Implementation of a Two-State Quantum Bit Commitment Protocol in Optical Fibers

Á J Almeida[1,2], A D Stojanovic[3], N Paunković[4,5], R Loura[4,5]
N J Muga[6,2], N A Silva[6,2], P Mateus[4,5], P S André[7,2] and A N Pinto[6,2]

November 20, 2015

Abstract

We demonstrate experimentally the feasibility of a two-state quantum bit commitment protocol, which is both concealing and partially binding, assuming technological limitations. The security of this protocol is based on the lack of long-term stable quantum memories. We use a polarization-encoding scheme and optical fiber as a quantum channel. The measurement probability for the commitment is obtained and the optimal cheating strategy demonstrated. The average success rates for an honest player in the case where the measurements are performed using equal bases are 93.4%, when the rectilinear basis is measured, and 96.7%, when the diagonal basis is measured. The rates for the case when the measurements are performed in different bases are 52.9%, when the rectilinear basis is measured, and 55.4% when the diagonal basis is measured. The average success rates for the optimal cheating strategy are 80% and 73.8%, which are way below the success rates of an honest player. Using a strict numerical validity criterion, we show that, for these experimental values, the protocol is secure.

1 Introduction

Recently, there has been a strong effort to develop quantum primitives, which are designed to change classical cryptographic protocols to their quantum generalizations. One group of these primitives are quantum-based two-party computation protocols, such as the bit commitment (BC) scheme. We demonstrate the practical feasibility of a two-state quantum-bit commitment (QBC) scheme [24] based on the B92 [4] cryptographic protocol, making use of technological limitations.

Regarding current trends in cryptography and information security, QBC is believed to have higher potential than BC [39]. Unfortunately, not even the laws of quantum mechanics allow us to realize all desirable cryptographic functionalities without further assumptions. One of the most noticeable results showed that non-relativistic QBC cannot be unconditionally secure, due to the EPR attack [23, 28]. Since then, the scientific work on QBC has been divided into theoretical and experimental. Regarding theoretical work, most attempts have been focused on evading the no-go theorem [3]. One of the first attempts extended its proof to cover ideal quantum coin tossing [22]. More complicated examples on how to apply the no-go proof to break some quantum as well as classical BC protocols which looked promising at that time were provided in [6]. Reference [34] further studied the security bounds of QBC quantitatively. Recent efforts proved the no-go theorem with alternative methods [8,20]. Although some results are obtained in favor of QBC, until now the no-go theorem has been well-accepted in quantum cryptographic community and there has been an effort to build a secure QBC under various settings [7, 18]. These impossibility results rule out the ability to build perfect cryptographic primitives. However, it could be possible to build QBC which is almost perfect. Aharonov first showed how to construct imperfect QBC with cheating probabilities smaller than 0.9143 [1]. The best protocol was due to Ambainis who constructed a QBC scheme (and a quantum coin flipping protocol) where no player can cheat with probability greater than 3/4 [2]. Since all implementations suffer from noise, several proposals for secure bit commitment under the noisy-storage model were presented [19,32,36,37], being also demonstrated experimentally [29]. The practical security of QBC assuming technological limitations was also presented in [11] (security against a quantum memoryless adversary was already pointed out in the original BB84 paper [5]). However, by joining quantum mechanics and relativity, it was demonstrated to be possible to create an unconditionally secure QBC protocol based on the exchange of quantum and classical information [17, 18], which was proved to be secure against quantum adversaries [9, 16]. This protocol was already implemented [21, 25]. An information-theoretically secure commitment scheme based on [33] and allowing long commitment times was recently implemented [26]. Even if they are unconditionally secure, relativistic protocols are also difficult to implement. Based on the work from [11], a practical two-state QBC protocol, along with noise and measurement errors calculations, was recently proposed [24].

We present an experimental implementation of the two-state QBC protocol proposed in [24]. An overview of the protocol considerations along with the noise analysis is presented, as well as its experimental implementation. Our experimental work is performed using optical fibers, and the encoding of qubits uses photon polarization. The security of the protocol is based on the lack of long-term stable quantum memories. Provided this technological limitation, the security of the protocol is based on the laws of quantum mechanics and not on mathematical hardness conjectures, which are the basis of all asymmetric classical cryptographic schemes (a generic advantage quantum cryptography has over classical, shown already by the pioneering key distribution protocols of Bennet and Brassard [4, 5]).

This paper contains five sections. In Section 2, we present the protocol definition along with the associated measurement probabilities. In Section 3, we show the experimental setup and discuss the results. In Section 4 we analyse the protocol's security against cheating attempts. Section 5 discusses the main conclusions of this work.

2 Protocol's Definition

QBC is a two-party protocol which allows Bob to know about Alice's commitment. The protocol is binding, i.e., Alice cannot change her commitment after the commitment phase, and concealing, i.e., Bob cannot learn Alice's commitment before the opening phase. In practice, QBC allows to solve trust issues when people are not close to each other. In this section we present the protocol steps, along with the underlying theory of noisy channels. First, it is important to notice that in this protocol it is Alice who makes the commitment (as in the classical BC), while Bob is initializing the protocol by sending individual photons (contrary to the classical BC, where Alice is sending classical bits).

It is emphasized that the qubit states $|0\rangle$ and $|1\rangle$ used in the protocol are not orthogonal. Indeed, we choose states such that $\langle 0|1\rangle = \cos(\pi/4)$. The states orthogonal to $|0\rangle$ and $|1\rangle$ are denoted by $|0^{\perp}\rangle$ and $|1^{\perp}\rangle$, respectively, so that $\langle 0^{\perp}|0\rangle = 0$ and $\langle 1^{\perp}|1\rangle = 0$. In that way, we defined two orthonormal bases $\mathcal{B}_0 = \{|0\rangle, |0^{\perp}\rangle\}$ and $\mathcal{B}_1 = \{|1\rangle, |1^{\perp}\rangle\}$, which define two orthogonal observables that we call $\hat{C}_0$ and $\hat{C}_1$:

$$\hat{C}_0 = 0\cdot|0\rangle\langle 0| + 1\cdot|0^{\perp}\rangle\langle 0^{\perp}|, \tag{1}$$

$$\hat{C}_1 = 1\cdot|1\rangle\langle 1| + 0\cdot|1^{\perp}\rangle\langle 1^{\perp}|. \tag{2}$$

