Oblivious transfer based on single-qubit rotations

J. Rodrigues P. Mateus N. Paunković A. Souto*

SQIG - Instituto de Telecomunicações
Departamento de Matemática - IST - UL

July 31, 2014

Abstract

We present a bit-string quantum oblivious transfer protocol based on single-qubit rotations. The proposed protocol does not violate the Lo's no-go theorem that prevents the unconditional security of 1-out-of-2 oblivious transfer. Our protocol is based on a previously proposed quantum public key protocol and its security relies on the laws of Quantum Mechanics. We also present a single-bit oblivious transfer based on the proposed bit-string protocol. The protocol can be implemented with current technology based on optics.

1 Introduction

Since the success of quantum cryptography, which allowed for unconditionally, secure exchange of secret keys [BB84, Eke91, Ben92], a hope appeared for designing quantum protocols with improved security with respect to their classical counterparts. One of the basic protocols used in building complex multiparty security schemes is the *Oblivious Transfer (OT) Protocol*.

OT can be seen as a game played by two parties, Alice and Bob. Alice has many secrets that wishes to share with Bob in such a way that at the end, on average, Bob learns half of those secrets and Alice does not know which secrets Bob really knows. Each instance of this protocol, used to reveal in half of the cases Alice's secret, is the Oblivious Transfer Protocol.

OT consists of two distinct phases: (i) the transferring phase, during which Alice sends an encoded secret information to Bob; (ii) the opening phase, during which Alice reveals enough information so that Bob can decode the secret with probability 1/2. Note that Bob knows if he got the message or not.

OT is said to be secure if the following properties hold: (i) the protocol is *concealing*, i.e., before the opening phase, Bob is not able to learn the message sent by Alice, while after the opening phase Bob learns the message with

*emails: jrodigues@math.ist.utl.pt, pmat@math.ist.utl.pt, npaunkovic@math.ist.utl.pt, a.souto@math.ist.utl.pt

probability 1/2; (ii) the protocol is *oblivious*, i.e., after the opening phase, Alice remains oblivious to whether or not Bob got the message.

Rabin was the first to formally present an oblivious transfer protocol in 1981 [Rab81]. The security of Rabin's OT relies on the fact that factoring large integers is not known to be possible to perform in polynomial time. Later, Even, Goldreich and Lempel presented a variation of this scheme called 1-*out-of*-2 *oblivious transfer* [EGL85]. The difference to Rabin's OT is that Alice sends two messages and Bob gets only one of the two with equal probability (again, Alice does not know which message Bob decoded). Although differently defined, Crépeau showed that when the messages are single bits the two flavors of oblivious transfer protocols are equivalent, in the sense that one can be built out of the other and vice versa [Cré88]. Furthermore, one can build an 1-out-of-2 oblivious transfer protocol that transmits bit-string messages from 1-out-of-2 oblivious transfer protocol for single bits [BCR86, CS93, BCS96].

The oblivious transfer is a building block of more complex security protocols [BCR86, Kil88, HL93] using Yao's garbled circuits [Yao86], and various secure multiparty computation schemes [CDM00, LP12, LZ13].

Another cryptographic primitive used in designing more complex secure protocols is bit commitment [BCC88]. Although it is not possible to construct an OT protocol out of a bit commitment [Sal98] it was shown that bit commitment can be reduced to 1-out-of-2 bit oblivious transfer protocol [BBCS92]. In Figure 1 we schematically present the classical reductions between the above discussed cryptographic primitives.

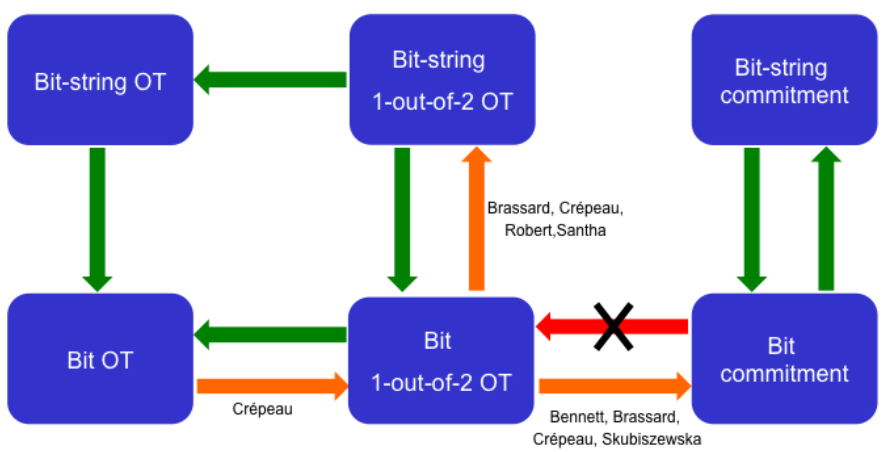

Figure 1: Classical reductions between cryptographic primitives. The green arrows represent straightforward reductions; the orange ones are non-trivial reductions; the red one is the impossible implication.

Due to the advance of quantum computation and quantum information, the development of cryptographic applications resilient to quantum adversaries has been extensively studied in the last decades. Wiesner launched the field of quantum cryptography in 1969 by presenting notions such as quantum money and quantum multiplexing (and only managed to publish his results in 1983 [Wie83]), the latter being essentially a quantum counterpart of a 1-out-of-2 oblivious transfer protocol.

Further developing Wiesner ideas, Bennett and Brassard presented the well-known BB84 quantum key distribution protocol [BB84], which was subsequently showed to be unconditionally secure [LC99, SP00, May01, SBPC$^+$09], while its classical counterparts are only computationally secure. Other example of a protocol whose quantum realization outperforms its classical counterpart is the recently proposed contract signing protocol [PBM11].

Despite these positive results, a number of no-go theorems imposed limits to quantum cryptography. Independently, Lo and Chau [LC96, LC97], and Mayers [May97], showed that unconditionally secure quantum bit commitment protocol is impossible, within the scope of non-relativistic physics (for unconditionally secure protocols that use relativistic effects, see [Ken99, Ken05, BFGGS13]). Subsequently, Lo [Lo97] proved similar no-go theorem for all "one-sided two-party computations" protocols. An immediate consequence of this result is the impossibility of having unconditionally secure 1-out-of-2 oblivious transfer. The alternative, ensuring practical security of such protocols, is to consider noisy or bounded memories [WST08, STW11, KWW12, NJM$^+$12, BFGGS13, LAA$^+$]. Recently, a (quantum) computationally secure version of oblivious transfer protocol was presented in [SMAaP].

