odd permutations. Hence $\mathbb{S}_n = \mathbb{E}_n \cup \mathbb{O}_n$.

As in [19], we consider the following subset of $\mathbb{S}_n$:

$$\mathbb{K}_n = \Big\{ \pi \in \mathbb{S}_n : \pi \circ \pi = id_n \text{ and } \pi(i) \neq i, \forall i \in \{1, \cdots, n\} \Big\}.$$

Example 3 *One can see that the permutation σ of Example 1 is not in $\mathbb{K}_6$ as $\sigma \circ \sigma \neq id_n$, e.g., $\sigma \circ \sigma(1) = \sigma(2) = 3 \neq 1$. We also do not have $\sigma(i) \neq i$ for $i = 6$.*

As an example of a permutation in $\mathbb{K}_6$ we have $\pi = (1\ 2)(3\ 6)(4\ 6)$.

One can immediately see that for an even n, any permutation $\pi \in \mathbb{K}_n$ can always be decomposed into $n/2$ transpositions since each element $i \in \{1, \ldots, n\}$ has to appear in (at least) one transposition (otherwise $\pi(i) = i$), and appears only once, as $\pi^2 = id_n$. Given that we assumed $n = 2(2m + 1)$, we have that $\pi \in \mathbb{K}_n$ if and only if it can be written as an odd number of transpositions and hence $\pi \in \mathbb{O}_n$.

A counting argument revels that the size of $\mathbb{K}_n$ is:

$$|\mathbb{K}_n| = \left(\begin{array}{c} n \\ n/2 \end{array} \right) \left(\frac{n}{2}\right)! = \frac{n!}{\left(\frac{n}{2}\right)!}.$$

Let $n \in \mathbb{N}$ and $\pi \in \mathbb{K}_n$, and consider the Hilbert space $\mathcal{H}_n = span\{|\sigma\rangle : \sigma \in \mathbb{S}_n\}$, such that for all σ and σ', $\langle \sigma | \sigma' \rangle = \delta_{\sigma,\sigma'}$. Let $|\psi_\pi^\pm(\sigma)\rangle = \frac{1}{\sqrt{2}}(|\sigma\rangle \pm |\sigma \circ \pi\rangle)$. Notice that for every π the set $\{|\psi_\pi^\pm(\sigma)\rangle : \sigma \in \mathbb{E}_n\}$ is an orthonormal basis.

Indeed, we have that

$$\left\langle \psi_\pi^\pm(\sigma) | \psi_\pi^\pm(\sigma') \right\rangle = \frac{1}{2} \left(\langle \sigma | \sigma' \rangle \pm \langle \sigma | \sigma' \circ \pi \rangle \pm \langle \sigma \circ \pi | \sigma' \rangle + \langle \sigma \circ \pi | \sigma' \circ \pi \rangle \right)$$

is either 1, when $\sigma = \sigma'$, or 0 otherwise. This is because $\sigma, \sigma' \in \mathbb{E}_n$ and $\pi \in \mathbb{O}_n$, and consequently $\langle \sigma | \sigma' \circ \pi \rangle = \langle \sigma \circ \pi | \sigma' \rangle = 0$.

On the other hand

$$\left\langle \psi_\pi^\pm(\sigma) | \psi_\pi^\mp(\sigma') \right\rangle = \frac{1}{2} \left(\langle \sigma | \sigma' \rangle \mp \langle \sigma | \sigma' \circ \pi \rangle \pm \langle \sigma \circ \pi | \sigma' \rangle - \langle \sigma \circ \pi | \sigma' \circ \pi \rangle \right)$$

is always 0: when $\sigma = \sigma'$, the first and last terms cancel each other, while the other two terms are always zero. Since $|\psi_\pi^\pm(\sigma)\rangle = \pm |\psi_\pi^\pm(\sigma \circ \pi)\rangle$, the set $\{|\psi_\pi^\pm(\sigma)\rangle : \sigma \in \mathbb{O}_n\}$ is also an orthonormal basis.

Consider the following quantum states defined in [19]:

$$\begin{aligned}\rho_\pi^+ &= \frac{1}{2n!}\sum_{\sigma\in\mathbb{S}_n}(|\sigma\rangle+|\sigma\circ\pi\rangle)(\langle\sigma|+\langle\sigma\circ\pi|)\\ &= \frac{1}{n!}\sum_{\sigma\in\mathbb{S}_n}\left|\psi_\pi^+(\sigma)\right\rangle\left\langle\psi_\pi^+(\sigma)\right|\\ &= \frac{2}{n!}\sum_{\sigma\in\mathbb{E}_n}\left|\psi_\pi^+(\sigma)\right\rangle\left\langle\psi_\pi^+(\sigma)\right|\end{aligned}$$

and

$$\begin{aligned}\rho_\pi^- &= \frac{1}{2n!}\sum_{\sigma\in\mathbb{S}_n}(|\sigma\rangle-|\sigma\circ\pi\rangle)(\langle\sigma|-\langle\sigma\circ\pi|)\\ &= \frac{1}{n!}\sum_{\sigma\in\mathbb{S}_n}\left|\psi_\pi^-(\sigma)\right\rangle\left\langle\psi_\pi^-(\sigma)\right|\\ &= \frac{2}{n!}\sum_{\sigma\in\mathbb{E}_n}\left|\psi_\pi^-(\sigma)\right\rangle\left\langle\psi_\pi^-(\sigma)\right|.\end{aligned}$$

We are interested in these particular states as they are orthogonal to each other and hence fully distinguishable, *provided one knows* which π was used to prepare them. Without the knowledge of π the problem of distinguishing these states is believed to be polynomially hard even for quantum computers, as stated in [19]. First, we state the problem:

Problem 4 ($\mathbb{QSCD}_{ff}$) *The* Quantum State Computational Distinction with Fully Flipped Permutations Problem*, denoted by $\mathbb{QSCD}_{ff}$, is defined as:*

Instances *Two quantum states $(\rho_\pi^+)^{\otimes k(n)}$ and $(\rho_\pi^-)^{\otimes k(n)}$ where $n = 2(2m+1)$ for some $m \in \mathbb{N}$, and k is some fixed polynomial, i.e., each state consists of $k(n)$ copies of ρ_π^+ and ρ_π^-, respectively.*

Question *Are $(\rho_\pi^+)^{\otimes k(n)}$ and $(\rho_\pi^-)^{\otimes k(n)}$ computationally indistinguishable if π is unknown, i.e., is the probability of a quantum polynomial time algorithm to be able to distinguish between the states $(\rho_\pi^+)^{\otimes k(n)}$ and $(\rho_\pi^-)^{\otimes k(n)}$, with unknown π, a negligible function?*[3]

The problem $\mathbb{QSCD}_{ff}$ is closely related to the hidden subgroup problem over symmetric groups for which no one knows an efficient quantum algorithm

[3]Note that the Problem could be stated in a more compact way by using mixed states $\rho^\pm = \sum_{\pi\in\mathbb{K}_n}\rho_\pi^\pm/|\mathbb{K}_n|$. Then, the Question would go as follows: are ρ^+ and ρ^- computationally indistinguishable? The choice of somewhat redundant presentation, by explicitly noting that permutation π is unknown, is chosen to emphasize the role of π as a secret key in our Oblivious Transfer protocol (see Protocol 13).

to solve it. In [19] the authors reduced the $\mathbb{QSCD}_{ff}$ problem to a variant of the unique graph automorphism problem, that is also presumably hard for quantum computers with polynomial time resources, proving the following hardness result:

Theorem 5 ([19]) *If there exists a polynomial-time quantum algorithm that solves $\mathbb{QSCD}_{ff}$ with non-negligible advantage, then there exists a polynomial-time quantum algorithm that solves the graph automorphism problem in the worst case for infinitely-many input lengths.*