For the measurement strategy, Alice is measuring one of the two observables defined in equation (2) (see a detailed discussion below). Since the angle between the two states $|0\rangle$ and $|1\rangle$, and the respective bases $\mathcal{B}_0$ and $\mathcal{B}_1$, is $\pi/4$, the probability of having a mismatch between the state sent and the measurement outcome is 1/2 [12]. We now turn our attention to factors which contribute to an increased quantum-bit error rate (QBER). We will divide them into two groups. The first group will represent the effects that change the quantum state of a photon – the noise as a consequence of the photon's interaction with the environment and misalignment of the experimental apparatus. Following [14], we call it the *optical noise* and model it by a depolarizing channel (see Section IV.A; note that the visibility V from Eq. (34) of [14] and the depolarizing channel parameter p given by Eq. (3) below are related by a simple relation $V = 1 - p$). The other group of factors that contribute to the QBER are imperfect single-photon sources, photon-absorption by the environment, finite detector efficiencies and detectors' dark counts. In contrast to the first group, we will refer to these factors as *non-optical noise.*

The protocol has four phases and runs as follows:

1. **Initialization:** Bob generates a random sequence of classical bits, encodes them in one of two polarization states, $|0\rangle$ or $|1\rangle$ and sends them to Alice. Bob then keeps the record of the states of the photons sent to Alice.

2. **Commitment:** Immediately after receiving a photon from Bob, Alice performs a measurement on it. She measures one of the two observables $\hat{C}_0$ or $\hat{C}_1$ on all photons received from Bob. The choice of the measurement observable is the following: if Alice wants to commit to 0 then she measures $\hat{C}_0$, if she wants to commit to 1 then she measures $\hat{C}_1$, on all photons.

3. **Opening:** Alice reveals her commitment. She informs Bob the observable she measured and the measurement results she obtained.

4. **Validation:** Bob performs a goodness-of-fit test to check whether Alice's measurements are statistically sound, and either accepts or rejects Alice's commitment based on this test (see the paragraph below).

There are various schemes that Bob can adopt to validate Alice's commitment. We here take advantage of the simplicity of the protocol and assume Bob uses the following test, known as the binomial test: let $p_c(r|b)$, with $c, r, b \in \{0, 1\}$, denote the conditional probability that Alice obtains result r when measuring observable $\hat{C}_c$ on state $|b\rangle$. All these can be easily computed or estimated by Bob before the protocol starts. Let $n(r|b)$ be the number of r's measured by Alice whenever state $|b\rangle$ was sent, and define $q(r|b) = \frac{n(r|b)}{n(b)}$. Then the sets $\{q(r|0)\}_{r\in\{0,1\}}$ and $\{q(r|1)\}_{r\in\{0,1\}}$ form sets of statistical data. Without loss of generality, suppose Alice is committing to 0. Let $P(q(r|0)||p_0(0|0))$ be the probability that a binomial distribution with probability of success $p_0(0|0)$ produces the statistics $\{q(r|0)\}_{r\in\{0,1\}}$, and analogously for $P(q(r|1)||p_0(1|1))$. To accept Alice's commitment, Bob checks that $P(q(r|0)||p_0(0|0)) > \alpha$ and that $P(q(r|1)||p_0(1|1)) > \alpha$, where α is a threshold probability to be determined by Bob himself. Furthermore, for viability purposes, one must require that if Alice commits to 1, she must be unable to pass the test of committing to 0. As noted in [24], this requirement is satisfied as long as it is secure against a cheating Alice. In Section 4 we analyze possible choices of the security parameter α and show that the protocol is indeed secure against a cheating Alice.

To analyze the optical part of the noise, we consider a white-noise model given by a depolarizing channel $\mathcal{E}_{\rm d}$ with a given probability p, that is:

$$\mathcal{E}_{\rm d}(\hat{\rho}) = (1 - p)\hat{\rho} + p\frac{\hat{I}}{2}\,, \tag{3}$$

where $\hat{\rho}$ is a general mixed state which represents the initial qubit state and $\hat{I}$ is the identity operator. It is worth considering the overall conditional probabilities obtained from each measurement. If by $p_c(r|b)$, with $c, r, b \in \{0, 1\}$, we denote a conditional probability that a result r is obtained when measuring observable $\hat{C}_c$ on state $|b\rangle$, then the conditional probabilities are given by the following expressions [24],

- If Alice measures $\hat{C}_0$:

$$p_0(0|0) = 1 - \frac{p}{2} \tag{4}$$
$$p_0(1|0) = \frac{p}{2} \tag{5}$$
$$p_0(0|1) = 1/2 \tag{6}$$
$$p_0(1|1) = 1/2. \tag{7}$$

- If Alice measures $\hat{C}_1$:

$$p_1(0|0) = 1/2 \tag{8}$$
$$p_1(1|0) = 1/2 \tag{9}$$
$$p_1(0|1) = \frac{p}{2} \tag{10}$$
$$p_1(1|1) = 1 - \frac{p}{2}. \tag{11}$$

Let $n_c(r|b)$, with $c, r, b \in \{0, 1\}$, be the number of results r when measuring observable $\hat{C}_c$ on state $|b\rangle$, and $n_c(b)$ the total number of detected photons sent in the state $|b\rangle$, when measuring $\hat{C}_c$. If Alice is honest, i.e., if she indeed measures only one out of the two commitment observables $\hat{C}_c$ on all qubits received from Bob, the statistics of her measurements will, due to the law of large numbers, approach the corresponding conditional probabilities in equations (4) and (8). Thus $\frac{n_0(0|0)}{n_0(0)} \approx p_0(0|0) = 1 - \frac{p}{2} = \mathrm{SRATE}_0^{\mathrm{opt}}$ and $\frac{n_0(1|0)}{n_0(0)} \approx p_0(1|0) = \frac{p}{2} = \mathrm{QBER}_0^{\mathrm{opt}}$, and analogously for other cases. We see that the first two expressions from equation (4) represent the optical contribution (opt) for the success (SRATE) and the quantum-bit error rates (QBER), respectively, obtained when measuring observable $\hat{C}_0$ on state $|0\rangle$ (and analogously for the last two expressions of equation (8)). Therefore, if the statistics of Alice's measurements approach equation (4), Bob accepts a commitment to 0; if they approach equation (8), Bob accepts a commitment to 1; otherwise Bob aborts the protocol. Note that up to this point we discussed only the so-called optical errors, due to external noise occurring during the emission, transmission and measurement of photons.

