Research Article | Vol. 32, No. 9 / 22 Apr 2024 / Optics Express 15955

Optics EXPRESS

Experimental implementation of a quantum zero-knowledge proof for user authentication

MARTA I. GARCÍA-CID,[1,2,*] DILEEPSAI BODANAPU,[3] ALBERTO GATTO,[4] PAOLO MARTELLI,[4] VICENTE MARTÍN,[2] AND LAURA ORTIZ[2,5]

[1] *Indra Sistemas S.A., 28108, Madrid, Spain*
[2] *Center for Computational Simulation, Universidad Politécnica de Madrid, 28660, Madrid, Spain*
[3] *Cohaerentia S.r.l, 20133, Milano, Italy*
[4] *Dip. di Elettronica, Informazione e Bioingegneria, Politecnico di Milano, 20133, Milano, Italy*
[5] *Depto. de Arquitectura y Tecnología de Sistemas Informáticos, ETSIInf, Universidad Politécnica de Madrid, 28660, Madrid, Spain*
[*] *migarcia@indra.es*

Abstract: A new interactive quantum zero-knowledge protocol for identity authentication implementable in currently available quantum cryptographic devices is proposed and demonstrated. The protocol design involves a verifier and a prover knowing a pre-shared secret, and the acceptance or rejection of the proof is determined by the quantum bit error rate. It has been implemented in modified Quantum Key Distribution devices executing two fundamental cases. In the first case, all players are honest, while in the second case, one of the users is a malicious player. We demonstrate an increase of the quantum bit error rate around 25% in the latter case compared to the case of honesty. The protocol has also been validated for distances from a back-to-back setup to more than 60 km between verifier and prover. The security and robustness of the protocol has been analysed, demonstrating its completeness, soundness and zero-knowledge properties.

1. Introduction

Zero knowledge proofs (ZKP) [1] are cryptographic mechanisms where a user (prover) has to prove to another user (verifier) that the first is aware of a secret, without revealing the secret itself or any information about it. Zero-knowledge proofs provide a powerful tool for enhancing online privacy and security in various domains. Depending on the scope of application, it may be the case that both the verifier and the prover are aware of the secret before carrying out the proof or, on the contrary, that only the prover knows the secret.

Depending on the initial setup and the specific needs of the system, a large number of use cases with ZKP applicability can be defined, among which stand out authentication systems to prove the identity of an entity or person [2]; privacy-preserving payments to verify that one party has sufficient funds to make a payment, without revealing the actual balance or transaction history [3]; or access control where users can prove that they have appropriate access to a system or resource without revealing any additional information [4].

The concept of ZKP was first introduced in 1985 by S. Goldwasser, S. Micali, and C. Rackoff [1] showing that certain types of problems, such as graph isomorphism, could be proven without revealing any additional information beyond the truth of the statement. Since then, ZKP have advanced rapidly, with new techniques, protocols, and applications being developed and refined, becoming an important tool in cryptography. As technologies mature, ZKP are expected to play an increasingly important role in enhancing privacy and security.

There are two distinct types of ZKP, interactive [1] and non-interactive [5] ZKP. In the former, both the prover and the verifier are required to be present simultaneously during the execution of the proof, as would be the case of the protocol proposed by Fiat-Shamir [2]. In the second type,

#517754 https://doi.org/10.1364/OE.517754
Journal © 2024 Received 10 Jan 2024; revised 20 Feb 2024; accepted 22 Feb 2024; published 16 Apr 2024

Optics EXPRESS

the verifier can launch the proof when the prover is absent, thus solving it later, as is the case of the Zero-knowledge succinct non-interactive argument of knowledge (zkSNARK) [6].

The implementation of ZKP protocols in quantum communications is of special interest for use cases such as the authentication of several users with access to the same quantum node within a quantum communication infrastructure (QCI).

Within the field of quantum cryptography, the quantum key distribution (QKD) provides secret symmetric keys between two remote parties thanks to the fundamental laws of quantum mechanics. The most widely studied and tested QKD protocol is BB84 [7]. Recently, other quantum-based cryptographic techniques have been explored, such as quantum digital signatures [8,9] or oblivious transfer [10], among others.