Following the classical equivalence [Cré88] between the two flavors of oblivious transfer, one might conclude that impossibility of having unconditionally secure 1-out-of-2 oblivious transfer would imply the same for oblivious transfer as well. But the rules of quantum physics present a wider range of possibilities, thus compromising classical reduction schemes. Namely, as to build the 1-out-of-2 oblivious transfer one has to run several oblivious transfer protocols as black boxes, the possibility of the so-called coherent attacks – joint quantum measurements on several black boxes – arises. Thus, having unconditionally secure quantum oblivious transfer protocol does not necessarily mean that it is possible to construct unconditionally secure 1-out-of-2 oblivious transfer. Indeed, He and Wang recently showed that in quantum domain the various types of oblivious transfer are no longer equivalent [HW06b] and constructed an unconditionally secure quantum single-bit oblivious transfer [HW06a] using entanglement. Consequently, classical reductions of bit-string to a single-bit protocols are also compromised in the quantum setting and need to be re-examined. Recent example of constructing an unconditionally secure quantum bit-string commitment protocol [Ken03], despite the above mentioned no-go theorems for single-bit commitment [LC96, LC97, May97] is yet another example of invalidity of classical reductions (see also a quantum bit-string generation protocol [BM04]). Therefore, a need of explicitly constructing quantum bit-string oblivious transfer protocol which is not based on classical reductions mentioned above arises [Cré88, BCR86, CS93, BCS96].

In this paper we present a quantum oblivious transfer protocol for bit-strings, based on the recently proposed public key crypto-system [Nik08]. Each bit of the string to be transferred is encoded in a quantum state of a qubit, in such a way that states corresponding to bit values 0 and 1 form an orthonormal basis. The key point of the protocol is that for each qubit, the encoding basis is chosen at random, from some discrete set of bases.

2 Resullts

In this section we present the protocol that achieves oblivious transfer of a bit-string message from Alice to Bob. The scheme uses hash functions which allow to certify if after the opening phase Bob got the message or not. A hash function produces a *digest* of a message – a string of smaller size – such that: (i) the probability of generating at random strings with the same hash value is negligible; (ii) the hash values are almost uniformly distributed over the set of all possible digests.

Our protocol is based on the public key crypto system [Nik08], and can be briefly summarized as follows. Given a reference, so-called computational, basis $\beta_0 = \{|0\rangle, |1\rangle\}$, Alice first encodes each bit m_i of the message $m = m_1 \dots m_k$ into the state $|m_i\rangle$ of the corresponding qubit. Then, she randomly chooses a bit value a, and for each m_i a rotation angle φ_i (taken from a given set of angles Φ), and rotates $|m_i\rangle$ by $(-1)^a \varphi_i$. Finalizing the transferring phase, she sends the qubits to Bob. Note that for each qubit i the encoding quantum states

$$|0_i^{(a)}\rangle = R((-1)^a \varphi_i) |0\rangle$$
$$|1_i^{(a)}\rangle = R((-1)^a \varphi_i) |1\rangle = R(\pi) |0_i^{(a)}\rangle ,$$

where rotations R are defined by $R(\varphi) |0\rangle = \cos(\varphi/2) |0\rangle + i \sin(\varphi/2) |1\rangle$, are mutually orthogonal and hence fully distinguishable, provided one knows the direction a and the angle φ_i of the rotation. Therefore, Bob cannot decipher the message m, unless given additional information about the encoding bases $\beta_i = \{|0_i^{(a)}\rangle, |1_i^{(a)}\rangle\}$. In Figure 2 we present a schematic description with $l = k$.

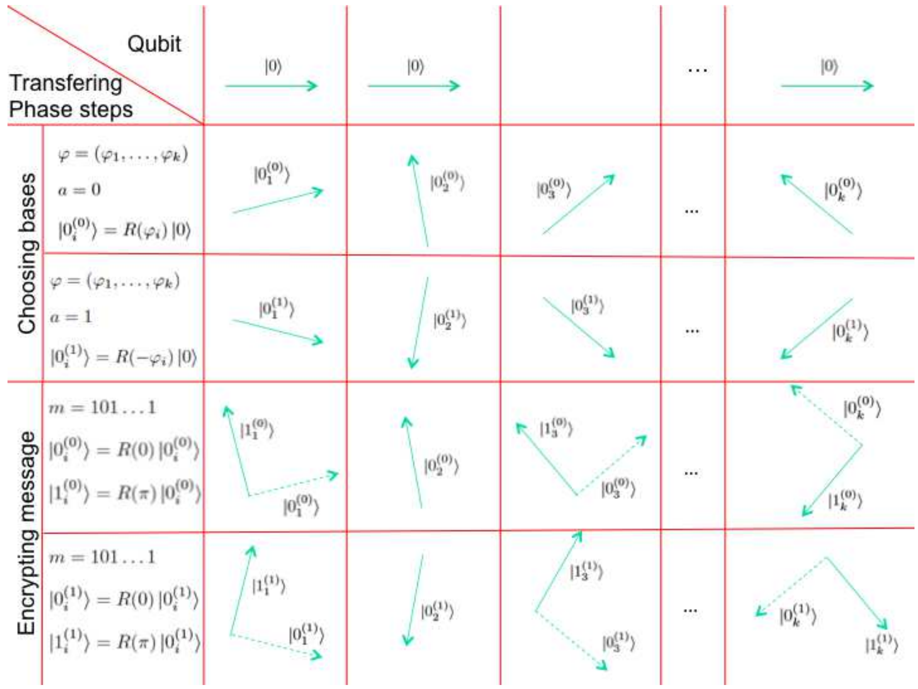

Figure 2: Schematic description of the transferring phase of our oblivious transfer protocol for $l = k$. The full arrows represent the actual states of qubits, while the dashed arrows in the last two lines (encryption of a message) represent $|0_i\rangle$ states.