As mentioned, the aim of the protocol is to be both binding and concealing. It is also worth mentioning that (in spite of recent efforts [27, 31]), long-term storage of photons is not going to be feasible in a foreseeable future. Therefore, Alice is forced to perform measurements as the photons arrive: she cannot postpone her commitment until after the commitment phase. Since an ideal single-photon source is very difficult to obtain, Bob is forced to use weak pulses to prevent the well-known splitting attack; the sending pulse rate should be chosen in a way such that the emission rate of multi-photons is much smaller than the emission rate of single photons. When several photons are emitted, all photons are in the same pure state of polarization. Otherwise, Alice could split two and measure $\hat{C}_0$ on one photon, and $\hat{C}_1$ on another. This way she could have results consistent with both commitments (and could thus postpone her

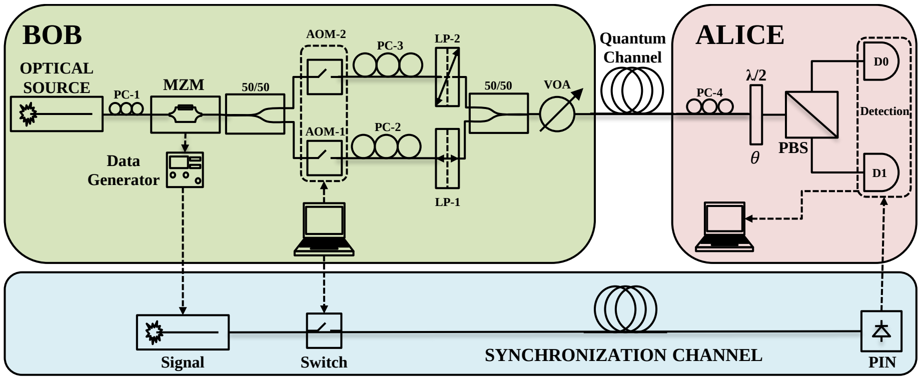

Figure 1: Experimental setup used in the proof-of-principle demonstration of the two-state QBC protocol proposed.

decision). We also make the basic assumption that Bob does not have access to Alice's laboratory and since she is revealing her commitment only during the opening phase, Bob does not get any knowledge about Alice's measurement before that phase. Therefore, since after the completion of the Initialization phase there is no information exchange between the two parties until the start of the Opening phase, the protocol is concealing.

Regarding Alice's measurements, one can also discuss her optimal cheating strategy for single-photon measurements. The optimal cheating observable is the observable "between" $\hat{C}_0$ and $\hat{C}_1$, i.e., it is observable whose eigenbasis is rotated by -$\pi/8$ from $\mathcal{B}_0$ (for the analysis of optimal cheating strategies in the context of quantum cryptography, see for example [10,13,34,38]). The cheating observable $\hat{C}_{\mathrm{ch}}$ is defined by mutually orthogonal vectors, $|\tilde{0}\rangle$ and $|\tilde{1}\rangle$, such that the angle between $|0\rangle$ and $|\tilde{0}\rangle$, and the angle between $|1\rangle$ and $|\tilde{1}\rangle$ is $\pi/8$,

$$\hat{C}_{\mathrm{ch}} = 0 \cdot |\tilde{0}\rangle\langle\tilde{0}| + 1 \cdot |\tilde{1}\rangle\langle\tilde{1}| \,. \tag{12}$$

If Alice obtains the result 0 (corresponding to vector $|\tilde{0}\rangle$), she infers that the state sent by Bob is $|0\rangle$. When we obtain the result 1 (corresponding to state $|\tilde{1}\rangle$), we infer that the state sent by Bob is $|1\rangle$. In the ideal case, the conditional probabilities for the cheating observable are written as,

$$p_{\mathrm{ch}}(0|0) = |\langle 0|\tilde{0}\rangle|^2 = \cos^2\left(\frac{\pi}{8}\right) \tag{13}$$

$$p_{\mathrm{ch}}(1|0) = |\langle 0|\tilde{1}\rangle|^2 = \sin^2\left(\frac{\pi}{8}\right) \tag{14}$$

$$p_{\mathrm{ch}}(0|1) = |\langle 1|\tilde{0}\rangle|^2 = \sin^2\left(\frac{\pi}{8}\right) \tag{15}$$

$$p_{\mathrm{ch}}(1|1) = |\langle 1|\tilde{1}\rangle|^2 = \cos^2\left(\frac{\pi}{8}\right). \tag{16}$$

In this case, the success rate is the probability to infer 0 when the state sent by Bob was $|0\rangle$, and the same for the case when the state sent by Bob was $|1\rangle$. Since the situation is symmetric, the two probabilities are the same. In terms of probabilities, $\mathrm{SRATE}_{\mathrm{ch}}^{\mathrm{opt}}$ and the $\mathrm{QBER}_{\mathrm{ch}}^{\mathrm{opt}}$ are written as:

$$\mathrm{SRATE}_{\mathrm{ch}}^{\mathrm{opt}}(0) = \frac{n_{\mathrm{ch}}(0|0)}{n_{\mathrm{ch}}(0)} \approx p_{\mathrm{ch}}(0|0) = 0.8536 \tag{17}$$

$$\mathrm{QBER}_{\mathrm{ch}}^{\mathrm{opt}}(0) = \frac{n_{\mathrm{ch}}(1|0)}{n_{\mathrm{ch}}(0)} \approx p_{\mathrm{ch}}(1|0) = 0.1464 \tag{18}$$

$$\mathrm{QBER}_{\mathrm{ch}}^{\mathrm{opt}}(1) = \frac{n_{\mathrm{ch}}(0|1)}{n_{\mathrm{ch}}(0)} \approx p_{\mathrm{ch}}(0|1) = 0.1464 \tag{19}$$

$$\mathrm{SRATE}_{\mathrm{ch}}^{\mathrm{opt}}(1) = \frac{n_{\mathrm{ch}}(1|1)}{n_{\mathrm{ch}}(0)} \approx p_{\mathrm{ch}}(1|1) = 0.8536. \tag{20}$$

If the error induced by noise produces the error for an honest player (Alice) identical to the error of a cheating player, then the two strategies (honest and cheating) are indistinguishable, and the protocol cannot be performed. Thus, the honest player error rate $\mathrm{QBER}_{\mathrm{ch}}^{\mathrm{opt}}$ must be smaller than that of a cheating player, which is ≈ 15 %.

3 Experimental Implementation

In this section we present the experimental setup used to implement the two-state QBC protocol, the corresponding experimental results and their analysis.