This work aims to adapt the concepts of classical zero-knowledge proofs to the field of quantum cryptography, and proposes a new quantum zero-knowledge proof (QZKP). Currently in the literature there are not many studies on QZKP, however some proposals and approaches, mainly for increasing the efficiency of QKD devices, have turned out to be of great interest for the design of the QZKP. Specifically, in 2005 the floating bases protocol was published [11,12], proposing an increase of the number of possible bases to be used in QKD protocols in order to achieve a more efficient system, simultaneously increasing the threshold of the allowed error rate and reducing the information that can be extracted by Eve. To carry out this scheme, it is required that Bob and Alice have a pre-shared secret key on which the selection of the bases will depend. Another strategy to improve the efficiency of the QKD devices is the one in [13], where the authors propose a decoy-state protocol for QKD characterized by a biased bases selection, where signal states are always encoded in basis Z, while decoy signals can be randomly encoded in basis X or Z with a pre-determined probability. More recently, in 2018, modifications of BB84 protocol were proposed through the use of pseudo-random states generated from a pre-shared secret key [14], in order to achieve higher key rates. The main drawback of the proposed scheme is the strict requirement of the employment of a perfect single-photon source. The use of pre-shared keys and the pseudorandom selection of the quantum states are the main concepts applied for the design of the proposed QZKP.

In this paper, we propose and implement a new interactive QZKP where both the prover and the verifier possess a shared secret in advance. It is important not to confuse a user-oriented authentication with the authentication of the classic channel in the QCI. The latter pursues the authentication at a network level, but there is still a need of guaranteeing the identity of the end user who is on the other side of the screen in such a way that his data remains private. In this work, a user-oriented authentication is addressed. A real use case of a user-oriented authentication could be a situation where the same computer is used by several doctors in a hospital to upload their patient information into the health system. When accessing the health system each of the doctor must be authenticated which could be done with the proposed QZKP. The proof is based on purely quantum mechanisms and has been implemented and experimentally tested on quantum cryptographic devices.

The paper is organized as follows: firstly, the design of the new QZKP in Section 2 is presented; then, the security of the protocol is analyzed in Section 3. Finally, the experimental setup and the outcomes are described in Section 4.

2. Quantum zero-knowledge proof

In this paper, we propose an interactive quantum zero-knowledge proof (QZKP), where both the verifier (Alice) and the prover (Bob) must pre-share a secret s to correctly validate the proof. In particular, Bob uses a QZKP with Alice to authenticate himself, as detailed in Fig. 1. This is always the case whenever a QKD channel has been established before. The proof is divided into three stages:

A. Pre-processing stage, when all the information and setup needed to carry out the QZKP are prepared. The procedures performed in this stage are purely classical and correspond to steps 1 and 2 of Fig. 1;

B. Quantum stage, in which the generation, transmission and measurement of the quantum states will be carried out, permitting to create a raw bit string in both the transmitter and receiver ends. In this case, quantum processes are taking place and correspond to steps 3, 4 and 5 of Fig. 1;

C. Verification stage, in which the validity or not of the proof is determined through an estimation of the error rate. To perform this evaluation, classical tools are used and correspond to steps 6, 7 and 8 of Fig. 1.