The interesting property that makes this problem suitable for cryptography is that it has a trapdoor that allows one to efficiently distinguish the states: one can distinguish, with certainty, $(\rho_\pi^+)^{\otimes k(n)}$ from $(\rho_\pi^-)^{\otimes k(n)}$, provided that an extra piece of information is given, in this case π. Furthermore, when using a permutation π' different from the trapdoor π, the probability of distinguishing these states is the same as plain guessing. In order to present the protocol and analyze its complexity and security, we need the following obvious proposition:

Proposition 6 *The following linear operators are unitary (for all $\sigma, \tau, \pi \in \mathbb{S}_n$):*

- $C_\circ^l = \sum_{\sigma,\tau} |\sigma, \sigma \circ \tau\rangle\langle\sigma, \tau|$;
- $C_\circ^r = \sum_{\sigma,\tau} |\sigma, \tau \circ \sigma\rangle\langle\sigma, \tau|$;
- $C_\pi = |0\rangle\langle 0| \otimes \sum_\sigma |\sigma\rangle\langle\sigma| + |1\rangle\langle 1| \otimes \sum_\sigma |\sigma \circ \pi\rangle\langle\sigma|$;
- $C_1 = \mathbb{1}_2 \otimes \sum_{\sigma \neq \pi} |\sigma\rangle\langle\sigma| + (|1\rangle\langle 0| + |0\rangle\langle 1|) \otimes |\pi\rangle\langle\pi|$;
- $C_{swap} = \sum_{\sigma,\tau} |\tau, \sigma\rangle\langle\sigma, \tau|$;
- $C_{sgn} = \sum_\sigma (-1)^{sgn(\sigma)} |\sigma\rangle\langle\sigma|$.

It is easy to see by explicit calculation that each operator C from the above proposition satisfies the unitarity condition $CC^\dagger = C^\dagger C = \mathbb{1}$ (here, as well as in the rest of the paper, $\mathbb{1}$ is the identity operator in the corresponding space).

The first two operations, $C_\circ^l$ and $C_\circ^r$, leave the state of the first register unchanged, while the state of the second is transformed into the state given by

the "left" and the "right" composition of the two permutations, respectively. Controlled operation C_π composes the second-register permutation with π from the right, while C_1 inverts the basis states $|0\rangle$ and $|1\rangle$ of the first register if the second is in the state $|\pi\rangle$ (both operations are defined for an arbitrary permutation, but in the paper we will constrain to cases $\pi \in \mathbb{K}_n$). Finally, C_{swap} swaps the states of the two registers, while C_{sgn} changes the sign in front of the basis vectors $|\sigma\rangle$.

The quantum algorithm presented in [19], Algorithm 7, justifies that given the private key π one can produce the states $(\rho_\pi^+)^{\otimes k(n)}$ in *polynomial time* using only Hadamard H and the operations defined in Proposition 6.

Algorithm 7 (to generate $(\rho_\pi^+)^{\otimes k(n)}$ [19]) *For the sake of simplicity of the presentation we consider a fixed n and the case where $k(n) = 1$. The reader can easily generalize the argument for $k(n)$ systems.*

Input $\pi \in \mathbb{K}_n$.

Output $\rho_\pi^+ = \dfrac{2}{n!} \displaystyle\sum_{\sigma \in \mathbb{E}_n} (|\sigma\rangle + |\sigma \circ \pi\rangle)(\langle\sigma| + \langle\sigma \circ \pi|)$.

Step 1. *Select a random $\sigma \in \mathbb{S}_n$ and prepare the initial state* $|0\rangle \otimes |id_n\rangle \otimes |\sigma\rangle \in \mathbb{C}^2 \otimes \mathbb{C}^{n \log n} \otimes \mathbb{C}^{n \log n}$.

Step 2. *Apply* $H \otimes \mathbb{1} \otimes \mathbb{1}$.

Step 3. *Apply* $C_\pi \otimes \mathbb{1}$.

Step 4. *Apply* $C_1 \otimes \mathbb{1}$.

Step 5. *Apply* $\mathbb{1} \otimes C_{swap}$.

Step 6. *Apply* $\mathbb{1} \otimes C_\circ^r$.

The third register is now in the state $|\psi_\pi^+(\sigma)\rangle = \frac{1}{\sqrt{2}}(|\sigma\rangle + |\sigma \circ \pi\rangle)$. *Since σ is chosen at random, the ensemble of such systems is represented by the mixed state ρ_π^+.*

Note that it is possible to prepare the state ρ_π^+ as a partial trace of an entangled state. In order to do that, one should start from $|0\rangle|id_n\rangle \frac{1}{\sqrt{n!}} \sum_{\sigma \in \mathbb{S}_n} |\sigma\rangle$. Upon applying Steps 1 to 6 of the previous algorithm the overall state becomes $|0\rangle \frac{1}{\sqrt{n!}} \sum_{\sigma \in \mathbb{S}_n} |\sigma\rangle \frac{1}{\sqrt{2}}(|\sigma\rangle + |\sigma \circ \pi\rangle)$ and the third register is again in the state ρ_π^+.

In the next lemma we show that one can easily transform ρ_π^+ into ρ_π^-, and vice versa, without knowing π. This property follows immediately from the fact that π is an odd permutation.

Lemma 8 ([19]) *There exists a* polynomial-time *quantum algorithm (in fact C_{sgn}) that, with probability* 1*, transforms ρ_π^+ into ρ_π^- and keeps completely mixed state $\rho_{\mathbb{1}} = \frac{1}{n!}\sum_{\sigma\in\mathbb{S}_n}|\sigma\rangle\langle\sigma|$ invariant, for any $n = 2(2m+1)$, with $m \in \mathbb{N}$, and any permutation $\pi \in \mathbb{K}_n$.*

Indeed, for a pure $|\psi_\pi^+(\sigma)\rangle$, with $\pi \in \mathbb{K}_n$, by applying C_{sgn} we get:

$$\begin{array}{rcl} |\psi_\pi^+(\sigma)\rangle & = & \dfrac{|\sigma\rangle + |\sigma\circ\pi\rangle}{\sqrt{2}} \\ & \stackrel{C_{sgn}}{\longrightarrow} & \dfrac{(-1)^{sgn(\sigma)}|\sigma\rangle + (-1)^{sgn(\sigma)+1}|\sigma\circ\pi\rangle}{\sqrt{2}} \\ & = & (-1)^{sgn(\sigma)}|\psi_\pi^-(\sigma)\rangle. \end{array}$$

Notice that determining the sign of a permutation is a computation that can be done in polynomial time. Furthermore, it is easy to see that this algorithm leaves $\rho_{\mathbb{1}}$ invariant.

The following algorithm explores the trapdoor property of $\mathbb{QSCD}_{ff}$: given π, one can distinguish in *polynomial time* and with probability 1 the quantum states $(\rho_\pi^+)^{\otimes k(n)}$ and $(\rho_\pi^-)^{\otimes k(n)}$ (see [19] for the details of the proof).

Algorithm 9 (distinguishing $(\rho_\pi^+)^{\otimes k(n)}$ from $(\rho_\pi^-)^{\otimes k(n)}$) *For the sake of simplicity of the presentation we consider a fixed n and the case where $k(n) = 1$. The reader can easily generalize the argument for $k(n)$ systems.*

Input $\pi \in \mathbb{K}_n$ *and a quantum state χ_π that is either ρ_π^+ or ρ_π^-.*

Output 0 *if $\chi_\pi = \rho_\pi^+$, and* 1 *if $\chi_\pi = \rho_\pi^-$.*

Step 1. *Prepare the system in the state $|0\rangle\langle 0| \otimes \chi_\pi$, where $|0\rangle \in \mathbb{C}^2$.*

Step 2. *Apply $H \otimes \mathbb{1}$.*

Step 3. *Apply C_π.*

Step 4. *Apply again $H \otimes \mathbb{1}$.*

Step 5. *Measure $M_+ = (0\cdot|0\rangle\langle 0| + 1\cdot|1\rangle\langle 1|) \otimes \mathbb{1}$ and output the result.*

After performing the second step the obtained state is $\frac{1}{2}|+\rangle\langle+| \otimes \chi_\pi$, with $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$. Since $C_\pi(|+\rangle(|\sigma\rangle \pm |\sigma\circ\pi\rangle)) = |\pm\rangle(|\sigma\rangle \pm |\sigma\circ\pi\rangle)$, the overall state after the third step is $|\pm\rangle\langle\pm| \otimes \rho_\pi^\pm$. So, by applying Hadamard on the first register and measuring it in the computational basis we get the desired outcome.