In the opening phase, Alice provides Bob with such (partial) information: she sends the so-called secret key, a string $\varphi = (\varphi_1, \ldots, \varphi_k)$ of rotation angles, but *not* the rotation direction a. Oblivious to the rotation direction, Bob can only guess it, which he will get correctly in 50% of the cases.

Together with the message m, Alice sends its digest $d = h(m)$, given by a suitable chosen hash function h. Upon receiving (m', d'), Bob checks if $d' = h(m')$. If so, he is convinced that the received message m' is indeed the intended message m (for technical details, see Section 3).

Below, we present a rigorous description of our bit-string OT protocol, where $\varphi_i = s_i\theta_n$.

Protocol 2.1 (Bit-string OT)**.**

> **Message to transfer** $m = m_1 \ldots m_k$*;*
>
> **Security parameter** $n, \theta_n = \pi/2^{n-1}$ *and a hash function* $h : \{0,1\}^k \to \{0,1\}^{k/2}$*;*
>
> **Secret key** $s = (s_1, \ldots, s_{3k/2})$*, where each* $s_i \in \{0, \ldots, 2^n - 1\}$.

Transferring phase:

1. *Alice chooses uniformly at random a bit* $a \in \{0,1\}$ *and prepares the following state:*

$$
\begin{aligned}
|\psi\rangle = & \bigotimes_{i=1}^{k} R(m_i\pi + (-1)^a \times s_i\theta_n)\,|0\rangle \bigotimes_{i=1}^{k/2} R(h_i(m)\pi + (-1)^a \times s_{i+k}\theta_n)\,|0\rangle \\
= & \left(\bigotimes_{i=1}^{n}\left[\cos\left(\frac{m_i\pi + (-1)^a \times s_i\theta_n}{2}\right)|0\rangle + \sin\left(\frac{m_i\pi + (-1)^a \times s_i\theta_n}{2}\right)|1\rangle\right]\right) \otimes \\
& \left(\bigotimes_{i=1}^{k/2}\left[\cos\left(\frac{h_i(m)\pi + (-1)^a \times s_{i+k}\theta_n}{2}\right)|0\rangle + \sin\left(\frac{h(m)_i\pi + (-1)^a \times s_{i+k}\theta_n}{2}\right)|1\rangle\right]\right)
\end{aligned}
$$

(Note that $h_i(m)$ *represents the* i^{th} *bit of the binary string* $h(m)$*).*

2. *Alice sends the state* $|\psi\rangle$ *to Bob.*

Opening phase:

3. *Alice sends* $s = (s_1, \ldots, s_{3k/2})$ *and* n *to Bob.*
4. *Bob checks if* s *is likely to be a possible output of a random process. [By encoding* s_i*'s into binary numbers Alice has to provide an* $n \times 3k/2$ *long bit-string produced a fair coin. A number of possible tests of random-number generators exist in literature, such as* χ^2*, Kolmogorov-Smirnov, Serial correlation, Two-level, K-distributivity, Serial and Spectral tests (for more details, see [Jai91], Chapter* 27*).]*
5. *Bob chooses uniformly at random* $a' \in \{0,1\}$ *and applies* $R((-1)^{a'} s_i\theta_n)$ *to each qubit of* $|\psi\rangle$*.*
6. *Bob applies the measurement operator* $M^{\otimes 3k/2} = (0 \times |0\rangle\langle 0| + 1 \times |1\rangle\langle 1|)^{\otimes 3k/2}$*.*
7. *Let* $m' \cdot h'$ *be the message that Bob recovers. He checks if* $h' = h(m')$*. If that is the case then Bob is almost sure that* $m' = m$*, otherwise he knows that* m' *is not the correct message.*

Notice that knowing $h(m)$ can potentially reveal the whole set A_m of the strings mapped to the same value of hash. Knowing A_m decreases Bob's uncertainty about the unknown string m, thus effectively revealing $k/2$ bits of information about string m. This information may help Bob to increase the probability of finding m, thus compromising the security of the protocol. Therefore we encrypt both the message m and $h(m)$ into a quantum state sent by Alice. Since, in order to confirm that he obtained the message m, Bob needs to learn the value $h(m)$ as well, one can consider the pair $(m, h(m))$ as a message to be transferred. For simplicity, in the rest of the paper we will denote the pair $(m, h(m))$ as a single message m to be transferred.

Finally, we present a simple way of using our protocol to achieve oblivious transfer of a single bit b by sending a bit-string message m with parity b.

Protocol 2.2 (Single-bit oblivious transfer)**.**

> **Message to transfer** *b;*
>
> **Security parameter** *n;*
>
> 1. *Alice chooses bit b.*
> 2. *Alice chooses an n-bit message m, such that $\bigoplus_{i=1}^{n} m_i = b$.*
> 3. *Alice and Bob perform protocol 2.1.*
> 4. *If Bob had got the right message m, then he performs $\bigoplus_{i=1}^{n} m_i = b$. Otherwise, he cannot recover the bit.*

3 Methods

In this section we prove the security of our oblivious transfer protocol. Oblivious transfer has to satisfy the following three properties:

Soundness If both Alice and Bob are honest, then with probability 1/2 Bob will obtain the right message. Bob knows if he got the right message or not;

Concealingness If Alice is honest Bob cannot learn the content of the message that Alice meant to send before the opening phase (the protocol is concealing). Furthermore, after the opening phase, Bob cannot learn the message in more than 50% of the cases.

Obliviousness If Bob is honest then Alice does not know if Bob received the message – she can only guess with probability 1/2 (the protocol is oblivious).

In our case, the probability of the soundness and concealingness properties is relaxed to $1/2+\varepsilon(k)$, where k is some fixed security parameter and $\varepsilon : \mathbb{N} \to \mathbb{R}$ is a negligible function, i.e., for every positive polynomial p there exists a $k_0 \in \mathbb{N}$ such that for all $k > k_0$, $\varepsilon(k) \leq 1/p(k)$.

Soundness of the protocol

In the following we prove the soundness of our protocol: if both parties are honest, then with probability $1/2 + \varepsilon(k)$ Bob will get the right message, where $\varepsilon(k)$ is negligible function on the size of the message $m = m_1 \dots m_k$.