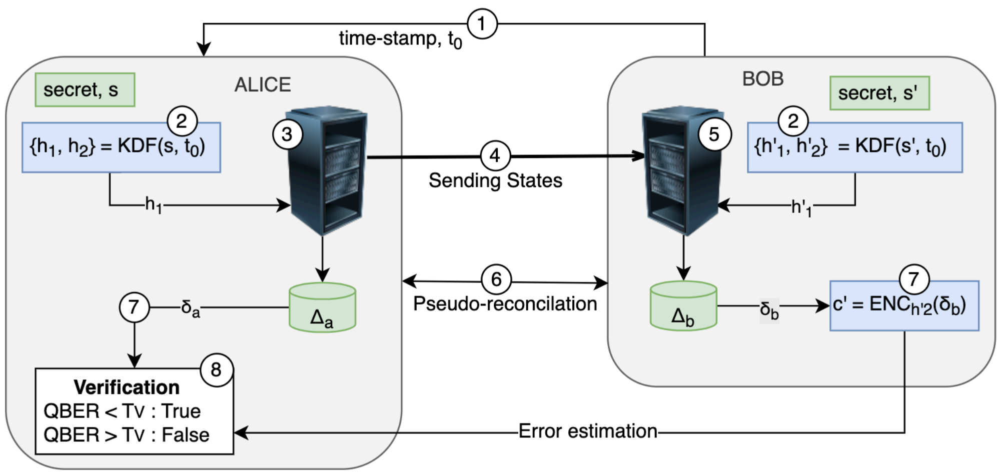

Fig. 1. Flowchart of the quantum zero-knowledge proof between Alice and Bob. Steps 1 and 2 correspond to the pre-processing stage where the information needed for the execution of the proof is prepared. Steps 3 to 5 correspond to the quantum stage, where the quantum states are prepared, sent and measured. In Steps 6 to 8 the verification of the proof is carried out by the estimation of the quantum bit error rate (QBER). If both are honest $s = s'$, otherwise $s \neq s'$. KDF means Key Derivation Function; $\Delta_{a,b}$ are raw measurements; $\delta_{a,b}$ are the results of the post-processing of $\Delta_{a,b}$; ENC means the encryption of $\delta_{a,b}$ with h'_2; and T_v is the verification threshold.

The pre-processing stage starts with a handshake between Alice and Bob, at the end of which an identical timestamp t_0 is generated in both sites. After that, given a secret s of any length, Alice and Bob apply a key derivation function (KDF) [15] that permits to derive h_1 and h_2, just giving t_0 and s as inputs. This step is carried out by both Alice and Bob simultaneously. The h_1 and h_2 resulting from this operation on Alice are $h_1 \in \{0, 1\}^m$ and $h_2 \in \{0, 1\}^n$, where the lengths m and n, being $n<m$, are values to be defined by the players before executing the protocol. The process is equivalently performed at Bob's side, where $h'_1 \in \{0, 1\}^m$ and $h'_2 \in \{0, 1\}^n$ are computed. In a scenario where both Alice and Bob are honest players $s = s'$, otherwise $s \neq s'$. More details about the KDF are given in Section 3.2.

Once $\{h_1, h_2\}$ and $\{h'_1, h'_2\}$ have been calculated, the second phase of the protocol proceeds to generate the quantum bit string. Unlike a conventional QKD protocol, where the bases and states are randomly selected, here the bases are determined on Alice's side by the bit-values of h_1, while a random selection of states within each basis is performed. Then, Alice sends the stream

Optics EXPRESS

of quantum signals to Bob, who will receive and measure them following the bases determined by the bit-values of h'_1.

When Bob really knows the secret and Alice is an honest verifier, $h_1 = h'_1$. Therefore, when preparing and measuring the quantum states, both will obtain an almost identical bit string, Δ_a^r in Alice's side and Δ_b^r in Bob's, meaning with the superindex r that these are raw strings without any post-processing. The obtained bit string is almost identical because, despite preparing the states and measuring them on the same bases, losses occur during their transmission, even in the absence of any malicious manipulation. If we consider an ideal setup, characterized by a perfect extinction ration at the receiver, with no errors in the transmission, neither in the devices, and in absence of eavesdroppers intercepting the communications, the bit string detected by Bob would be identical to the generated one by Alice.

Once the transmission and measurement of the quantum states is concluded, the verification stage begins with a partial sifting process. This process differs from the standard procedure employed in QKD. In the QZKP, Bob does not publish the bases on which he has measured, because otherwise he would reveal the h_1 value related to the secret, which violates the zero-knowledge principle. Instead, he simply announces to Alice the time instants in which he detected a single photon; then, both Alice and Bob selects just these bits from their respective strings, obtaining a sifted string, Δ_a^s for Alice and Δ_b^s for Bob, without revealing any information. The superindex s means that these are the sifted strings.