3.1 Experimental Setup

The scheme of the experimental setup that we have used is presented in Fig. 1. On Bob's side, a pump at $\lambda_{\mathrm{p}} = 1550.92$ nm from a tunable laser source passes through a polarization controller (PC-1) and is externally modulated using a Mach-Zehnder modulator (MZM) to produce optical pulses with a full-width at half maximum of approximately 1 ns, and a repetition rate of 100 kHz. The pulse goes into a 50/50 beam splitter, and two acousto-optic modulators (AOM-1 and AOM-2) will work as a switch. The PC- 2 and PC-3 are used to adjust the polarizations of the photons in the lower and upper arms, respectively. The axis of the linear polarizer LP-1 is set at 0°, preparing the $|0\rangle$ polarization state. Analogously, the axis of the linear polarizer LP-2 is set at 45°, preparing the $|1\rangle$ polarization state. Next, photons pass through a 50/50 beam coupler and are attenuated using a variable optical attenuator (VOA), obtaining an average number $\mu \approx 0.2$ of photons per pulse, (such as in [14]), thus decreasing the probability to have beam-splitter attacks. Then, they reach an optical fiber (single-mode fiber with an attenuation coefficient, $\alpha \approx 0.2$ dB/km) that works as a quantum channel.

At the receiving side, Alice can choose the commitment basis by setting a half-wave plate ($\lambda/2$, with λ being the wavelength of the wave) to $2\theta = 0°$, 45°, or -22.5°, and uses a polarization-beam splitter (PBS) to discriminate between 0° and 90°. The PC-4 is used to compensate random rotations of polarization in the quantum channel. Regarding Alice's commitment, if the wave plate is set at $2\theta = 0°$ it means Alice chooses $\hat{C}_0$, if it is set at $2\theta = 45°$ it means Alice chooses $\hat{C}_1$, and if it is set at $2\theta = -22.5°$ it means Alice chooses $\hat{C}_{\rm ch}$. The photons are detected using two avalanche photodiodes (D0 and D1) [30]. D0 (id200) has a dark count probability per time gate, $t_{\rm g} = 5$ ns, of $P^0_{\rm dc} = 3 \times 10^{-5}$, and a quantum detection efficiency $\eta_0 \approx 7\%$. D1 (id201) has a dark count probability per time gate, $t_{\rm g} = 5$ ns, of $P^1_{\rm dc} = 6 \times 10^{-5}$, and a quantum detection efficiency $\eta_1 \approx 9\%$. A synchronization pulse at $\lambda_{\rm s} = 1547.72$ nm from a distributed feedback laser is used to trigger the detectors, where a switch allows to send pulses with the same repetition rate of the encoded photons. These pulses are detected using a photodiode detector (PIN), which is connected to both detectors. In the synchronization channel, an optical fiber is used with the same length as the quantum channel in order to allow synchronization between Bob and Alice's measurement devices.

3.2 Experimental Results

To demonstrate the feasibility of the experimental setup shown in Fig. 1, we have performed measurements of both $\hat{C}_0$ and $\hat{C}_1$. The rates obtained by Alice when the basis of her measurement observable $\hat{C}_c$ (with $c \in \{0,1\}$) coincides with the basis $\mathcal{B}_b$ (with $b \in \{0,1\}$) from which the state was prepared by Bob ("measurements in equal bases"), as well as when they are different ("measurements in different bases"), are plotted for both cases. The sequence of bits to encode was given by a pseudo-random binary sequence (PRBS) with 2^{17} bits. In a single run we sent the full sequence of bits and recorded the results. In Fig. 2 we show the measurement results obtained when Alice and Bob had a quantum channel of 16 km between them, for both $\hat{C}_0$ and $\hat{C}_1$ as a function of the run. A run means that Bob sent a pattern with the 2^{17} bits through the system and Alice have performed the measurements.

From the experimental results obtained, we can infer several conclusions. First, we notice that the success rates for the case when the measurements are performed using equal bases are always higher than 90%, which is above the minimum theoretical security limit. The average success rate is 93.4 % when $\hat{C}_0$ is measured and 96.7 % when $\hat{C}_1$ is measured. Second, the rates for the case when the measurements are performed in different bases are always close to 50%, as expected. In this case, the average success rate is 52.9 % when $\hat{C}_0$ is measured and 55.4 % when $\hat{C}_1$ is measured. The results are according to theory, since in the ideal case, when the measurements are performed in equal bases, the success rate should be 100%. For measurements in different bases, in the ideal case the rate should be 50%, since the probability to detect a photon is the same for D0 or D1. As described in equations (4) and (8), in the realistic case

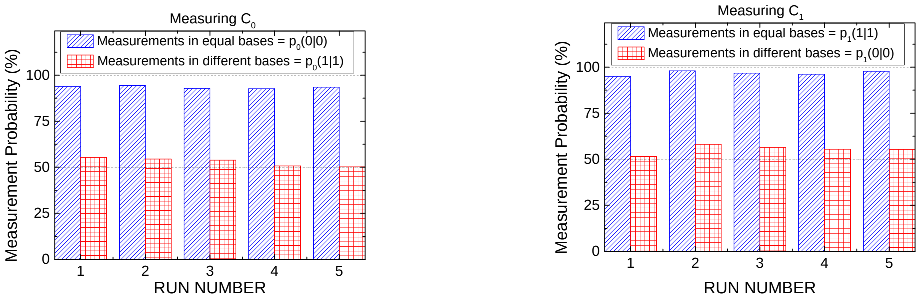

Figure 2: Experimental results of the measurement probability for five different runs obtained when Alice and Bob are interconnected with a quantum channel of 16 km. The dashed line represents the theoretical value for measurements in equal bases and the dash-dotted line the theoretical value for measurement in different bases.

of noisy channels the alignment between Bob and Alice is not perfect, which will lead to wrong detections, and consequently to a rate lower than 100%, or different from 50%, depending if we are talking about measurements in equal bases or different bases, respectively.

The SRATEs and QBERs are a consequence of both optical (depolarizing channel) and non-optical noises (imperfect single-photon sources, photon absorption by the environment, finite detector efficiency and dark counts). Thus,

$$\begin{aligned} \mathrm{SRATE}_i &= \mathrm{SRATE}_i^{\mathrm{opt}} + \mathrm{SRATE}_i^{\mathrm{non-opt}}, \qquad (21)\\ \mathrm{QBER}_i &= \mathrm{QBER}_i^{\mathrm{opt}} + \mathrm{QBER}_i^{\mathrm{non-opt}}\,, \qquad (22) \end{aligned}$$

with $i = 0,\, 1$. Theoretically, the non-optical QBER can be written as,

$$\mathrm{QBER}^{\mathrm{non-opt}} = \frac{P_{\mathrm{dc}}^i}{\mu t_{\mathrm{link}} \eta_i}\,, \qquad (23)$$

where μ is the average number of photons per pulse and $t_{\mathrm{link}} = 10^{(-\alpha L/10)}$, with L being the fiber length (see equations. (31)-(33) in [14], page 166).