First assume that Alice and Bob had chosen to rotate the state in opposite directions, i.e., $a \neq a'$. Without loss of generality assume that Alice chooses

$a = 0$, to rotate clockwise all the qubits. The qubits Alice sent to Bob are in the following state:

$$\begin{aligned} |\psi\rangle &= \bigotimes_{i=1}^{k} R(m_i\pi + s_i\theta_n)\,|0\rangle \\ &= \bigotimes_{i=1}^{k} \cos\left(\frac{m_i\pi + s_i\theta_n}{2}\right)|0\rangle + \sin\left(\frac{m_i\pi + s_i\theta_n}{2}\right)|1\rangle\,. \end{aligned}$$

In the opening phase Bob receives from Alice the additional information, the secret key $s = (s_1, \ldots, s_k)$.

By the assumption, Bob decides to rotate each qubit received from Alice counterclockwise ($a' = 1$) by $-s_i\theta_n$. The states he gets are either $|0\rangle$ or $|1\rangle$:

$$\begin{aligned} R(-s_i\theta_n)(R(m_i\pi + s_i\theta_n)\,|0\rangle) &= R(m_i\pi)\,|0\rangle \\ &= \cos\left(\frac{m_i\pi}{2}\right)|0\rangle + \sin\left(\frac{m_i\pi}{2}\right)|1\rangle \\ &= |m_i\rangle\,. \end{aligned}$$

Bob measures M on the above state and the result is m_i with probability 1. We conclude that if Bob chooses to rotate in the direction contrarily to Alice's choice, then with probability 1 Bob will recover the bit sent by Alice.

On the other hand, if Alice and Bob decide to rotate each qubit of the message in the same direction ($a = a'$), say clockwise, the qubits' states are transformed into ($i = 1 \ldots k$):

$$\begin{aligned} R(s_i\theta_n)(R(m_i\pi + s_i\theta_n)\,|0\rangle) = &\; R(m_i\pi + 2s_i\theta_n)\,|0\rangle) \\ = &\; \cos\left(\frac{2s_i\theta_n + m_i\pi}{2}\right)|0\rangle + \sin\left(\frac{2s_i\theta_n + m_i\pi}{2}\right)|1\rangle \\ = &\; |\tilde{m}_i\rangle\,. \end{aligned}$$

If $m_i = 0$ then the above state becomes $|\tilde{m}_i\rangle = \cos(s_i\theta_n)\,|0\rangle + \sin(s_i\theta_n)\,|1\rangle$ and by measuring M Bob gets the correct answer with probability $\cos^2(s_i\theta_n)$; if $m_i = 1$ then the above state becomes $|\tilde{m}_i\rangle = -\sin(s_i\theta_n)\,|0\rangle + \cos(s_i\theta_n)\,|1\rangle$ and again Bob gets the correct bit with probability $\cos^2(s_i\theta_n)$. Hence

$$\Pr(m_i; M, |\tilde{m}_i\rangle) = \cos^2(s_i\theta_n).$$

Assuming that the key s is chosen at random, the probability of recovering the whole message by rotating in the wrong direction becomes negligible, and the expected probability of recovering message m when measuring $M^{\otimes k}$ on the state $|\psi'\rangle = \bigotimes_{i=1}^{k} R((-1)^{a'} s_i\theta_n)\,|\psi\rangle$ is:

$$\begin{aligned} \Pr(\mathrm{m}; M^{\otimes k}, |\psi'\rangle) &= \Pr(a' \neq a) \times \Pr(m|a' \neq a) + \Pr(a' = a) \times \Pr(m|a' = a) \\ &\leq \frac{1}{2} + \frac{1}{2}\prod_{i=1}^{k}\cos^2(s_i\theta_n). \end{aligned}$$

Clearly, when Alice chooses the values s_i at random, the expected probability of Bob recovering the message m in case Alice and Bob perform equal rotations becomes negligible, i.e., $\varepsilon(k) = \frac{1}{2}\prod_{i=1}^{k}\cos^2(s_i\theta_n)$ is negligible. To see that, notice that on average half of values for the rotation angles $s_i\theta_n/2$ fall in the interval $[\pi/4; 3\pi/4]$, giving the upper bound $\varepsilon(k) \leq 2^{-k/2}$.

The information received by Bob consists of two parts: one corresponding to the actual message sent by Alice, and the other corresponding to its hash value. At the end of the protocol, Bob checks if he recovered the correct message by comparing its hash value with the latter part of information received. Note that by the properties of universal hash functions, the probability that the hash of the first part matches the second one is negligible in the case Alice and Bob performed the same rotation (see Appendix for more detailed description of the properties of hash functions).

Concealingness of the protocol

In this subsection we show that if Alice is honest, the probability of Bob recovering Alice's message before the opening phase is negligible. Furthermore, after the opening phase Bob recovers the message with, up to a negligible value, probability 1/2.

The first part of the statement follows directly from the security of the public key crypto system [Nik08] (see the discussion on one-way functions and state distinguishability in the Appendix), and is basically a consequence of the fact that, from Bob's point of view, without knowing the key s and the rotation direction a, each message m is described by the same mixed state – a complete mixture.

After receiving the secret key s, qubits received from Alice are in the following mixed state (for convenience, in the following we consider $a \in \{+,-\}$, where "+" stands for clockwise rotation and "−" otherwise):

$$\rho_B(s) = \frac{1}{2}\sum_{a\in\{+,-\}}\left(\frac{1}{2}\right)^k \sum_{m_1\in\{0,1\}}\ldots\sum_{m_k\in\{0,1\}} |m_1(s_1)\rangle_a\langle m_1(s_1)|\otimes\ldots\otimes|m_k(s_k)\rangle_a\langle m_k(s_k)|\,,$$

where $|m_i(s_i)\rangle_\pm = \cos\left(\frac{m_i\pi}{2} \pm \frac{s_i\theta_n}{2}\right)|0\rangle + \sin\left(\frac{m_i\pi}{2} \pm \frac{s_i\theta_n}{2}\right)|1\rangle$. Note that $\rho_B(s)$ can be written as a tensor product of single-qubit states $\rho_B(s_i) = \frac{1}{2}(\rho_0(s_i) + \rho_1(s_i))$, where $\rho_{m_i}(s_i) = \frac{1}{2}(|m_i(s_i)\rangle_+\langle m_i(s_i)| + |m_i(s_i)\rangle_-\langle m_i(s_i)|)$. The optimal probability of guessing bit's value m_i is then given by the Helstrom formula [Hel69]:

$$\mathrm{P}_H(\rho_0(s_i), \rho_1(s_i)) = \frac{1}{2} + \frac{1}{4}\mathrm{Tr}|\rho_0(s_i) - \rho_1(s_i)| = \frac{1}{2}(1 + |\cos(s_i\theta_n)|).$$

Analogously to the proof of soundness of the protocol, averaging over all possible keys s we see that the expected value of obtaining the message is negligible.