Then, an error estimation between Δ_a^s and Δ_b^s is performed, to evaluate the quantum bit error rate (QBER). Typically in QKD, this process is done by both Alice and Bob publishing the same fragment of key as plain text and comparing them. Thus, the number of errors obtained in the selected fragment represents an estimate of the error in the rest of the key. After this comparison, the published fragment is discarded. In QZKP, it is not possible to directly publish a clear fragment of Δ_a^s or Δ_b^s because it would reveal an information strongly related to the pre-shared secret s. Instead, the selected fragment of Δ_b^s in Bob, named δ_b with length n, is encrypted with h'_2 by means of an One-Time Pad (OTP) procedure, whereby a bit-by-bit XOR is made between δ_b and h'_2, obtaining $c' = ENC_{h'_2}(\delta_b)$. The fragment δ_b is built by selecting random positions (i.e. random bit elements) of Δ_b^s. This random selection of the position of the elements that conform δ_b could be carried out at Alice's side, by means of a Quantum Random Number Generator (QRNG) and, afterwards, sent to Bob. Thus, Bob sends c' to Alice who is able to decrypt it as $ENC_{h_2}(c') = ENC_{h_2}(ENC_{h'_2}(\delta_b)) = \delta_b$, if $h_2 = h'_2$. Finally, Alice computes the QBER estimation between δ_a and δ_b. In QZKP, only a rough estimation of the error rate is needed. Errors are neither corrected, nor is privacy amplification performed, since a secret symmetric key is not required at the end of the process.

Finally, once the QBER has been estimated, the validity of the proof is verified: if the QBER exceeds a certain predefined verification threshold, T_v, the proof will give a negative result; on the other hand, if $QBER<T_v$, the proof will be positive, proving the identity of Bob. The QZKP must be performed iteratively N times to guarantee a correct statistical estimate of the QBER.

3. Security proof

3.1. Security assumptions

A set of security assumptions must be taken into account during the execution of the protocol.

First of all, in the different security analysis of the QKD BB84 protocol [16,17], a set of assumptions on the adversary are considered that apply equally to the QZKP. Specifically, it is considered that:

1. Any adversary (external or participant) has unlimited computational power, even with access to a quantum computer;
2. The quantum channel is considered untrusted;

3. An external adversary is able to eavesdrop the communication on the classic channel but not to inject messages or modify the content of the information since the channel is assumed to be authenticated.

Moreover, a security perimeter for both Alice and Bob nodes must be guaranteed, in order to avoid any unauthorized physical access to the hardware; as well, appropriate cybersecurity measures are needed to ensure that no side-channels attacks can be performed in both the classical and quantum channels.

3.2. Key-derivation function details

Regarding the KDF, they are basic and essential components of current cryptographic systems. Their goal is to take some source of initial keying material and derive from it one or more cryptographically strong secret keys. Two types of KDF are defined, according to the standard NIST SP800-56C (r2) [15]:

- One-step key derivation: from a series of inputs, and a secret value, the cryptographic material is derived.
- Two-steps key derivation: prior to the derivation, a transformation of the secret is applied.

In the QZKP proposed here, a two-steps key derivation function with a counter mode is recommended [18]. The general structure has two main phases:

1. Extract phase: the keying material (s) and a salt value (t_0) are taken as input and a fixed-length pseudorandom key K_{IN} is extracted.
2. Expand phase: the pseudorandom key K_{IN} is expanded into several additional pseudorandom keys (h_1, h_2).

Additional input values in the second phase are a label and context, which are fixed values, and the required output length $(m + n)$. It is worth noting that, even though both sources of entropy, (h_1, h_2) are directly derived from the secret s, the actual encryption $\delta_a \oplus h_2$ is between two independent elements, since δ_a, even though derived from s, is actually built as a random string of bits and therefore independent of h_2.

3.3. QZKP security analysis

A ZKP has to guarantee completeness, soundness and zero-knowledge. In the following, the security of the proposed QZKP is demonstrated.