The optical noise is given by equations (4) and (8) from Section 2 and plays an important role in the results. The non-optical noise does not depend on the state emitted by the source (Bob's apparatus) nor the observable measured by Alice, but it does depend on the result obtained. However it is worth mentioning that both detectors have different detection efficiencies ($\eta_0 \approx 7\%$ for D0 and $\eta_1 \approx 9\%$ for D1) and their dark count probabilities per time gate are also different ($P_{\mathrm{dc}}^0 = 3\times 10^{-5}$ for D0 and $P_{\mathrm{dc}}^1 = 6\times 10^{-5}$ for D1).

Using equations (4), (8) and (23), equation (22) can be rewritten as,

$$\mathrm{QBER}_i = \frac{p_i}{2} + \frac{P_{\mathrm{dc}}^i}{\mu t_{\mathrm{link}} \eta_i}\,, \qquad (24)$$

which includes both optical and non-optical contributions.

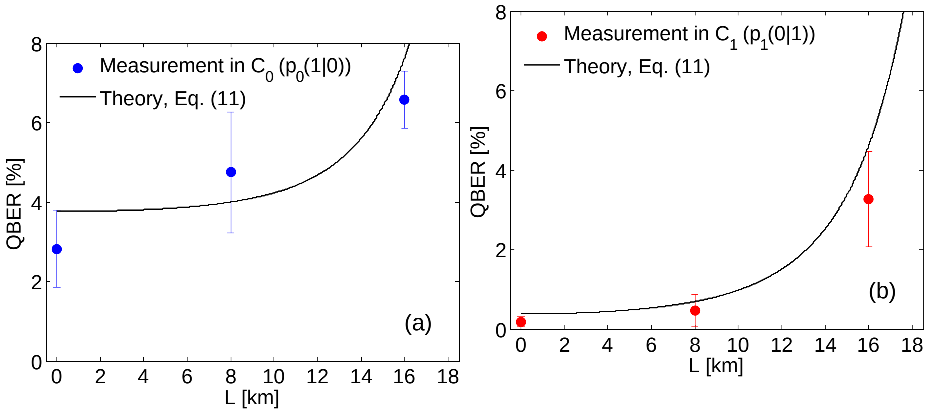

Figure 3: Average QBER as a function of the fiber length when measuring (a) $\hat{C}_0$ (QBER$_0$), and (b) $\hat{C}_1$ (QBER$_1$), along with the theoretical fit from equation (24), where $p_0 = 7.1 \times 10^{-2}$ and $p_1 = 1 \times 10^{-3}$ were used as fitting parameters. The error bars represent the standard deviation of the experimental values. The correlation coefficient between experimental and theoretical data was $r^2 = 0.77$ when $\hat{C}_0$ was measured and $r^2 = 0.99$ when $\hat{C}_1$ was measured.

In addition to Fig. 2, we can plot the measurement results for the average QBER over the number of runs for several fiber lengths, and use the variables p_i in equation (24) as fitting parameters, as shown in Fig. 3. As expected, the QBER increases with the fiber length. The difference between the QBER values in the measurements in $\hat{C}_0$ and $\hat{C}_1$ is due to several reasons: different dark count probabilities and quantum efficiencies of the two detectors and different losses in each channel.

Rewriting equation (24) we obtain

$$p_i(L) = 2\left(\mathrm{QBER}_i - \frac{P^i_{\mathrm{dc}}}{\mu t_{\mathrm{link}} \eta_i}\right). \tag{25}$$

From this equation, using the experimental results from Fig. 3, where each QBER$_i$ is the average value of 5 runs for each fiber length, we plot the values of $p_i(L)$ in Fig. 4, which show the probability of the occurrence of white noise.

In order to check the optimal cheating strategy for Alice, we performed measurements of $\hat{C}_{\mathrm{ch}}$. The results are shown in Fig. 5. From this figure it can be seen there's a relatively good agreement between experimental results and theoretical predictions. In Fig. 6 we present the experimental results of the QBER for measurements of $\hat{C}_{\mathrm{ch}}$ for several fiber lengths. We can see that the QBER is a bit higher than the theoretical value, mainly because of the difficulty to set the half-wave plate ($\lambda/2$) at exactly $2\theta = -22.5°$ and the unavoidable optical noise. The differences between measurements of ones and zeros are also due to efficiency and dark counts differences in the two detectors and different losses in each channel. In fact, the same type of error due to bad alignment exists

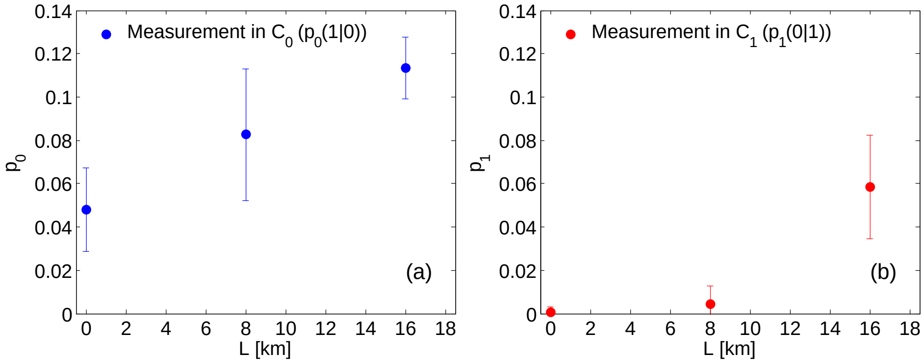

Figure 4: Calculated values for (a) p_0 and (b) p_1 as a function of L, using equation (25). The error bars represent the standard deviation of the experimental values.

when measuring $\hat{C}_0$ and $\hat{C}_1$, but since it is much easier to align the equipment for those two measurements, we can assume that when measuring $\hat{C}_0$ and $\hat{C}_1$, this type of error is negligible, with respect to the measurement of the cheating observable. The average rates for the optimal cheating strategy were 80% when measuring zeros and 73.8% when measuring ones.