Therefore, the only way for Bob to recover the message m is to follow the protocol and choose direction a' at random, in which case he obtains m with probability 1/2. Note that Bob cannot guess rotation direction a with probability bigger than 1/2, as the mixed states corresponding to either direction are completely indistinguishable. Indeed a single-qubit state can be written as $\rho_B(s_i) = \frac{1}{2}(\rho_+(s_i) + \rho_-(s_i))$, where $\rho_\pm(s_i) = \frac{1}{2}(|0(s_i)\rangle_\pm\langle 0(s_i)| + |1(s_i)\rangle_\pm\langle 1(s_i)|) = \mathbb{1}/2$.

The above proof is valid for single qubit measurement of a cheating Bob. We conjecture that the protocol is secure against multi-qubit measurements as well. Indeed, if Bob were able to, using coherent multi-qubit measurements, learn the message sent by Alice, then for sufficiently large n he would be able to distinguish virtually any two quantum states.

Obliviousness of the protocol

To finish the security discussion we prove that the protocol is unconditionally oblivious: at the end of the protocol Alice does not know whether Bob received the right message of not.

At the end of the protocol, since Bob performs local operations and measurements, Alice has no way of knowing if Bob had chosen the right rotation, or not. Therefore, if being honest and sending the state prescribed by the Protocol, Alice cannot know if an honest Bob received the message or not. Therefore, to be able to know with certainty if Bob recovered the message or not, while maintaining the 50% of Bob's success, a cheating Alice can only use the following strategy: in 50% of the cases she sends a cheating state $|\psi_{ch}\rangle$ that would reveal m independently of Bob's choice of rotation, and in the remaining cases she sends a completely random state.

Nevertheless, if Alice is dishonest and wants to ensure that an honest Bob would get the message by sending $|\psi_{ch}\rangle$, her probability to do so without being noticed will be exponentially close, with respect to the message length k, to 1/2. Below, we give an upper bound to the mentioned probability.

Let l be the number of s_i's for which $\varphi_i = s_i\theta_n \in [\pi/8; 3\pi/8]$. For such cases we can consider the rearranged secret key $s = s_1 \dots s_l$ and the corresponding message $m = m_1 \dots m_l$. Depending on his choice of rotation direction a' Bob will measure one of the two observables $C_\pm(s) = \sum_{m=0}^{2^l-1} m \cdot P_\pm(m; s)$, where one-dimensional projectors are given by $P_\pm(m; s) = \bigotimes_{i=0}^{l} P_\pm(m_i; s_i) = \bigotimes_{i=0}^{l} |m_i(s_i)\rangle_\pm\langle m_i(s_i)|$.

For given m and s Alice wants to maximize the probability Pr_{ch} of Bob obtaining m measuring $C_\pm(s)$ on $|\psi_{ch}\rangle$, given by

$$\mathrm{Pr}_{ch} = \frac{1}{2}\left(||P_+(s)\,|\psi_{ch}\rangle\,||^2 + ||P_-(s)\,|\psi_{ch}\rangle\,||^2\right).$$

From triangle inequality of the trace distance $D(|\phi\rangle, |\psi\rangle) = \sqrt{1 - |\langle\phi|\psi\rangle|^2}$, we have ($|\pm\rangle = \bigotimes_{i=0}^{l} |m_i(s_i)\rangle_\pm$):

$$\mathrm{Pr}_{ch} \le \frac{1}{2}\left(1 + |\langle +|-\rangle|^2\right) \le \frac{1}{2}\left(1 + \cos^{2l}(\pi/8)\right).$$

If the values s_i were produced uniformly at random, then the probability that $\varphi_i = s_i\theta_n \in [\pi/8; 3\pi/8]$ is 1/4. As a consequence, the random variable that counts the number l of such φ_i's follow the binomial distribution $\mathcal{B}(k, 1/4)$, with k being the number of trials (the length of the total message m) and mean equal to 1/4. For sufficiently large k, it can be approximated by the normal distribution $\mathcal{N}(\mu, \sigma^2)$ with the mean $\mu = k/4$ and the variance $\sigma^2 = k/16$. Therefore, in $\Pr[(k - 3\sqrt{k})/4 \leq l \leq (k + 3\sqrt{k})/4] = 99.8\%$ of the cases Alice's probability to learn if Bob got the message or not will be $\Pr_{ch} = 1/2 + \varepsilon(k)$, where $\varepsilon(k)$ is negligible.

4 Discussion

In this paper we proposed a novel scheme for obliviously transferring a bit-string message from Alice to Bob. The scheme presented does not violate the Lo's no-go theorem [Lo97] and its security is based on the laws of quantum physics.

We proved that the protocol is unconditionally secure against *any* cheating strategy of Alice (it is unconditionally oblivious). Furthermore, we proved that it is unconditionally concealing, provided Bob performs only single-qubit measurements. Although intuitively our protocol should, at least for sufficiently large n, be secure against multi-qubit measurements, a detailed analysis of its security against Bob's coherent attacks remains to be done (similarly as for the case of recently proposed and performed quantum signatures protocol [DWA14, CDD$^+$14]).

Our protocol does not use entanglement and its optical implementation could be performed using today's technology.