Completeness can be described as: given that both the verifier and the prover are honest and both know the secret, the prover is able to convince the verifier that he does indeed know the secret without revealing it. In the absence of malicious actors, since both parties are aware of the secret, they will get the same bases configuration for states preparation (Alice) or their measurement (Bob). Therefore, in an ideal scenario without photon losses and electronic noise, the results of Δ_a^r and Δ_b^r will be perfectly equivalent. Therefore, the estimate of the error would be $QBER = 0$ and Bob can fully convince Alice of the knowledge of the secret. However, as we will see in Section 4, in a realistic implementation, transmission losses and additional sources of noise could be present, increasing the measured the error rate to $QBER \neq 0$.

Assuming that the verifier is honest but the prover is malicious and unaware of the secret, it must be ensured that a dishonest prover is not able to convince the verifier that he knows the secret, except with a negligible probability, to prove the **soundness** of the proof. These malicious attempts are reflected in the measured QBER, resulting from the execution of the protocol. As

Optics EXPRESS

proposed by H.-K. Lo analysis [19], the QBER is given by:

$$QBER = \frac{p_{A,Z}^2 \cdot e_B^Z + p_{A,X}^2 \cdot e_B^X}{p_{A,Z}^2 + p_{A,X}^2} = \frac{(1-r)^2 p_B^X + r^2 p_B^Z}{2\left[(1-r)^2 + r^2\right]} \tag{1}$$

where, $0<r \leq 1/2$ is a variable parameter which depends on the value of the bits in h_1; $p_{A,Z} = (1-r)p_\mu$ and $p_{A,X} = rp_\mu$ are Alice's probabilities of preparing the states in each basis; $e_B^Z = p_B^X/2 = (1-p_B^Z)/2$ the error rate for the case when Alice prepares the state on Z basis and Bob measures on X basis; and $e_B^X = p_B^Z/2$ the error rate for the case when Alice prepares the state on X basis and Bob measures on Z basis. To try to cheat on Alice, Bob can carry out the following strategy. Given $p_B^Z = 0.5$ and $r = 1/2$, that is, 50% of the signal states are encoded in the Z basis and 50% in the X basis, since Bob does not know the value of h_1, he will measure the signals randomly. In this way he will guess correctly 50% of the times in the selected basis and of the other 50% he will get an uncorrelated result but he will guess correctly the value of the resulting bit half of the times. In total, he will get 75% of the measurements correct, but without knowing which elements are wrong and which are correct. This strategy raises the QBER to 25% without taking physical errors into account. Therefore, for a $T_v<25\%$ the proof would give a negative result, proving the soundness of the QZKP. This analysis agrees with what is obtained in Eq. (1) by introducing the parameters.

At last, if the prover is honest and the verifier a malicious player, the later learns nothing from the proof, demonstrating **zero-knowledge**. For this aim, Alice could try a similar strategy as in the previous scenario, preparing the quantum states using random bases, since she does not know the secret, s. Alice can also try to extract information from the string fragment δ_b during the error estimation process. However, she does not know the value of h_2', and without this value, it is not possible to correctly decrypt the OTP. If she tries to guess the value of each bit of c', the probability of success guessing all the elements will be: $P_{guess} = 1/2^n$. In both cases, the obtained QBER will behave similarly as before.

More complex attacks can be considered, such as collective attacks that can be performed in the classical part of the protocol and in the transmission of the quantum states. To the best of our knowledge, collective and coherent attacks on the quantum states differs from the ones analyzed for BB84 protocol, since in the QZKP case no information about the basis is published for distillation purposes. Thus, in the case of an eavesdropper with the capability of storing quantum states, he would not be able to extract information about the secret.

4. Protocol implementation

4.1. Experimental system

The protocol described in Section 2 has been implemented experimentally exploiting a pair of discrete-variable (DV) quantum cryptographic devices, already tested for standard QKD transmission also in a deployed network in coexistence with classical channels [20]. A schematic of the transmitter and receiver is shown in Fig. 2.