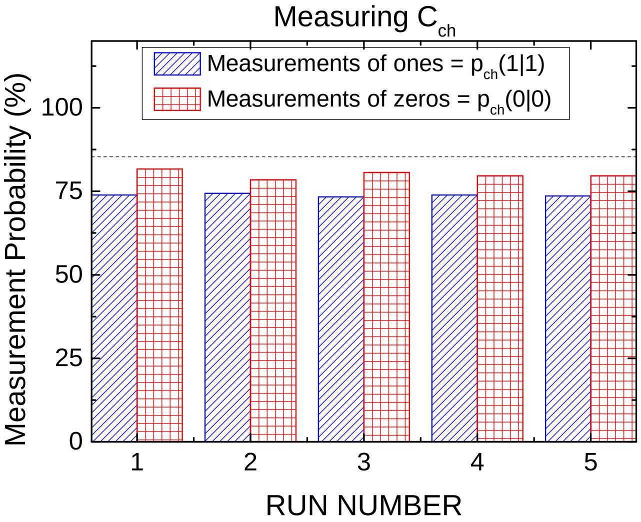

Figure 5: Experimental results of the measurement probability for five different runs obtained from the measurements in $\hat{C}_{\rm ch}$, when Alice and Bob are interconnected with a quantum channel with 16 km. The dashed line represents the theoretical value for measurements of both zeros and ones.

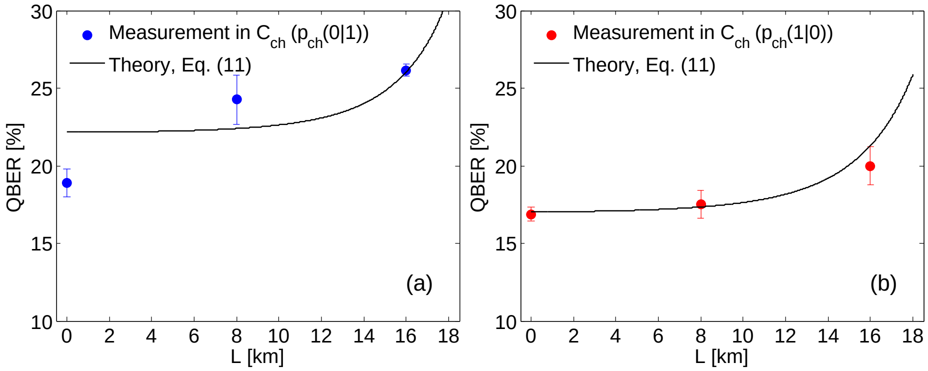

Figure 6: Average QBER as a function of the fiber length when measuring (a) ones in $\hat{C}_{\text{ch}}$, and (b) zeros in $\hat{C}_{\text{ch}}$, along with the theoretical fit from equation (24), where $p_0 = 0.439$ and $p_1 = 0.334$ are average values. The error bars represent the standard deviation of the experimental values. The correlation coefficient between experimental and theoretical data was $r^2 = 0.43$ when ones were measured in $\hat{C}_{\text{ch}}$ and $r^2 = 0.98$ when zeros were measured in $\hat{C}_{\text{ch}}$.

4 Security Against a Cheating Alice

In this Section we analyse the security of the protocol against the above described cheating Alice. First, we use the experimental results for Alice's measurements of observables $\hat{C}_0$ and $\hat{C}_1$ to calibrate the equipment, i.e., to establish Bob's precise quantitative validity criterion. Then, we show that the experimentally obtained results of a cheating Alice would not pass such criterion, showing that the protocol is secure. First, we describe how Bob forms the viability criterion introduced in Section 2.

The probability that an honest Alice obtains n_0 times the value 0 when measuring N_0 particles in state $|0\rangle$ is given by a binomial distribution with mean value

$$\mu_0 = N_0 p_0(0|0) \tag{26}$$

and variance

$$\sigma_0^2 = N_0 p_0(0|0)(1 - p_0(0|0)). \tag{27}$$

Since, for sufficiently large N_0, this binomial distribution behaves like a normal distribution with the same parameters, the binomial test described in Section 2 reduces to the well-known $68 - 95 - 99.7$ rule of thumb, for significance levels of 32%, 5% and 0.3%, respectively. For a significance level of 0.3%, Bob accepts Alice's statistics for whenever $|0\rangle$ was sent if

$$n_0 \in [\mu_0 - 3\sigma_0, \mu_0 + 3\sigma_0], \tag{28}$$

which will henceforth be called the "3σ security criterion". This ensures that if an honest Alice is committing to 0, then she has $\approx 99.7\%$ chance of having the first part of her data set accepted by Bob as a valid commitment. In terms of the security parameter α introduced in Section 2, this corresponds to setting

$$\alpha = \Pr[n_0 = \mu_0 - 3\sigma_0]. \tag{29}$$

Analogously, Bob now proceeds to test the second portion of Alice's statistics, those when state $|1\rangle$ was sent, and accepts them if

$$n_1 \in [\mu_1 - 3\sigma_1, \mu_1 + 3\sigma_1]. \tag{30}$$

Finally, Bob validates Alice's commitment as a whole if both conditions (28) and (30) are satisfied. For the "3σ security criterion", the protocol will fail to accept an honest Alice's commitment around 6 times every thousand runs.

Concretely, Fig. 2 represents the measured conditional probabilities $p_0(r|b)$, when taking into account both optical and non-optical errors. The exact values are given by

$$\begin{align} p_0(0|0) &= 0.934 \tag{31}\\ p_0(1|0) &= 0.066 \tag{32}\\ p_0(0|1) &= 0.471 \tag{33}\\ p_0(1|1) &= 0.529. \tag{34} \end{align}$$

In this case, given that in each run of the protocol there were on average about $N_0 \approx N_1 \approx 350$ measurement outcomes, we have

$$\begin{align} \mu_0 &= 326.9 \tag{35}\\ \sigma_0 &= 4.64 \tag{36}\\ \mu_1 &= 185.15 \tag{37}\\ \sigma_1 &= 9.34. \tag{38} \end{align}$$

In particular, we have $[\mu_0 - 3\sigma_0, \mu_0 + 3\sigma_0] = [312.98, 340.82]$.

We now compute the probability that a cheating Alice passes the previous goodness-of-fit test. The exact values represented in Fig. (5) are

$$\begin{align} p_{\mathrm{ch}}(0|0) &= 0.8 \tag{39}\\ p_{\mathrm{ch}}(1|0) &= 0.2 \tag{40}\\ p_{\mathrm{ch}}(0|1) &= 0.262 \tag{41}\\ p_{\mathrm{ch}}(1|1) &= 0.738. \tag{42} \end{align}$$

It suffices to note that for $N_0 \approx N_1 \approx 350$ measurement outcomes obtained when measuring $\hat{C}_{\mathrm{ch}}$, a cheating Alice would obtain around $280 = N_0 p_{\mathrm{ch}}(0|0)$ times the value 0. Since $280 \notin [312.98, 340.82]$, the statistics from a cheating Alice would not be accepted by Bob as a valid commitment to 0. Note that even if we had chosen $[\mu_0 - 10\sigma_0, \mu_0 + 10\sigma_0]$ as the acceptance interval (significance level of 10^{-15}), so as to increase the chance of an honest Alice being rightfully accepted, a cheating Alice would, on average, still fail to pass that test.