Finally we discuss the need for the use of hash functions. Recall that at the end of the protocol Bob must be sure if he got the intended message or not. This property is guaranteed by comparing the computed hash value of the received message m with the presumed hash value sent by Alice together with m. Such acknowledgment of the validity of the message decoded by Bob could be done differently. Suppose that out of all possible messages (PM), Alice is constrained to send m from a smaller set of messages (VM), such that verifying that m is in VM can be easily done, but only Alice knows the elements of VM. Note that in order to keep the probability of receiving a message from Alice to 1/2, up to a negligible term, the size of VM must be exponentially smaller than the size of PM. For example, VM could be the set of solutions to a hard mathematical problem, say 3-SAT problem. Alternatively, the message sent might be written in an existing human language, say English, making it easily recognizable by any English-language speaker.

Future lines of research include formulating other quantum security protocols that use single-qubit rotations to encode bit values into quantum states taken from a number of different bases. One such immediate application is in designing a quantum bit-string commitment protocol and compare it with the existing proposals. Furthermore, similarly when generating (randomized) secret keys, single-qubit rotations could be used in creating undeniable signatures.

Acknowledgments

This work was partially supported by FCT projects PEst-OE/EEI/LA0008/2013 and ComFormCrypt PTDC/EIA-CCO/113033/2009, SQIG's initiative PQDR (Probabilistic, Quantum and Differential Reasoning) and IT project PQantum, as well as Network of Excellence, Euro-NF. João Rodrigues and André Souto also acknowledge respectively the FCT grants SFRH / BD / 75085 / 2010 and SFRH / BPD / 76231 / 2011.

Appendix

Here, we provide notation, necessary definitions and results for defining and proving the security of our proposal. First, we give the definition of *quantum one-way functions*, based on [LF05, Nik08].

A *quantum one-way function* is a map $f : N \to \mathcal{H}$, where $N \subset \mathbb{Z}$ and $\mathcal{H}$ is a Hilbert space, such that:

1. f is easy to compute: there is a polynomial-time (in the number of bits of the input s) quantum algorithm that computes $f(s) \in \mathcal{H}$, with $s \in N$;

2. Hard to invert: without any additional information, inverting $f(s)$ in polynomial time on the input size is impossible by fundamental physical laws of quantum (information) theory.

If inversion is computed in polynomial-time using some additional information, called the trapdoor, then f is called a *trapdoor quantum one-way function.* In a sense, the trapdoor is a "key" to unlock the input s.

One of the most relevant quantities used in Information Theory is the *mutual information* between two random variables X and Y, denoted by $I(X : Y)$, which quantifies the amount of correlations between X and Y, and is defined by

$$I(X : Y) = H(X) + H(Y) - H(X, Y),$$

where H is the well known Shannon entropy. Notice that $I(X : Y)$ is a symmetric function with respect to X and Y. Mutual information is useful in evaluating various features of information processing protocols. For example, it is used to quantify the effects of noise in the transmission process: how much information about the original message, given by random source X, is contained in the received message distorted by noise, given by the random variable Y.

Another application is in quantifying the efficiency of a decryption process: how much information about the encrypted message, given by a random source X, is contained in the decrypted message, given by random variable Y. If each letter $i \in \{1, \ldots, n\}$ of a random variable X is encrypted in a quantum state ρ_i, then the maximal amount of information that a receiver can obtain about

X is called the *accessible information* and is quantified by $I(X:Y)$, where Y is the random variable corresponding to the results of the optimal measurement performed on received states ρ_i.

The Holevo bound provides an upper bound on the accessible information.

Let $\{\rho_1, \dots, \rho_n\}$ be a set of mixed states and let ρ_X be one of the states drawn according to the probability distribution $P = \{p_1, \dots, p_n\}$. Then, for any measurement, described by POVM elements $\{E_Y\}$, performed on ρ_X, the amount of accessible information $I(X:Y)$ about the variable X, knowing the outcome Y of the measurement, is upper bounded by

$$I(X:Y) \leq S(\rho) - \sum_i p_i S(\rho_i),$$

where $\rho = \sum_i p_i \rho_i$ and S is the von Neumann entropy.

An immediate consequence of this result is that a qubit cannot carry more than one bit of classical information.

There are several candidates for quantum one-way functions studied in [GC01, BCWW01] (a slightly different variation of quantum one-way function, with input being quantum as well, was considered in [LF05]). Recently, another candidate for a quantum one-way function was proposed in [Nik08]. This function considers qubit rotations R and is given by

$$f(s) = R(s\theta_n) |0\rangle = \cos(s\theta_n/2) |0\rangle + \sin(s\theta_n/2) |1\rangle$$

where $s \in \{0, \dots, 2^n - 1\}$ and $\theta_n = \pi/2^{n-1}$, for some fixed n, and $\{|0\rangle, |1\rangle\}$ is a fixed computational basis (i.e., f is not a function of a quantum state). Notice that this is a quantum one-way function because:

- Qubit rotations $R(s\theta_n)$ can be easily implemented up to an arbitrary accuracy by a quantum algorithm involving a universal set of gates ([NC04], [Nik08]).
- Due to Holevo bound, the maximal amount of information that can be extracted by means of a POVM on a single qubit is 1 bit. Since s has n bits, it is impossible to recover s from a single qubit in the state $R(s\theta_n)|0\rangle$.

Moreover, f can be used to construct a quantum trapdoor one-way function $F(s, b)$, where s is the trapdoor information for learning an unknown bit b [Nik08]:

$$F(s, b) = R(b\pi) f(s) = R(b\pi) R(s\theta_n) |0\rangle = R(s\theta_n + b\pi) |0\rangle .$$

Note that inverting F (learning both s and b) is at least as hard as inverting f. Also, the ensemble of qubits, each in a state $F(s_i, b_i)$, where s_i and b_i are random, is described by a complete mixture $\rho = \mathbb{1}/2$, if s_i and b_i are unknown [Nik08]. Therefore, every binary measurement that could be used to infer unknown bit b would give completely random value. Nevertheless, if s is known, by applying the rotation $R(-s\theta_n)$ to $F(s, b)$ and measuring the result in the computational basis, one obtains b with certainty. Therefore, $F(s,b)$ is a polynomial quantum trapdoor one-way function.