The DV-QKD prototypes are based on the implementation of the standard BB84 protocol with polarization encoding and decoy-state method [21]. Alice and Bob exploit a fully-automatic synchronized architecture, thanks to using two different distributed-feedback (DFB) lasers with identical nominal wavelength as sources for the quantum channel and of the auxiliary channel [22]. The quantum signal is composed by weak optical pulses with 20 ns time duration and 1 kHz repetition rate. The selected wavelength is 1310 nm, useful to avoid Spontaneous Raman scattering photons generated by co-propagating classical sources in the C-band. The decoy-state is implemented as signal (μ), weak decoy-state (ν) and vacuum states (0), each of them characterized by a pre-determined probability of occurrence, p_μ, p_ν, p_0, respectively. The measured losses of the receiver module are about 5 dB. The proposed scheme has been implemented firstly in a

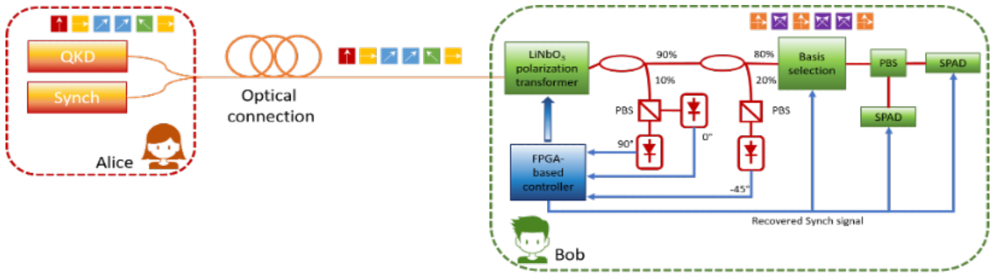

Fig. 2. Schematics of the pair of discrete-variable quantum cryptographic devices.

back-to-back (B2B) scenario, considering two cases: 1) all actors are honest and 2) the prover is a malicious user who does not know the secret and randomly measures the quantum states received from the verifier.

After the validation of the QZKP in these first, short-distance experiments, the distance between Alice and Bob was increased in order to evaluate the impact on the QBER in the honest condition, ensuring that a relevant number of false positives or false negatives do not occur. For this aim, the QZKP has been tested in a point-to-point standard single-mode fiber (SSMF) link and its performance has been measured, in order to estimate the impact of losses on the QZKP solution. The different distances were emulated by inserting optical attenuation in a controlled manner. All the intermediate elements were previously characterized to determine the initial losses introduced by the setup, these being a total of $2.5dB$. Taking into account that the losses in a standard optical fiber are $0.21dB/km$, the setup establishes an emulated initial distance between the devices of $11.9km$. Thus, the evaluated propagation distances ranges from 11.9 km to 60.6 km, covering a link attenuation from 2.5 dB to around 13 dB.

4.2. Parameter settings

In all the experiments carried out for the honest case, the protocol parameters have remained constant except for the length of sifted string $\Delta^s_{a,b}$, named L_Δ, that were modified to cover string lengths between 256 *bit* and 2048 *bit*. In the case of the length n of $\delta_{a,b}$, the use of 15% of the total of $\Delta^s_{a,b}$ was established for the QBER estimation. All the values of the parameter settings are collected in Table 1.

The same approach was applied for the execution of the dishonest case but, in this case, the protocol was modified in Bob's side in order to perform random measurements due to the assumption that he ignores the secret, as explained in Section 3. For each experiment, we provide in Table 1 the emulated distance in km, being B2B the back-to-back configuration; the losses in dB; the length L_Δ of $\Delta^s_{a,b}$; the number of iteration that the QZKP has been executed; the average time the system takes for generating 1 bit; the average QBER estimation; and the standard deviation of the QBER. As we can see in Fig. 3, the time needed for the generation of 1 *bit* shows a logarithmic behaviour when increasing the losses in the honest case.

4.3. Analysis of results

4.3.1. Comparison between honest and dishonest cases

For each case, the QZKP procedure has been run for more than 170 iterations, as shown in Table 1. The outcomes obtained for the average estimated QBER and the standard deviation of the results are shown in Table 1 and Fig. 4.