We have shown that the above algorithm is able to distinguish with certainty between $\chi_\pi = (\rho_\pi^+)^{\otimes k(n)}$ and $\chi_\pi = (\rho_\pi^-)^{\otimes k(n)}$, using only polynomial quantum

resources, provided that we use the correct π. We will show later that if $\chi_{\pi'}$ is created with a different permutation $\pi' \neq \pi$, then the answer will be a random variable with distribution close to uniform (see Theorem 14 for details).

Algorithm 9 provides a computational approach to the problem of distinguishing the two states and is suitable for defining the public key scheme presented in [19]. In our work, due to the nature of the problem at hand, we will instead consider measurements. We will show next that the result of Algorithm 9 is equivalent to measuring the orthogonal observable

$$M_\pi = 0 \cdot P_\pi^+ + 1 \cdot P_\pi^-$$

where

$$\begin{aligned} P_\pi^\pm &= \sum_{\sigma \in \mathbb{E}_n} \left|\psi_\pi^\pm(\sigma)\right\rangle\left\langle\psi_\pi^\pm(\sigma)\right| \\ &= \frac{1}{2}\sum_{\sigma \in \mathbb{E}_n} (|\sigma\rangle \pm |\sigma \circ \pi\rangle)(\langle\sigma| \pm \langle\sigma \circ \pi|). \end{aligned}$$

Proposition 10 *Applying Algorithm 9 with π and measuring $M_\pi = 0 \cdot P_\pi^+ + 1 \cdot P_\pi^-$ are equivalent processes: the probability distribution of the outcomes of the Algorithm 9 is the same as the probability distribution of the outcomes of the measurement M_π, and the resulting states are the same.*

As in Algorithm 9, we consider a fixed n and the case where $k(n) = 1$. The reader can easily generalize the argument for $k(n)$ systems using $M_\pi^{\otimes k(n)}$ instead of M_π.

Proof: In order to prove this proposition, first notice that by the linearity of the measurement, it is enough to show the result only for the case of a general pure $|\psi\rangle$. Since for every π the set $\{|\psi_\pi^\pm(\sigma)\rangle : \sigma \in \mathbb{E}_n\}$ is a basis, we can write

$$|\psi\rangle = \sum_{\sigma \in \mathbb{E}_n} \left(c_\sigma^+ \left|\psi_\pi^+(\sigma)\right\rangle + c_\sigma^- \left|\psi_\pi^-(\sigma)\right\rangle\right).$$

We first compute the following:

$$\begin{aligned} &P_\pi^\pm|\psi\rangle \\ =&\sum_{\sigma \in \mathbb{E}_n} \left|\psi_\pi^\pm(\sigma)\right\rangle\left\langle\psi_\pi^\pm(\sigma)\right|\left(\sum_{\sigma' \in \mathbb{E}_n}\left(c_{\sigma'}^+\left|\psi_\pi^+(\sigma')\right\rangle + c_{\sigma'}^-\left|\psi_\pi^-(\sigma')\right\rangle\right)\right) \\ =&\sum_{\sigma,\sigma' \in \mathbb{E}_n} \left|\psi_\pi^\pm(\sigma)\right\rangle\left(c_{\sigma'}^+\left\langle\psi_\pi^\pm(\sigma)|\psi_\pi^+(\sigma')\right\rangle + c_{\sigma'}^-\left\langle\psi_\pi^\pm(\sigma)|\psi_\pi^-(\sigma')\right\rangle\right) \\ =&\sum_{\sigma \in \mathbb{E}_n} c_\sigma^\pm\left|\psi_\pi^\pm(\sigma)\right\rangle. \end{aligned}$$

The result of the first 4 Steps of the Algorithm 9 is ($|\psi_\pi^\pm(\sigma)\rangle = \pm|\psi_\pi^\pm(\sigma\pi)\rangle$):

$$
\begin{aligned}
&(H\otimes\mathbb{1})C_\pi(H\otimes\mathbb{1})|0\rangle|\psi\rangle \\
&= \frac{1}{\sqrt{2}}(H\otimes\mathbb{1})C_\pi(|0\rangle+|1\rangle)|\psi\rangle \\
&= \frac{(H\otimes\mathbb{1})}{\sqrt{2}}C_\pi\left(|0\rangle|\psi\rangle+|1\rangle\sum_{\sigma\in\mathbb{E}_n}\left(c_\sigma^+\left|\psi_\pi^+(\sigma)\right\rangle+c_\sigma^-\left|\psi_\pi^-(\sigma)\right\rangle\right)\right) \\
&= \frac{(H\otimes\mathbb{1})}{\sqrt{2}}\left(|0\rangle|\psi\rangle+|1\rangle\sum_{\sigma\in\mathbb{E}_n}\left(c_\sigma^+\left|\psi_\pi^+(\sigma)\right\rangle-c_\sigma^-\left|\psi_\pi^-(\sigma)\right\rangle\right)\right) \\
&= \frac{|0\rangle+|1\rangle}{2}\sum_{\sigma\in\mathbb{E}_n}\left(c_\sigma^+\left|\psi_\pi^+(\sigma)\right\rangle+c_\sigma^-\left|\psi_\pi^-(\sigma)\right\rangle\right) \\
&\quad +\frac{|0\rangle-|1\rangle}{2}\sum_{\sigma\in\mathbb{E}_n}\left(c_\sigma^+\left|\psi_\pi^+(\sigma)\right\rangle-c_\sigma^-\left|\psi_\pi^-(\sigma)\right\rangle\right) \\
&= |0\rangle\sum_{\sigma\in\mathbb{E}_n}c_\sigma^+\left|\psi_\pi^+(\sigma)\right\rangle+|1\rangle\sum_{\sigma\in\mathbb{E}_n}c_\sigma^-\left|\psi_\pi^-(\sigma)\right\rangle \\
&= |0\rangle P_\pi^+|\psi\rangle+|1\rangle P_\pi^-|\psi\rangle.
\end{aligned}
$$

Measuring the first register in the computational basis (Step 5 of Algorithm 9) collapses the second register (up to a normalization factor) in the state $P_\pi^\pm|\psi\rangle$ with probability $||P_\pi^\pm|\psi\rangle||^2$, just as if M_π was measured.

An immediate corollary is that M_π distinguishes ρ_π^+ and ρ_π^- with probability one.

At the end of an oblivious transfer protocol, Bob must know if he received the message or not. In our protocol, this step is guaranteed by a *universal hash function*. These functions map larger strings to strings of smaller size, hence collisions are unavoidable, *i.e.*, different messages can be mapped to the same hash. Despite this fact, one can design these functions in such a way that:

- they are computationally efficient, *i.e.*, one can compute its value from a message in polynomial time;
- hashes are almost equally distributed.

Definition 11 *Let A and B be two sets of size a and b, respectively, such that $a > b$, and let $\mathbb{H}$ be a collection of hash functions $h : A \to B$. $\mathcal{H}$ is said to be a* universal family of hash functions *if, for all $x, y \in A$*

$$\Pr_{h\in\mathbb{H}}[h(x) = h(y)] \leq \frac{1}{b}.$$

A straightforward consequence of this definition is the following theorem.