Based on the above discussion, we present the secure public key cryptographic protocol proposed in [Nik08]:

Protocol 4.1 (Public Key Encryption Scheme)**.**

Message to transfer $m = m_1 \dots m_l$ *with* $l \le k$*;*

Security parameter n*;*

Secret key $s = (s_1, \dots, s_k)$*, where each* $s_i \in \{0, \dots, 2^n - 1\}$*;*

Public Key Generation:

1. *For all* $1 \le i \le k$*, Alice chooses uniformly at random* $s_i \in \{0, \dots, 2^n - 1\}$*, and* $s = (s_1, \dots, s_k)$ *will be her private key.*
2. *Alice generates the corresponding public key:*

$$\begin{aligned} |\psi\rangle &= \bigotimes_{i=1}^{k} R(s_i\theta_n)\,|0\rangle \\ &= \bigotimes_{i=1}^{k} \left(\cos\left(\frac{s_i\theta_n}{2}\right)|0\rangle + \sin\left(\frac{s_i\theta_n}{2}\right)|1\rangle \right). \end{aligned}$$

Encryption:

3. *Bob wishes to send message* $m = m_1, \dots m_l$ *where* $l \le k$*.*
4. *Bob obtains Alice's public key,* $|\psi\rangle$*.*
5. *Bob encrypts his message* m *(padded with* 0 *if necessary) as follows*

$$\begin{aligned} |\psi(m)\rangle &= \bigotimes_{i=1}^{k} R(m_i\pi)\,|\psi\rangle \\ &= \bigotimes_{i=1}^{k} \left(\cos\left(\frac{s_i\theta_n}{2} + \frac{m_i\pi}{2}\right)|0\rangle + \sin\left(\frac{s_i\theta_n}{2} + \frac{m_i\pi}{2}\right)|1\rangle \right). \end{aligned}$$

6. *Bob sends* $|\psi(m)\rangle$ *to Alice.*

Decryption:

7. *Alice uses private key as follows*

$$\begin{aligned} |\psi'(m)\rangle &= \bigotimes_{i=1}^{k} R(-s_i\theta_n)\,|\psi(m)\rangle \\ &= \bigotimes_{i=1}^{k} \left(\cos\left(\frac{m_i\pi}{2}\right)|0\rangle + \sin\left(\frac{m_i\pi}{2}\right)|1\rangle \right) \\ &= \bigotimes_{i=1}^{k} |m_i\rangle\,. \end{aligned}$$

8. *Alice performs measurements on each $|m_i\rangle$ in the computational basis.*

Obviously, the Public Key Generation corresponds to computation of $f(s)$, the Encryption phase computes $F(s, b)$ and the Decryption phase corresponds to inversion of $F(s, b)$ with the trapdoor information s, which allows to learn message m. Therefore Protocol 4.1 is secure. In Figure 3 we present a schematic description of the public key cryptosystem.

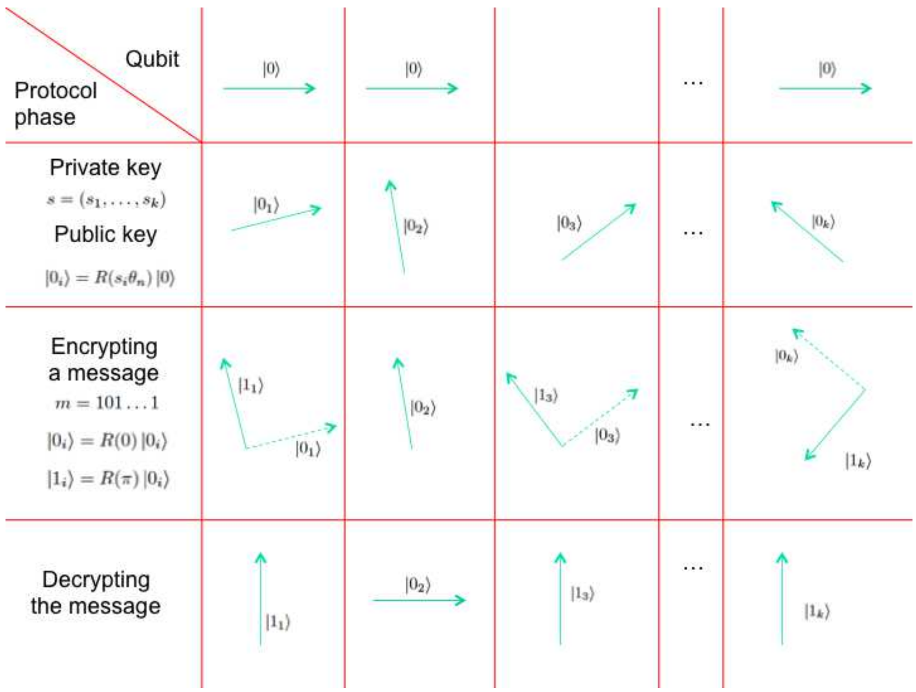

Figure 3: Schematic description of the public key cryptosystem for $l = k$. The full arrows represent the actual states of qubits, while the dashed arrows in the third line (encryption of a message) represent $|0_i\rangle$ states.

At the end of the Oblivious transfer protocol, Bob has to be assured of the fact that he received the message or not. There are different ways to guarantee this feature. The solution adopted in this paper is to use a *universal hash function*. A hash function maps strings to other strings of smaller size. Therefore, different strings are mapped to the same hash value. Hash functions have to satisfy the following two constrains,

- their value can be computed in polynomial time on the length of the input string;
- The hash values of a randomly chosen string are uniformly distributed.

Consider two sets A and B of size a and b, respectively, such that $a > b$, and consider a collection $\mathbb{H}$ of hash functions $h : A \to B$. If

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

then $\mathbb{H}$ is called a *universal family of hash functions*. From the above definition, it is easy to derive that the size of a set A_x of strings $x \in A$ mapped to the same hash value $h(x)$ is at most N/b.

In particular, requiring that A contains all strings of length ℓ and B to be a set of strings of length $\ell/2$, the number of strings with the same hash value is $2^{\ell/2}$, hence the probability of finding such a string is negligible in ℓ. For more details on constructing universal families of hash functions, see for example [CW79].

References

[BB84] 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.

[BBCS92] C. Bennett, G. Brassard, C. Crépeau, and M. Skubiszewska. Practical quantum oblivious transfer. In Joan Feigenbaum, editor, *Advances in Cryptology CRYPTO'91*, volume 576 of *Lecture Notes in Computer Science*, pages 351–366. Springer Berlin Heidelberg, 1992.