Note that such a low allowance for statistical error shows that, in a real-life implementation, one can use far less photon pulses than those used here: $2^{17} \approx 130000$. Indeed, in [24], Section V, it was shown that to guarantee a 3 standard-deviation allowance, it is enough to have around $N_0 \approx N_1 \approx 50$ measurement outcomes, which corresponds to about $2^{13} \approx 8000$ photon pulses. In fact, the above optimal probability to cheat for single-qubit measurements decreases exponentially with respect to the number of photons (see for example *Theorem 4* of [35]), i.e. it is given by a *negligible function* (a function $\varepsilon : \mathbb{N} \to \mathbb{R}$ is said to be negligible if for every positive polynomial p there exists a $n_0 \in \mathbb{N}$ such that for all $n > n_0$, $\varepsilon(n) \leq 1/p(n)$, see for example [15]).

It is interesting to note that even having perfect detectors (with perfect efficiency and no dark counts) cannot help a cheating Alice. Note that perfect detectors will only improve the results of $\hat{C}_0$ and $\hat{C}_1$ measurements used to establish Bob's numerical verification criterion, reducing them to the case of optical noise only, given by equations (4) and (8). In other words, Bob's verification criterion will be even tighter than in the case of non-ideal detectors. While the perfect detectors will also improve the chances of a cheating Alice, it will not be enough to significantly compromise the protocol's security. Indeed, assuming the "noisy" verification criterion given by equation (28), for the experimental values given by equations (31) and (35) and perfect cheating statistics given by equation (2), the protocol's security significance level is still of the order of 10^{-8}, which corresponds to a "6σ security criterion" (i.e., even a cheating Alice with exceptional access to perfect technology is successful only once in around every 100 million runs).

A general theoretical discussion of the protocol's security and viability was presented in [24], where it was shown that if the protocol is secure against a cheating Alice, then it is also viable: an honest Alice trying to commit to 1 can never pass the test of committing to 0.

5 Conclusions

We have implemented a two-state quantum bit commitment protocol in optical fibers. The encoding of qubits was performed using two nonorthogonal states of polarization. We were able to implement the protocol even when photons travel through an optical fiber with several kilometers in length. We also presented results obtained for the optimal cheating strategy for Alice, showing good agreement with the theory. We noticed that the success rates for the case when the measurements were performed using equal bases were always higher than 90%. The rates for the case when the measurements were performed in different bases were always close to 50%. In this case, the average success rate was 52.9 % when $\hat{C}_0$ was measured and 55.4 % when $\hat{C}_1$ was measured. When measuring the observable for the optimal cheating strategy the average success rates were 80% when measuring zeros and 73.8% when measuring ones. We presented a detailed numerical validity criterion for Bob to either accept or reject

Alice's commitment, and showed that, with the above mentioned experimental rates, the protocol is secure against cheating attempts.

Finally, we note that although we presented the experimental implementation of a two-state protocol, with the necessary adjustments it can be converted to a four-state protocol. Note that in this case Bob's criterion would be split into 4 different conditions similar to Eqs. (28) and (30), thus making it harder for a cheating Alice to succeed. In general, the more states there are, the less photons are needed in each run of the protocol to ensure a given level of security. A rigorous theoretical analysis of the dependence of the level of security with respect to the number of photons used can be done by following the arguments in Reference [24], which can be straightforwardly adapted to the 4-state protocol.

Acknowledgments

This work was supported in part by the FCT - Fundação para a Ciência e a Tecnologia, through the PhD Grants SFRH/BD/79482/2011 and SFRH/BD/-79571/2011 and the Post Doctoral Grants SFRH/BPD/77286/2011 and SFRH/BPD/96457/-2013, by the FCT and the Instituto de Telecomunicações under the PEst-OE/EEI/LA0008/2011 program, project 'P-Quantum', the PEst-OE/EEI/LA0008/2013 program, project 'CV-Quantum' and by the Conselho de Reitores das Universidades Portuguesas (CRUP), project 'Ação Integrada E 91/12'.

The authors would like to thank Eng. João Prata from the Instituto de Telecomunicações, Aveiro, for his contribution regarding electronics.

References

[1] D. Aharonov, A. Ta-Shma, U. Vazirani, and A. Yao. Quantum bit escrow. In *Proceedings of the Thirty-second Annual ACM Symposium on Theory of Computing*, STOC '00, pages 705–714, New York, NY, USA, 2000. ACM.

[2] A. Ambainis. A new protocol and lower bounds for quantum coin flipping. *J. Comput. Syst. Sci.*, 68(2):398–416, March 2004.

[3] John S. Bell. On the einstein podolsky rosen paradox. *Physics*, 1(3):195–200, 1964.

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

[5] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers Systems and Signal Processing*, volume 175, pages 175–179. Bangalore, India, 1984.

[6] G. Brassard, C. Crépeau, D. Mayers, and L. Salvail. Defeating classical bit commitments with a quantum computer. *arXiv:quant-ph/9806031*, June 1998.

[7] A. Chailloux, I. Kerenidis, and B. Rosgen. Quantum commitments from complexity assumptions. In Luca Aceto, Monika Henzinger, and Jir Sgall, editors, *Automata, Languages and Programming*, volume 6755 of *Lecture Notes in Computer Science*, pages 73–85. Springer Berlin Heidelberg, 2011.

[8] J. W. Choi, D. Hong, K.-Y. Chang, D. P. Chi, and S. Lee. Non-static Quantum Bit Commitment. *arXiv:0901.1178*, January 2009.

[9] Sarah Croke and Adrian Kent. Security details for bit commitment by transmitting measurement outcomes. *Phys. Rev. A*, 86:052309, Nov 2012.

[10] Liu Dan, Pei Chang-xing, Quan Dong-xiao, Han Bao-bin, and Zhao Nan. A new attack strategy for bb84 protocol based on, breidbart basis. In *Communications and Networking in China, 2009. ChinaCOM 2009. Fourth International Conference on*, pages 1–3, Aug 2009.

[11] A. Danan and L. Vaidman. Practical Quantum Bit Commitment Protocol. *Quantum Inf. Process.*, 11(3):769–775, June 2012.