Theorem 12 *Let A and B be two sets of size a and b, respectively, such that $a > b$ and let $\mathbb{H}$ be a collection of hash functions $h : A \to B$. If $\mathbb{H}$ is a universal family of hash functions then for any set $A' \subset A$ of size N and for any $x \in A$, the expected number of collisions between x and other elements in A' is at most N/b.*

Notice that, in particular, if we request A to contain all strings of length ℓ and B to have length say $\omega = \lfloor\sqrt{\ell}\rfloor$, then the number of expected collisions is $2^\omega = 2^{\lfloor\sqrt{\ell}\rfloor}$, hence the probability of finding a collision is negligible in ℓ. There are several standard ways to construct universal families of hash functions (see [9] for examples and details). In this paper, we prove the security of our protocol for a specific universal family of hash functions that are easy to construct. For simplicity, we postpone the description of this rather technical detail for the proof of Theorem 15.

3 The bit-string oblivious transfer protocol

In this section, we present a quantum protocol that achieves oblivious transfer of a bit-string from Alice to Bob in polynomial time. As already mentioned in the introduction, oblivious transfer protocol is a protocol in which Alice sends (transfers) a message $m = m_1 m_2 \dots m_\ell$ of length ℓ to Bob (during the transfer phase), which is recovered by him with only 50% of probability during the opening phase (the *transfer is probabilistic*). The protocol must satisfy two additional properties: be *concealing*, *i.e.*, Bob must not learn m before the opening phase; and be *oblivious*, *i.e.*, after the opening phase Alice must *not know with certainty* if Bob received m or not. Notice that Bob, unlike Alice, *does know* at the end of the protocol if he received the intended message. In the rest of this section, we present our results in terms of orthogonal measurements M_π, which according to Proposition 10 can be realized in polynomial time by applying Algorithm 9.

Protocol 13 (Bit-string oblivious transfer)

Security parameters ℓ *and* $n \geq \ell$.

Message to transfer $m = m_1 \dots m_\ell$.

Universal hash function $h : \Sigma^\ell \to \Sigma^\omega$.

Secret key $\pi \in \mathbb{K}_n$.

Transfering phase

Step 1. *Alice generates uniformly at random the secret key* $\pi \in \mathbb{K}_n$.

Step 2. *Using Algorithm 7 with* π*, and the operation* C_{sgn}*, she constructs the state* $\rho_\pi^m = \rho_\pi^{m_1} \otimes \rho_\pi^{m_2} \otimes \ldots \otimes \rho_\pi^{m_\ell}$ *where* $\rho_\pi^{m_i} = \rho_\pi^+$ *if* $m_i = 1$*, and* $\rho_\pi^{m_i} = \rho_\pi^-$ *otherwise.*

Step 3. *Alice sends* ρ_π^m *and* $y = h(m)$ *to Bob.*

Opening phase

Step 4. *Bob generates uniformly at random* $\tau \in \mathbb{S}_n$ *and sends it to Alice.*

Step 5. *Alice computes uniformly at random either* $\delta = \pi \circ \tau$ *or* $\delta = \tau \circ \pi$*, and sends it back to Bob.*

Step 6. *Bob computes uniformly at random either* $\gamma = \delta \circ \tau^{-1}$ *or* $\gamma = \tau^{-1} \circ \delta$.

Step 7. *Bob measures the observable* $M_\gamma^{\otimes \ell}$ *on the system given by Alice, obtaining the result* $\tilde{m}$.

Step 8. *Bob checks if* $h(\tilde{m}) = y$*. If so, he concludes that the message sent by Alice is* $\tilde{m}$*, i.e.,* $\tilde{m} = m$.

Step 9. *If Bob got the correct message, he chooses another* $\pi' \in \mathbb{K}_n$ *and measures the observable* $M_{\pi'}^{\otimes \ell}$ *on the system, obtaining result* $r = r_1 \ldots r_\ell$*. If approximately half of the results* r_i *are different from the corresponding* m_i*, then Bob accepts the message; otherwise he aborts the protocol declaring that Alice tried to cheat.*

Below, we present an informal analysis of the security of the protocol, while the rigorous security criterion is given in the statement of Theorem 15. As discussed in the Introduction, in this paper we only consider the security of the protocol *per se*, while the security of complex schemes that use our protocol as a black box subroutine is to be carried out when analyzing particular realizations of such schemes. The protocol's security depends on parameter n through Theorem 5, which is satisfied asymptotically, i.e. for *sufficiently large* values of n. The dependence on ℓ comes through Probabilistic transfer requirement (see below Point 2 of Theorems 14 and 15), stated in terms of negligible functions $\varepsilon(\ell)$, again for *sufficiently large* values of ℓ. [A function $\varepsilon(\ell)$ is said to be negligible if $\varepsilon(\ell) < 1/p(\ell)$ for any polynomial $p(\ell)$ and sufficiently large ℓ.] Note that, since we require that $n \geq \ell$, [4] the security of the protocol is stated in terms of

[4] In fact, we require $\ell \leq c_1 n$ and $n \leq c_2 \ell$. To simplify the presentation, we take $n \geq \ell$.

a negligible function in ℓ: any security bound proven for n is at the same time a bound for ℓ (recall that a function is negligible if it scales to zero faster than the inverse of any polynomial, *for sufficiently large* value of its argument).

To show that our proposal is a bit-string oblivious transfer protocol we must prove that:

1. If Alice is honest, then the protocol is computationally *concealing*, *i.e.*, Bob cannot learn the message m before the opening phase. Notice that this follows directly from the hardness assumption of computational indistinguishability of states ρ^+ and ρ^- (Theorem 5) and from the fact that the hash function used for comparison has exponentially many collisions, *i.e.*, only with negligible probability Bob can correctly invert h in probabilistic polynomial time and obtain m.

2. If Alice is honest, then roughly in 50% of the cases Bob will obtain m (*probabilistic transfer*). Notice that the acknowledgment that $\tilde{m}$ is correct is given by the comparison of y with $h(\tilde{m})$;

3. If Bob is honest, then the protocol is *oblivious*, *i.e.*, Alice cannot learn with certainty whether Bob got the message m or not. This is a consequence of the impossibility of faster than light information transmission and it is ensured by the last step of the protocol. The *rationale* for Step 9 is to prevent Alice from cheating by sending a state that would allow her to know with certainty that Bob would receive the message. We postpone the discussion of this point for the end of the paper.

Notice that if the order of compositions agree in Steps 5 and 6 of the Protocol, *i.e.*, Alice and Bob applied respectively τ and τ^{-1} on the same side, then $\gamma = \pi$; otherwise, if Alice and Bob applied τ and τ^{-1} on different sides, then both $\gamma = \tau^{-1} \circ \pi \circ \tau$ and $\gamma = \tau \circ \pi \circ \tau^{-1}$ belong to $\mathbb{K}_n$ but are different from π (in fact, $\tau^{-1} \circ \pi \circ \tau = \tau \circ \pi \circ \tau^{-1}$).

Also, due to the properties of hash functions, the probability of two randomly chosen messages having the same hash value is negligible. Therefore, if in Step 8 of the Protocol $h(\tilde{m}) = y = h(m)$, then $\tilde{m}$ is, up to negligible probability, the actual message m.

Therefore, if both Alice and Bob are honest, then Bob measures with equal probability either $M_{\pi}^{\otimes \ell}$ or $M_{\pi'}^{\otimes \ell}$, where $\pi' = \tau \circ \pi \circ \tau^{-1} \in \mathbb{K}_n$ for some $\tau \in \mathbb{S}_n$. If he measures $M_{\pi}^{\otimes \ell}$, then the measurement result $\tilde{m}$ will indeed be equal to m, which he can confirm by comparing $h(\tilde{m})$ and y. Otherwise, and since π' does not match the used π, each single-system measurement will yield a random $\tilde{m}_i$,

and by confirming that $h(\tilde{m}) \neq y$, Bob will know that he did not receive the intended message.