[BCC88] G. Brassard, D. Chaum, and C. Crépeau. Minimum disclosure proofs of knowledge. *J. Comput. Syst. Sci.*, 37(2):156–189, October 1988.

[BCR86] 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.

[BCS96] G. Brassard, C. Crepeau, and M. Santha. Oblivious transfers and intersecting codes. *Information Theory, IEEE Transactions on*, 42(6):1769–1780, Nov 1996.

[BCWW01] H. Buhrman, R. Cleve, J. Watrous, and R. De Wolf. Quantum fingerprinting. *Physical Review Letters*, 87:2001, 2001.

[Ben92] Charles H. Bennett. Quantum cryptography using any two nonorthogonal states. *Phys. Rev. Lett.*, 68:3121–3124, May 1992.

[BFGGS13] 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.

[BM04] J. Barrett and S. Massar. Security of quantum bit-string generation. *Phys. Rev. A*, 70:052310, Nov 2004.

[CDD+14] 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.

[CDM00] 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.

[Cré88] C. Crépeau. Equivalence between two flavours of oblivious transfers. In *A Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology*, CRYPTO '87, pages 350–354, London, UK, UK, 1988. Springer-Verlag.

[CS93] 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.

[CW79] J. Carter and M. Wegman. Universal classes of hash functions. *J. Comput. Syst. Sci.*, 18(2):143–154, 1979.

[DWA14] V. Dunjko, P. Wallden, and E. Andersson. Quantum digital signatures without quantum memory. *Phys. Rev. Lett.*, 112:040502, Jan 2014.

[EGL85] S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. *Commun. ACM*, 28(6):637–647, 1985.

[Eke91] Artur K. Ekert. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.*, 67:661–663, Aug 1991.

[GC01] D. Gottesman and I. Chuang. Quantum digital signatures. Technical report, 2001.

[Hel69] C. Helstrom. Quantum detection and estimation theory. *Journal of Statistical Physics*, 1(2):231–252, 1969.

[HL93] 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 - ASIACRYPT '91*, volume 739 of *Lecture Notes in Computer Science*, pages 312–320. Springer Berlin Heidelberg, 1993.

[HW06a] 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.

[HW06b] G. P. He and Z. D. Wang. Oblivious transfer using quantum entanglement. *Phys. Rev. A*, 73:012331, Jan 2006.

[Jai91] R. Jain. *The art of computer systems performance analysis - techniques for experimental design, measurement, simulation, and modeling.* Wiley professional computing. Wiley, 1991.

[Ken99] A. Kent. Unconditionally secure bit commitment. *Phys. Rev. Lett.*, 83:1447–1450, Aug 1999.

[Ken03] A. Kent. Quantum bit string commitment. *Physical Review Letters*, 90:237901, Jun 2003.

[Ken05] A. Kent. Secure classical bit commitment using fixed capacity communication channels. *J. Cryptology*, 18(4):313–335, 2005.

[Kil88] 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.

[KWW12] R. Koenig, S. Wehner, and J. Wullschleger. Unconditional security from noisy quantum storage. *IEEE Transactions on Information Theory*, 58(3):1962–1984, 2012.

[LAA$^+$] 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. *Accepted for publication in Phys. Rev. A.*

[LC96] H. Lo and H. Chau. Is quantum bit commitment really possible? *CoRR*, quant-ph/9603004, 1996.

[LC97] H. K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Phys. Rev. Lett.*, 78:3410–3413, Apr 1997.

[LC99] H. K. Lo and H. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283(5410):2050–2056, 1999.

[LF05] X. Lu and D. Feng. Quantum digital signature based on quantum one-way functions. In *Advanced Communication Technology, 2005, ICACT 2005. The 7th International Conference on*, volume 1, pages 514–517, 2005.

[Lo97] H. K. Lo. Insecurity of quantum secure computations. *Phys. Rev. A*, 56:1154–1162, Aug 1997.

[LP12] Y. Lindell and B. Pinkas. Secure two-party computation via cut-and-choose oblivious transfer. *J. Cryptology*, 25(4):680–722, 2012.

[LZ13] Y. Lindell and H. Zarosim. On the feasibility of extending oblivious transfer. In *TCC*, pages 519–538, 2013.

[May97] D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Physycal Review Letters*, page 3414, 1997.

[May01] D. Mayers. Unconditional security in quantum cryptography. *J. ACM*, 48(3):351–406, May 2001.

[NC04] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information (Cambridge Series on Information and the Natural Sciences)*. Cambridge University Press, 1 edition, January 2004.

[Nik08] G. Nikolopoulos. Applications of single-qubit rotations in quantum public-key cryptography. *Phys. Rev. A*, 77:032348, Mar 2008.

[NJM+12] 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.

[PBM11] N. Paunković, J. Bouda, and P. Mateus. Fair and optimistic quantum contract signing. *Physical Review A*, 84(6):062331–062331, December 2011.

[Rab81] M. Rabin. How to exchange secrets by oblivious transfer, 1981.

[Sal98] L. Salvail. The search for the holy grail in quantum cryptography. In *Lectures on Data Security*, pages 183–216, 1998.

[SBPC+09] 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.

[SMAaP] A. Souto, P. Mateus, P. Adão, and N. Paunković. Bit-string oblivious transfer based on quantum state computational distinguishability. *Submitted to Phys. Rev. Lett.*

[SP00] 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.

[STW11] C. Schaffner, B. M. Terhal, and S. Wehner. Robust cryptography in the noisy-quantum-storage model. *Quantum Information & Computation*, 9(11):963–996, 2011.

[Wie83] S. Wiesner. Conjugate coding. *SIGACT News*, 15(1):78–88, January 1983.

[WST08] S. Wehner, C. Schaffner, and B. M. Terhal. Cryptography from noisy storage. *Phys. Rev. Lett.*, 100:220502, Jun 2008.

[Yao86] A. Yao. How to generate and exchange secrets. In *Proceedings of the 27th Annual Symposium on Foundations of Computer Science*, SFCS '86, pages 162–167, Washington, DC, USA, 1986. IEEE Computer Society.