When verifier and prover are honest (blue stars), the QBER is far below the standard security threshold value of 11% [16]. In particular, the measured average QBER shows an error floor of

Table 1. Parameter settings established during the QZKP executions of the honest and dishonest cases and results of the emulated distance in km, being B2B the back-to-back configuration; the losses in dB; the length L_Δ of $\Delta^s_{a,b}$; the number of iteration that the QZKP has been executed; the average time the system takes for generating 1 bit; the average QBER estimation; and the standard deviation of the QBER.

Distance (km)	Losses (dB)	L_Δ (bits)	Iterations	Time (s)	QBER	σ_{QBER}
Honest Case						
B2B	0	2048	173	0.033	0.029	0.007
11.90	2.50	1024	189	0.077	0.028	0.008
13.62	2.86	1024	858	0.065	0.033	0.009
16.14	3.39	1024	165	0.084	0.024	0.009
17.48	3.67	1024	171	0.089	0.029	0.009
20.19	4.24	1024	612	0.088	0.033	0.010
22.62	4.75	512	229	0.119	0.023	0.011
27.81	5.84	512	10	0.135	0.033	0.014
32.48	6.82	512	10	0.166	0.027	0.009
37.38	7.85	512	10	0.216	0.028	0.011
44.00	9.24	512	11	0.294	0.021	0.010
49.00	10.29	256	11	0.376	0.040	0.022
51.14	10.74	256	11	0.406	0.028	0.016
56.33	11.83	256	10	0.520	0.037	0.013
60.62	12.73	256	26	0.465	0.033	0.018
Dishonest Case						
B2B	0	2048	190	0.030	0.266	0.015

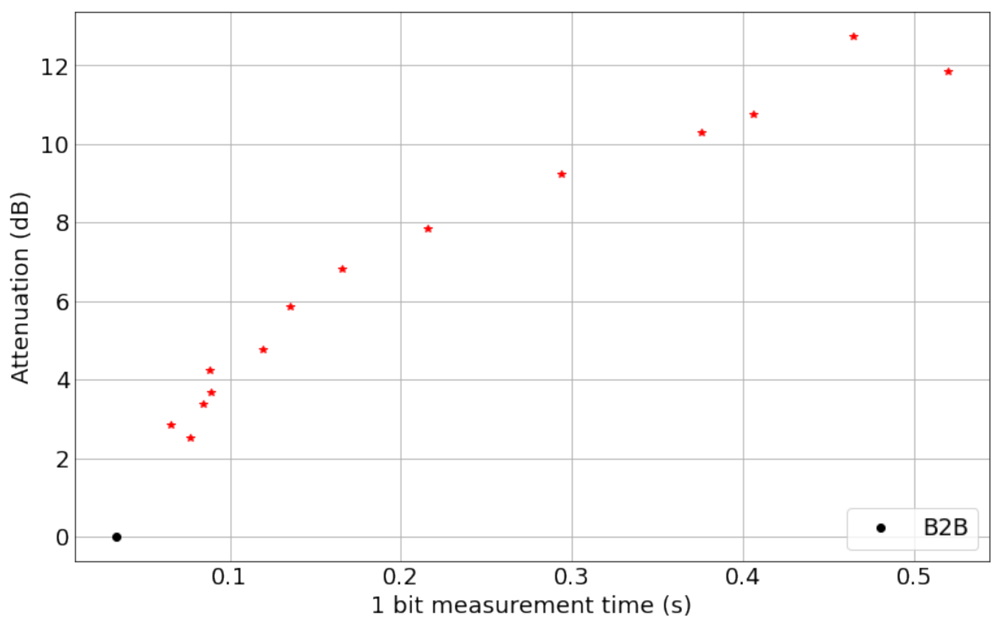

Fig. 3. Amount of time needed for the generation of 1 bit in the honest case. The time needed shows a logarithmic behaviour when increasing the losses. The black dot corresponds to the back-to-back (B2B) configuration.