This way, if both parties are honest, Bob will recover the message with probability 1/2. We formalize these in the following theorem:

Theorem 14 (Correctness of the Protocol 13) *Assume that $\mathbb{QSCD}_{ff}$ is polynomially hard even for quantum computers. If Alice and Bob correctly run Protocol 13 to transfer message $m = m_1 \dots m_\ell$ from Alice to Bob, then:*

1. **(Concealing)** *Bob cannot infer m before the opening phase except with negligible probability on ℓ, the size of the message m.*
2. **(Probabilistic transfer)** *Bob will receive m with probability $1/2 + \varepsilon(\ell)$, where $\varepsilon(\ell)$ is a negligible function.*
3. **(Oblivious)** *Alice remains oblivious to the fact that Bob received the message.*

Proof: We prove each item stated in the theorem separately.

1. Since Bob is honest, he does not perform any quantum operations other than those prescribed by the protocol. In particular, he does not perform any measurement on the quantum system received by Alice before the opening phase. On the other hand, since it is assumed that h is a universal hash function, trying to recover m by computing the inverse of h is only possible with negligible probability. In fact, since the hash function h maps strings of length ℓ to strings of length $\omega = \lfloor \sqrt{\ell} \rfloor$, by Theorem 12 one can recover m with probability $2^{-\lfloor \sqrt{\ell} \rfloor}$ which is negligible in ℓ (recall that by negligible we mean that the probability to recover m scales to zero faster than the inverse of any polynomial in the length of the message).

2. It is easy to see that after Step 6 of Protocol 13, $\gamma = \pi$ with probability 1/2 if both Alice and Bob make their choices in Steps 5 and 6 at random, and Bob chooses τ uniformly at random.

   For $\gamma = \pi$, the result that the measurement $M_\pi^{\otimes \ell}(\rho_\pi^m)$ equals m follows from Proposition 10.

   It remains to show that when $\gamma = \pi' \neq \pi$, by performing the measurement $M_\gamma^{\otimes \ell}$, the probability of recovering m from the quantum state ρ_π^m sent by Alice is negligible. First we prove that for any σ the result of the

measurement of $M^{\ell}_{\pi'}$ is random. Observe that

$$
\begin{aligned}
&P^{\pm}_{\pi'}(\left|\psi^{+}_{\pi}(\sigma)\right\rangle) = \sum_{\sigma'\in\mathbb{E}_n} \left|\psi^{\pm}_{\pi'}(\sigma')\right\rangle \left\langle\psi^{\pm}_{\pi'}(\sigma')|\psi^{+}_{\pi}(\sigma)\right\rangle \\
&= \sum_{\sigma'\in\mathbb{E}_n} \frac{(|\sigma'\rangle \pm\ |\sigma'\circ\pi'\rangle)(\langle\sigma'| \pm \langle\sigma'\circ\pi'|)(|\sigma\rangle + |\sigma\circ\pi\rangle)}{2\sqrt{2}} \\
&= \sum_{\sigma'\in\mathbb{E}_n} \frac{(|\sigma'\rangle \pm |\sigma'\circ\pi'\rangle)(\langle\sigma'|\sigma\rangle + \langle\sigma'|\sigma\circ\pi\rangle \pm \langle\sigma'\circ\pi'|\sigma\rangle \pm \langle\sigma'\circ\pi'|\sigma\circ\pi\rangle)}{2\sqrt{2}} \\
&= \begin{cases} \displaystyle\sum_{\sigma'\in\mathbb{E}_n} \frac{(|\sigma'\rangle \pm |\sigma'\circ\pi'\rangle)(\langle\sigma'|\sigma\rangle + \langle\sigma'\circ\pi'|\sigma\circ\pi\rangle)}{2\sqrt{2}}, & \text{if } \sigma\in\mathbb{E}_n \\ \displaystyle\sum_{\sigma'\in\mathbb{E}_n} \frac{(|\sigma'\rangle \pm |\sigma'\circ\pi'\rangle)(\langle\sigma'|\sigma\circ\pi\rangle \pm \langle\sigma'\circ\pi'|\sigma\rangle)}{2\sqrt{2}}, & \text{if } \sigma\in\mathbb{O}_n \end{cases} \\
&= \frac{1}{2\sqrt{2}}\left(|\sigma\rangle \pm |\sigma\circ\pi'\rangle + |\sigma\circ\pi\rangle \pm |\sigma\circ\pi\circ\pi'\rangle\right) \\
&= \frac{1}{2}\left(\left|\psi^{\pm}_{\pi'}(\sigma)\right\rangle \pm \left|\psi^{\pm}_{\pi'}(\sigma\circ\pi\circ\pi')\right\rangle\right. \\
&= \frac{1}{\sqrt{2}}\left(\frac{1}{\sqrt{2}}(\left|\psi^{\pm}_{\pi'}(\sigma)\right\rangle \pm \left|\psi^{\pm}_{\pi'}(\sigma\circ\pi\circ\pi')\right\rangle)\right).
\end{aligned}
$$

Since $\left|\psi^{\pm}_{\pi'}(\sigma)\right\rangle$ and $\left|\psi^{\pm}_{\pi'}(\sigma\circ\pi\circ\pi')\right\rangle$ are orthogonal, the vector $\frac{1}{\sqrt{2}}(\left|\psi^{\pm}_{\pi'}(\sigma)\right\rangle \pm \left|\psi^{\pm}_{\pi'}(\sigma\circ\pi\circ\pi')\right\rangle)$ is a unit one and $||P^{\pm}_{\pi'}(\psi^{+}_{\pi})||^2 = 1/2$. Hence, the probability of recovering $\pm$ from ρ^{+}_{π} is

$$
\begin{aligned}
Prob(+; M_{\pi'}, \rho^{+}_{\pi}) &= \mathrm{Tr}[P^{+}_{\pi'}\rho^{+}_{\pi}P^{+}_{\pi'}] \\
&= \frac{2}{n!}\sum_{\sigma\in\mathbb{E}_n} \mathrm{Tr}[P^{+}_{\pi'}\left|\psi^{+}_{\pi'}(\sigma)\right\rangle\left\langle\psi^{+}_{\pi'}(\sigma)\right|P^{+}_{\pi'}] \\
&= \frac{2}{n!}\sum_{\sigma\in\mathbb{E}_n} ||P^{+}_{\pi'}(\psi^{+}_{\pi})||^2 = \frac{1}{2}
\end{aligned}
$$

and similarly $Prob(-; M_{\pi'}, \rho^{+}_{\pi}) = \frac{1}{2}$. *Mutatis mutandis* we also have that $Prob(\pm; M_{\pi'}, \rho^{-}_{\pi}) = \frac{1}{2}$. Hence, by measuring $M^{\otimes\ell}_{\pi'}$ on ρ^{m}_{π} the probability of recovering m is negligible in ℓ.

To conclude the proof of the second item we need to show that Bob aborts the protocol in Step 9 only with negligible probability.

Notice that to reach Step 9, where Bob aborts the protocol, he must had run successfully the verification in Step 7. This implies that Bob performed the measurement with the correct trapdoor π, hence the state stayed invariant, i.e., it is still ρ^{m}_{π}. If Bob chooses in Step 9 random $\pi' \neq \pi$, then the probability of recovering each bit of the message, as just seen above, is equal to $1/2$ and so, by a simple binomial argument,

the probability of having a significant difference from half of the states is negligible on ℓ.

3. Notice that Alice must send a permutation δ, such that both $\delta \circ \tau^{-1}$ and $\tau^{-1} \circ \delta$ are from $\mathbb{K}_n$. Bob's choice to compose δ with τ^{-1} on the left, or on the right, is random and unknown to Alice: after sending δ there is no more communication between Alice and Bob and there is no information transmission from Bob to Alice. Therefore, the choice of Bob's measurement observable $M_\gamma^{\otimes \ell}$ is also unknown to Alice as well: Alice cannot know if Bob has obtained the message m, or not.

Finally we prove the security of the protocol. In the description of the protocol, only the encrypted message is sent as a state of a quantum system (ρ_π^m), while the hash value $h(m)$ is sent as a classical information. Nevertheless, even if joint *quantum* measurements on both systems carrying the encrypted message and the hash value were allowed, this would not give advantage to a cheating Bob.