[12] A. K. Ekert, B. Huttner, G. M. Palma, and A. Peres. Eavesdropping on quantum-cryptographical systems. *Phys. Rev. A*, 50:1047–1056, August 1994.

[13] Christopher A. Fuchs, Nicolas Gisin, Robert B. Griffiths, Chi-Sheng Niu, and Asher Peres. Optimal eavesdropping in quantum cryptography. i. information bound and optimal strategy. *Phys. Rev. A*, 56:1163–1172, Aug 1997.

[14] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden. Quantum cryptography. *Rev. Mod. Phys.*, 74:145–195, March 2002.

[15] Oded Goldreich. Foundations of cryptography: A primer. *Found. Trends Theor. Comput. Sci.*, 1(1):1–116, April 2005.

[16] J. Kaniewski, M. Tomamichel, E. Hanggi, and S. Wehner. Secure bit commitment from relativistic constraints. *IEEE Trans Inf Theory*, 59(7):4687–4699, July 2013.

[17] A. Kent. Unconditionally secure bit commitment with flying qudits. *New J. Phys.*, 13(11):113015, November 2011.

[18] A. Kent. Unconditionally Secure Bit Commitment by Transmitting Measurement Outcomes. *Phys. Rev. Lett.*, 109(13):130501, September 2012.

[19] R. Konig, S. Wehner, and J. Wullschleger. Unconditional security from noisy quantum storage. *IEEE Trans Inf Theory*, 58(3):1962–1984, March 2012.

[20] Q. Li, C. Li, D.-Y. Long, W. H. Chan, and C.-H. Wu. On the impossibility of non-static quantum bit commitment between two parties. *Quantum Inf. Process.*, 11(2):519–527, 2012.

[21] Yang Liu, Yuan Cao, Marcos Curty, Sheng-Kai Liao, Jian Wang, Ke Cui, Yu-Huai Li, Ze-Hong Lin, Qi-Chao Sun, Dong-Dong Li, Hong-Fei Zhang, Yong Zhao, Teng-Yun Chen, Cheng-Zhi Peng, Qiang Zhang, Adán Cabello, and Jian-Wei Pan. Experimental unconditionally secure bit commitment. *Phys. Rev. Lett.*, 112:010504, Jan 2014.

[22] H.-K. Lo and H. F. Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D*, 120:177–187, September 1998.

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

[24] R. Loura, Á. J. Almeida, P. S. André, A. N. Pinto, P. Mateus, and N. Paunković. Noise and measurement errors in a practical two-state quantum bit commitment protocol. *Phys. Rev. A*, 89(5):052336, May 2014.

[25] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden. Experimental bit commitment based on quantum communication and special relativity. *Phys. Rev. Lett.*, 111:180504, Nov 2013.

[26] T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, S. Wehner, and H. Zbinden. Practical Relativistic Bit Commitment. *Phys. Rev. Lett.*, 115(3):030502, July 2015.

[27] P. C. Maurer, G. Kucsko, C. Latta, L. Jiang, N. Y. Yao, S. D. Bennett, F. Pastawski, D. Hunger, N. Chisholm, M. Markham, D. J. Twitchen, J. I. Cirac, and M. D. Lukin. Room-Temperature Quantum Bit Memory Exceeding One Second. *Science*, 336:1283–1286, June 2012.

[28] D. Mayers. Unconditionally Secure Quantum Bit Commitment is Impossible. *Phys. Rev. Lett.*, 78:3414–3417, April 1997.

[29] N. H. Y. Ng, S. K. Joshi, C. Chen Ming, C. Kurtsiefer, and S. Wehner. Experimental implementation of bit commitment in the noisy-storage model. *Nat. Commun.*, 3, December 2012.

[30] G. Ribordy, N. Gisin, O. Guinnard, D. Stucki, M. Wegmuller, and H. Zbinden. Photon counting at telecom wavelengths with commercial InGaAs/InP avalanche photodiodes: current performance. *J. Mod. Opt.*, 51:1381–1398, September 2004.

[31] Kamyar Saeedi, Stephanie Simmons, Jeff Z. Salvail, Phillip Dluhy, Helge Riemann, Nikolai V. Abrosimov, Peter Becker, Hans-Joachim Pohl, John J. L. Morton, and Mike L. W. Thewalt. Room-temperature quantum bit storage exceeding 39 minutes using ionized donors in silicon-28. *Science*, 342(6160):830–833, 2013.

[32] C. Schaffner, B. Terhal, and S. D. C. Wehner. Robust Cryptography In The Noisy-Quantum-Storage Model. *Quantum Inf. Comp.*, 11-12:963–996, 2009.

[33] J.-R. Simard. Classical and quantum strategies for bit commitment schemes in the two-prover model. Master's thesis, McGill University, 2007.

[34] R. W. Spekkens and T. Rudolph. Optimization of coherent attacks in generalizations of the BB84 quantum bit commitment protocol. *Quantum Inf. Comp.*, 2(1):66–96, 2002.

[35] V. Vedral. The role of relative entropy in quantum information theory. *Rev. Mod. Phys.*, 74:197–234, Mar 2002.

[36] S. Wehner, C. Schaffner, and B. M. Terhal. Cryptography from Noisy Storage. *Phys. Rev. Lett.*, 100(22):220502, June 2008.

[37] Stephanie Wehner, Marcos Curty, Christian Schaffner, and Hoi-Kwong Lo. Implementation of two-party protocols in the noisy-storage model. *Phys. Rev. A*, 81:052336, May 2010.

[38] M. Williamson and V. Vedral. Eavesdropping on practical quantum cryptography. *J. Mod. Opt.*, 50:1989–2011, 2003.

[39] P. Zoller, T. Beth, D. Binosi, R. Blatt, H. Briegel, D. Bruss, T. Calarco, J. I. Cirac, D. Deutsch, J. Eisert, A. Ekert, C. Fabre, N. Gisin, P. Grangiere,

M. Grassl, S. Haroche, A. Imamoglu, A. Karlson, J. Kempe, L. Kouwenhoven, S. Kröll, G. Leuchs, M. Lewenstein, D. Loss, N. Lütkenhaus, S. Massar, J. E. Mooij, M. B. Plenio, E. Polzik, S. Popescu, G. Rempe, A. Sergienko, D. Suter, J. Twamley, G. Wendin, R. Werner, A. Winter, J. Wrachtrup, and A. Zeilinger. Quantum information processing and communication. Strategic report on current status, visions and goals for research in Europe. *Eur. Phys. J. D*, 36:203–228, November 2005.