Let $\mathcal{H}_m$ and $\mathcal{H}_h$ be the Hilbert spaces of the systems carrying the encrypted message and the hash value $h(m)$, respectively. In the following, we show that performing joint measurements over the entire Hilbert space $\mathcal{H}_{mh} = \mathcal{H}_m \otimes \mathcal{H}_h$ cannot achieve better cheating efficiency than an optimal strategy involving only measurements on sub-systems given by $\mathcal{H}_m$ and $\mathcal{H}_h$.

After the transferring phase, Bob's description of the joint system received from Alice is given by the quantum state (recall that hash-values are bit-strings of length ω):

$$\begin{aligned} \rho_B &= \frac{1}{|\mathbb{K}_n|} \sum_\pi \frac{1}{2^k} \sum_m \rho_\pi^m \otimes |h(m)\rangle\langle h(m)| \\ &= \frac{1}{|\mathbb{K}_n|} \sum_\pi \frac{1}{2^\omega} \sum_h \left(\frac{1}{2^{k-\omega}} \sum_{m_h \in h^{-1}} \rho_\pi^{m_h} \right) \otimes |h\rangle\langle h|. \end{aligned}$$

Note that states $|h\rangle \in \mathcal{H}_h$ are orthogonal to each other (they are fully distinguishable).

The aim of a cheating Bob is to discriminate among $|\mathbb{K}_n| \cdot 2^k$ states $\{\rho_\pi^m \otimes |h(m)\rangle\langle h(m)|\}$. The optimal probability of success of the joint-measurement discrimination strategy is the expected success probability of the same strategy when applied on the systems from sub-ensembles, each having the same hash-value h: $p_{succ}^J = \sum_h 2^{-\omega} p_{succ}^J(h)$, where $p_{succ}^J(h)$ is the success probability of the joint-measurement strategy for the sub-ensemble given by a fixed hash value h. Each such sub-ensemble consists of $|\mathbb{K}_n| \cdot 2^{k-\omega}$ uncorrelated product

states $\{\rho_\pi^{m_h} \otimes |h\rangle\langle h| : m_h \in h^{-1}\}$, with the hash value h being the same for all elements of the sub-ensemble. Thus, the success probability of the joint-measurement strategy for each sub-ensemble is at most the optimal success probability of discriminating between the states $\{\rho_\pi^{m_h}\}$ having the same hash value h. Since states $|h\rangle$ are orthogonal to each other, by performing the sub-system measurements only (first measuring onto $\mathcal{H}_h$ in the $\{|h\rangle\}$ basis, and then performing an optimal discrimination measurement onto $\mathcal{H}_m$), Bob can achieve the optimal probability of discriminating among the states $\{\rho_\pi^m \otimes |h(m)\rangle\langle h(m)|\}$.

Therefore, one can assume that Bob is allowed to perform quantum measurements only on the system that carries the encrypted message. Below, we prove the protocol's security. We emphasize that the concealing and oblivious properties are satisfied against arbitrary cheating strategies of Alice and Bob, while the transfer is probabilistic as long as Bob is restricted to perform a few-qubit coherent measurements.

Theorem 15 (Security) *Assume that $\mathbb{QSCD}_{ff}$ is polynomially hard even for a quantum computer. The Protocol 13 is secure against cheating, i.e.*

1. **(Concealing)** *If Alice is honest, then even if he cheats, Bob cannot in polynomial time learn m before the opening phase, unless with negligible probability on ℓ.*

2. **(Probabilistic transfer)** *If Alice is honest, and Bob is restricted to few-qubit coherent measurements, then he will receive m with probability $1/2 + \varepsilon(\ell)$, where $\varepsilon(\ell)$ is a negligible function.*

3. **(Oblivious)** *If Bob is honest, then Alice cannot learn with certainty if he received the message even if she tries to cheat.*

Proof:

1. Notice that upon receiving a system from Alice the only thing Bob can do in order to learn its state (and hence the message m) is to simply "look" at it, *i.e.*, perform a measurement in order to distinguish between ρ_π^+ and ρ_π^- (without knowing π). The concealing property follows directly from Theorem 5 proved in [19], which states that distinguishing ρ_π^+ from ρ_π^- without knowing π is polynomially hard even for a quantum computer. In other words, under the assumption that $\mathbb{QSCD}_{ff}$ is polynomially hard for a quantum computer, only with negligible probability one can, *without knowing* π, prepare in polynomial time a measurement that can distinguish ρ_π^+ from ρ_π^- with non-negligible advantage (i.e., the

two states are *(quantum) computationally indistinguishable*). Moreover, if our Protocol 13 were not concealing, i.e., there would exist a (quantum) polynomial-time strategy that distinguishes ρ_π^+ from ρ_π^-, which could be used to devise an attack to the crypto-system developed in [19]. This is strongly believed to be false, since otherwise the power of quantum computers would be much stronger that it is conjectured by the community. For this reason, it is enough to show that Bob cannot learn (unless with negligible probability) neither π, nor the message m.

Notice that since Alice does not send π, the probability that Bob guesses the correct π is negligible on ℓ (since in the protocol we assume $n \geq \ell$): the size of $\mathbb{K}_n$ is

$$|\mathbb{K}_n| = \frac{n!}{(n/2)!} ,$$

which is already for $n = 10$ huge enough for practical purposes. Note that the additional information provided by Alice, the hash value $h(m)$, cannot help Bob recovering the message m, for suitable chosen universal family of hash functions. First, we prove the concealing property using a particular hash function. Then, we show that the same is valid for a whole universal family of hash functions.

The message m can be divided into $\omega = \lfloor\sqrt{\ell}\rfloor$ consecutive blocks of bits $\bar{m}_i$ $(i = 1, \ldots, \omega)$, each of the same length $\lfloor\sqrt{\ell}\rfloor$: $m = \bar{m}_1 \ldots \bar{m}_\omega$. The bits $h_i(m)$ of the hash function are given by the parity of the i-th block of the message m: $h_1(m) = m_1 \oplus \ldots \oplus m_\omega$, etc. Note that each bit of $h(m)$ is independent of each other and depends only on specific block $\bar{m}_i$ of size ω. Therefore, if $h(m)$ would allow to recover m with some non-negligible probability p, then $h_1(m)$ alone would help to recover $\bar{m}_1 = m_1 \oplus \ldots \oplus m_\omega$, with the same probability p. Such cheating strategy is impossible, assuming that the cryptographic system presented in [19] is secure.

Note that if a cryptographic system is computationally secure for coding a message m of length ℓ, then it must be computationally secure when encrypting a polynomially shorter message, say $\bar{m}_1$. Then, by guessing the parity of $\bar{m}_1$, and using the above cheating strategy, one would be able to break the crypto system with non-negligible probability $p/2$.

From the above hash function h, it is easy to define the whole universal family of hash functions, indexed by permutations from $\mathbb{S}_\ell$, for which the concealing property is satisfied. Given $\alpha \in \mathbb{S}_\ell$, one can define the hash function $h_\alpha(m) = h_{id_n}(m_{\alpha(1)} \ldots m_{\alpha(\ell)})$, where h_{id_n} is the above h.

Obviously, the concealing property is valid for the whole set $\{h_\alpha | \alpha \in \mathbb{S}_\ell/\mathbb{S}_\omega\}$ of universal hash functions.

2. Suppose Bob is restricted to perform single-qubit measurements (for a recent version of quantum digital signatures secure against single-qubit measurements, see [14, 10]), and the hash function is given as in previous item 1 of this theorem. Note that upon receiving δ from Alice, Bob knows both π and $\pi' = \tau \circ \pi \circ \tau^{-1}$, but *does not know which of the two was used* by Alice to encrypt the message m into the quantum state given to him.

   The bit value $h_i(m) = h_i(\bar{m}_i)$ of the hash $h(m)$ is the parity of the corresponding block $\bar{m}_i$. For each bit of the block $\bar{m}_i$, say the first bit, its value is completely uncorrelated with $h_i(\bar{m}_i)$, unless one knows the values of all other bits: in order for the measurement observable on the first qubit to be a function of the hash value, Bob needs to know the values of all other bits from that block. On the other hand, within the remaining $\omega - 1$ bits, each one is completely uncorrelated with the others, and the hash value $h_i(\bar{m}_i)$ (since the value of the first bit is not known). Therefore, Bob's choice of the single-qubit measurement observable on each of the remaining $\omega - 1$ qubits is independent on the hash value.

   Moreover, the fact that the same secret key π is used to encrypt all bits of the message, thus establishing correlations between single-qubit states, cannot help Bob in choosing the optimal cheating observable: since for each pair (π, π') the states ρ^b_π and $\rho^b_{\pi'}$ (with $b = 0, 1$) are not fully distinguishable, and Bob will, unless he chooses to measure the right M_π (which can happen only with probability $1/2$), inevitably obtain wrong results for single bits [5]. Nevertheless, he can know that he obtained wrong bit values only upon performing measurements on *all* qubits of a single block. Therefore, Bob is forced to perform the same measurement on each of qubits of a single block (with possible exception of the last one), which is a function of *both* π and π' (and, as shown above, not $h(m)$).

   Let that measurement be given by the (orthogonal) observable $M = 0 \cdot P^+ + 1 \cdot P^-$. In order to achieve $Prob(+; M, \rho^+_{\pi/\pi'}) = 1$ (i.e., recover the bit value 0 encoded in the state $\rho^+_{\pi/\pi'}$), the eigenspace $\mathcal{H}^+$ for the value 0 of the observable M must contain the ranges of $\rho^+_{\pi/\pi'}$, given by the

[5] Note that the strategy of randomly choosing the permutation and performing measurements accordingly within a single block, gives Bob a chance that, with probability $1/2$, confirm that the choice was wrong. This way, even if his choice was wrong, Bob will, with probability exponentially close to 1, learn all of m but a few first blocks. Nevertheless, even in the best case scenario (only the first block $\bar{m}_1$ is wrongly decrypted), there are exponentially many (in fact, $2^{\sqrt{\ell}-1}$) possible messages that Alice could have sent.

eigenspaces $\mathcal{H}^{+}_{\pi/\pi'}$ of the observables $M_{\pi/\pi'}$: $\mathcal{H}^{+}_{\pi} \cup \mathcal{H}^{+}_{\pi'} \subseteq \mathcal{H}^{+}$. As proven in item 2 of previous Theorem, $Prob(\pm; M_{\pi'}, \rho^{+}_{\pi}) = Prob(\pm; M_{\pi'}, \rho^{-}_{\pi}) = 1/2$ (and analogously when measuring M_{π} on $\rho^{\pm}_{\pi'}$): the eigenspaces of the two observables M_{π} and $M_{\pi'}$ corresponding to two different outcomes 0 and 1 are not orthogonal to each other, and thus the two projectors P^{+} and P^{-} cannot be orthogonal. As a consequence, for each pair $\pi, \pi' \in \mathbb{K}_n$, the probability q of distinguishing between $\{\rho^{+}_{\pi}, \rho^{+}_{\pi'}\}$ and $\{\rho^{-}_{\pi}, \rho^{-}_{\pi'}\}$ (i.e., inferring the bit value) is strictly *smaller* than 1. Therefore, the probability of recovering the remaining $\omega - 1$ bits, and thus the whole block, is negligible (of the order of $q^{-\omega}$).

The above argument can be extended to few-qubits measurements. Assume Bob can perform two-qubit measurements with four possible outcomes $00, 01, 10$, and 11, used to infer four distinct two-bit messages. Following the above analysis, in order to *perfectly* infer a two-bit message, say 00, the corresponding eigenspace $\mathcal{H}^{00}$ of the Bob's observable must satisfy $\mathcal{H}^{00}_{\pi} \cup \mathcal{H}^{00}_{\pi'} \subseteq \mathcal{H}^{00}$, where $\mathcal{H}^{00}_{\pi} = \mathcal{H}^{0}_{\pi} \otimes \mathcal{H}^{0}_{\pi}$, etc. Again, since the eigenspaces $\mathcal{H}^{s}_{\pi}$ and $\mathcal{H}^{s'}_{\pi'}$, corresponding to two different two-bit strings s and s', are not orthogonal to each other, there is a finite optimal (expected) probability q of distinguishing between different two-bit strings which, for large enough blocks, results in negligible cheating probability (Bob can increase the 1/2 probability of learning the overall message sent by Alice by only a negligible amount).

Note that as the size of a string that can be coherently measured increases (the number L of qubits that can be coherently measured), the eigenspaces $\mathcal{H}^{s}_{\pi}$ and $\mathcal{H}^{s'}_{\pi'}$, corresponding to two different L-bit strings s and s', become more and more closer to orthogonal. In order to know how long a block should be, such that for a given L Bob's probability to cheat is negligible, i. e. find $\omega = \omega(L)$, one has to solve the equation $[q(L)]^{\omega/L} = \varepsilon(\omega)$, where $q(L)$ is the (expected) probability of distinguishing between two L-bit strings, and $\varepsilon(\omega)$ is a negligible function. A detailed analysis of the relationship between the length ω of the block $\bar{m}$ (and thus the length $\ell = \omega^2$ of the overall message m) and the size L of disposable coherent measurements is a matter of further study.

3. To finish the argument of the security of Protocol 13 we show that the protocol is unconditionally *oblivious* against a cheating Alice, *i.e.*, there is no strategy for Alice which would enable her to know with certainty if Bob received the message m or not. This is ensured by the last step of the protocol. Notice that since Alice cannot know beforehand which permutation τ will be chosen by Bob, nor she knows which γ Bob choses

in Step 6 of the protocol, she does not know which measurement $M_\gamma^{\otimes \ell}$, with $\gamma \in \mathbb{K}_n$, is performed by Bob in Step 7. Therefore, in order to know if Bob received the message m, she must prepare a state ρ^m that leads to the same answer m regardless of the measurement selected by Bob. Obviously, in order to satisfy the requirement that Bob learns m in 50% of the cases, she sends uniformly at random either ρ^m, in which case she knows with certainty that Bob got the message, or a completely mixed state $(\mathbb{1}/n!)^{\otimes \ell}$, in which case she knows with certainty that Bob does not get the message except with negligible probability. So, if Alice wants to be non-oblivious, she needs to prepare states that give with certainty the same result for every measurement M_π, and are thus invariant, which is the reason for introducing Step 9. If Bob got the correct message, he can recheck that Alice did not use this cheating strategy by performing another measurement of the same kind but with a different π'. Since the state sent by Alice has to be invariant for any measurement, measuring the state with this π' will lead to the same result as the original choice and Bob will thus abort the protocol.

4 Conclusions

Oblivious transfer is an important primitive for designing cryptographic protocols and secure multiparty computation schemes. In this paper we proposed a polynomial-time quantum protocol for oblivious transfer of a bit-string from Alice to Bob based on the $\mathbb{Q}\$\mathbb{C}\mathbb{D}_{ff}$ state distinguishability problem. We showed that, assuming $\mathbb{Q}\$\mathbb{C}\mathbb{D}_{ff}$ to be polynomially hard even for a quantum computer, our protocol is computationally concealing, unconditionally oblivious, and achieves the goal of transferring information with probability close to $1/2$, as long as Bob can perform only few-qubit coherent measurements (while security against most general coherent attacks performed on *all* qubits of the message is left as an open question). The oblivious and the probabilistic transferring properties rely on the laws of quantum mechanics, while the acknowledgment of the message transfer is ensured by the use of hash functions. Note that, in general, one may not need to use hash functions. For example, if the message sent by Alice is of a particular type, say an NP-problem (*e.g.* SAT or some hard optimization problem), then there is no need to encode the message in the hash value: Bob can verify if he received the message by simply checking if it is the solution of the problem. Also if the message sent by Alice is a binary code of some text in a human language, then the verification of the meaningful information serves as acknowledgment.

Acknowledgments

This work was partially supported, under the CV-Quantum internal project at IT, by FCT PEst-OE/EEI/LA0008/2013 and UID/EEA/50008/2013 and EU FEDER, namely via the FCT projects ComFormCrypt PTDC/EIA-CCO/113033/2009, and CaPri initiative. André Souto also acknowledges the FCT postdoc grant SFRH/BPD/ 76231/2011.

References

[1] J. Barrett and S. Massar. Security of quantum bit-string generation. *Phys. Rev. A*, 70:052310, Nov 2004.

[2] M. Ben-Or, M. Horodecki, D. Leung, D. Mayers, and J. Oppenheim. In Joe Kilian, editor, *Theory of Cryptography*, volume 3378 of *Lecture Notes in Computer Science*, pages 386–406, 2005.

[3] C. Bennett and G. Brassard. Quantum Cryptography: Public Key Distribution and Coin Tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, New York, 1984. IEEE Press.

[4] C. Bennett, G. Brassard, C. Crépeau, and M. Skubiszewska. Practical quantum oblivious transfer. In Joan Feigenbaum, editor, *Advances in Cryptology*, volume 576, pages 351–366. Springer Berlin Heidelberg, 1992.

[5] N. Bouman, S. Fehr, C. Gonzalez-Guillen, and C. Schaffner. An all-but-one entropic uncertainty relation, and application to password-based identification. In Kazuo Iwama, Yasuhito Kawano, and Mio Murao, editors, *Theory of Quantum Computation, Communication, and Cryptography*, volume 7582 of *Lecture Notes in Computer Science*, pages 29–44. Springer Berlin Heidelberg, 2013.

[6] G. Brassard, C. Crepeau, and J.. Robert. Information theoretic reductions among disclosure problems. In *Foundations of Computer Science, 1986., 27th Annual Symposium on*, pages 168–173, Oct 1986.

[7] G. Brassard, C. Crepeau, and M. Santha. Oblivious transfers and intersecting codes. *Information Theory, IEEE Transactions on*, 42(6):1769–1780, Nov 1996.

[8] H. Buhrman, M. Christandl, P. Hayden, H. Lo, and S. Wehner. Security of quantum bit string commitment depends on the information measure. *Phys. Rev. Lett.*, 97:250501, Dec 2006.

[9] J. Carter and M. Wegman. Universal classes of hash functions. *J. Comput. Syst. Sci.*, 18(2):143–154, 1979.

[10] R. Collins, R. Donaldson, V. Dunjko, P. Wallden, P. Clarke, E. Andersson, J. Jeffers, and G. Buller. Realization of quantum digital signatures without the requirement of quantum memory. *Phys. Rev. Lett.*, 113:040502, Jul 2014.

[11] R. Cramer, I. Damgård, and U. Maurer. General secure multi-party computation from any linear secret-sharing scheme. In *Proceedings of the 19th International Conference on Theory and Application of Cryptographic Techniques*, EUROCRYPT'00, pages 316–334, Berlin, Heidelberg, 2000. Springer-Verlag.

[12] C. Crépeau. Equivalence between two flavours of oblivious transfers. In *CRYPTO*, pages 350–354, 1987.

[13] C. Crepeau and M. Santha. Efficient reduction among oblivious transfer protocols based on new self-intersecting codes. In Renato Capocelli, Alfredo Santis, and Ugo Vaccaro, editors, *Sequences II*, pages 360–368. Springer New York, 1993.

[14] V. Dunjko, P. Wallden, and E. Andersson. Quantum digital signatures without quantum memory. *Phys. Rev. Lett.*, 112:040502, Jan 2014.

[15] S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. *Commun. ACM*, 28(6):637–647, 1985.

[16] L. Harn and H. Lin. An oblivious transfer protocol and its application for the exchange of secrets. In Hideki Imai, RonaldL. Rivest, and Tsutomu Matsumoto, editors, *Advances in Cryptology*, volume 739 of *Lecture Notes in Computer Science*, pages 312–320. Springer Berlin Heidelberg, 1993.

[17] G. P. He and Z. D. Wang. Nonequivalence of two flavors of oblivious transfer at the quantum level. *Phys. Rev. A*, 73:044304, Apr 2006.

[18] G. P. He and Z. D. Wang. Oblivious transfer using quantum entanglement. *Phys. Rev. A*, 73:012331, Jan 2006.

[19] Akinori Kawachi, Takeshi Koshiba, Harumichi Nishimura, and Tomoyuki Yamakami. Computational indistinguishability between quantum states

and its cryptographic application. *Journal of Cryptology*, 25(3):528–555, 2012.

[20] A. Kent. Unconditionally secure bit commitment. *Phys. Rev. Lett.*, 83:1447–1450, Aug 1999.

[21] A. Kent. Quantum bit string commitment. *Physical Review Letters*, 90:237901, Jun 2003.

[22] A. Kent. Secure classical bit commitment using fixed capacity communication channels. *J. Cryptology*, 18(4):313–335, 2005.

[23] J. Kilian. Founding crytpography on oblivious transfer. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC '88, pages 20–31, New York, NY, USA, 1988. ACM.

[24] R. Koenig, S. Wehner, and J. Wullschleger. Unconditional security from noisy quantum storage. *IEEE Transactions on Information Theory*, 58(3):1962–1984, 2012.

[25] Y. Lindell and B. Pinkas. Secure two-party computation via cut-and-choose oblivious transfer. *J. Cryptology*, 25(4):680–722, 2012.

[26] Yehuda Lindell and Hila Zarosim. On the feasibility of extending oblivious transfer. In *TCC*, pages 519–538, 2013.

[27] H. Lo and H. Chau. Is quantum bit commitment really possible? *CoRR*, quant-ph/9603004, 1996.

[28] H. K. Lo. Insecurity of quantum secure computations. *Phys. Rev. A*, 56:1154–1162, Aug 1997.

[29] H. K. Lo and H. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050–2056, 1999.

[30] H. K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Phys. Rev. Lett.*, 78:3410–3413, Apr 1997.

[31] R. Loura, Á. Almeida, P. André, A. Pinto, P. Mateus, and N. Paunković. Noise and measurement errors in a practical two-state quantum bit commitment protocol. *Phys. Rev. A.*, 89:052336, May 2014.

[32] D. Mayers. On the security of the quantum oblivious transfer and key distribution protocols. In Don Coppersmith, editor, *CRYPTO*, volume 963 of *Lecture Notes in Computer Science*, pages 124–135. Springer, 1995.

[33] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Physycal Review Letters*, page 3414, 1997.

[34] D. Mayers. Unconditional security in quantum cryptography. *J. ACM*, 48(3):351–406, May 2001.

[35] N. Ng, S. Joshi, C. Ming, C. Kurtsiefer, and S. Wehner. Experimental implementation of bit commitment in the noisy-storage model. *Nature Communications*, 3:1326–, 2012.

[36] N. Paunković, J. Bouda, and P. Mateus. Fair and optimistic quantum contract signing. *Physical Review A*, 84(6):062331–062331, December 2011.

[37] M. Rabin. How to exchange secrets by oblivious transfer. 1981.

[38] R. Renner and R. König. Universally composable privacy amplification against quantum adversaries. In Joe Kilian, editor, *Theory of Cryptography*, volume 3378 of *Lecture Notes in Computer Science*, pages 407–425. Springer Berlin Heidelberg, 2005.

[39] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *Rev. Mod. Phys.*, 81:1301–1350, Sep 2009.

[40] C. Schaffner, B. M. Terhal, and S. Wehner. Robust cryptography in the noisy-quantum-storage model. *Quantum Information & Computation*, 9(11):963–996, 2011.

[41] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J. Comput.*, 26(5):1484–1509, October 1997.

[42] P. W. Shor and J. Preskill. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441–444, Jul 2000.

[43] S. Wehner, C. Schaffner, and B. M. Terhal. Cryptography from noisy storage. *Phys. Rev. Lett.*, 100:220502, Jun 2008.

[44] S. Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, January 1983.