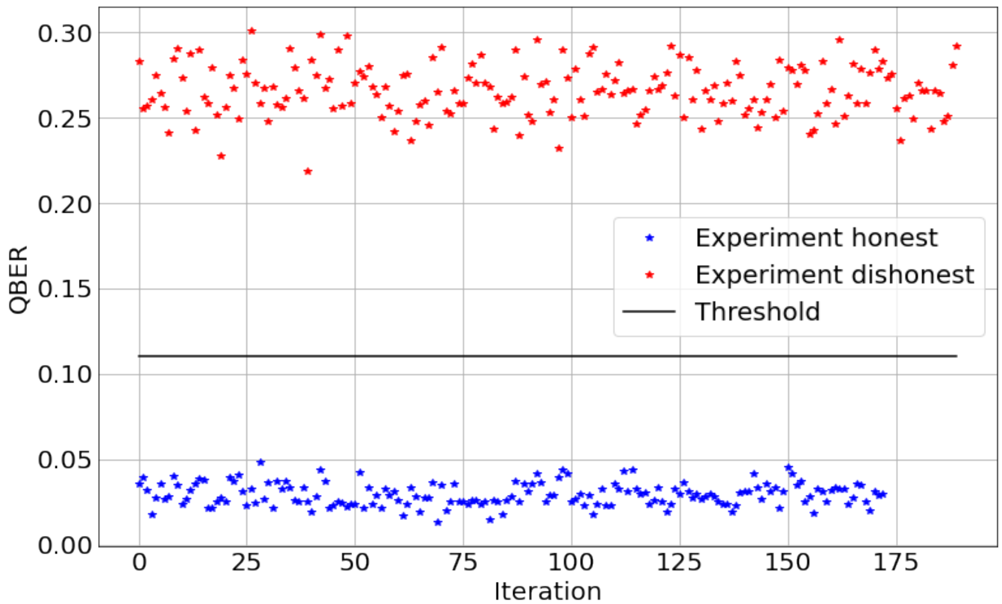

Fig. 4. Experimental results of the QBER in a back-to-back setup. Blue stars: all players are honest, Red stars: dishonest prover. The black line refers to the standard security threshold value of 11% for the BB84 protocol [16].

2.9%, owing to the non-idealities of the system, as the finite polarization extinction ratio (ER) of the polarization beam splitter (PBS), limited to 20 dB, and the presence of dark counts in the two employed single-photon avalanche detectors (SPADs). On the other hand, in presence of a dishonest prover (red stars), the QBER increases up to 26.6%, overcoming the security limit of 11% of the BB84 protocol. The QBER performance is stable in time over all the 170 iterations; some fluctuations are visible both for honest users and dishonest prover, owing to the limited number of bits used for the estimation of the QBER, which is a 15% of m; in case of a raw key length of $m = 2048$ bits, the estimation is performed on $n = 307$ bits. The standard deviations for the two considered configurations are 0.7% and 1.5%, respectively. The stronger fluctuation in the dishonest case comes from the limited number of detections and from the statistical behavior of the prover, who measures randomly with equal probability for each basis, while the bases sent by Alice are $N_\mu^Z = p_\mu \cdot m \cdot (1-r)$ in Z and $N_\mu^X = p_\mu \cdot m \cdot r$ in X, being p_μ the signal probability, m the length of h_1. Anyway, the presence of the fluctuation does not introduce any false positive or false negative condition, permitting to complete the user authentication in all iterations.

4.3.2. Results over the distance

The measured QBER performance in function of the experimented additional losses is reported in Fig. 5 and in Table 1.

As before, several acquisitions have been measured for each propagation length, corresponding to several executions of the QZKP. In Fig. 5, the average values of the QBER together with their standard deviations are shown. The minimum attenuation at 0 dB corresponds to the already described B2B scenario. As can be seen, as the link losses increase, the QBER increases slightly, although it is always far below from the security threshold of 11%. As already explained, a minimum error rate close to 3% is present, owing to the limited polarization ER generated by the intrinsic properties of the optical devices and by unavoidable misalignments arising before the PBS. An improvement in the optical components and of the polarization alignment would reduce

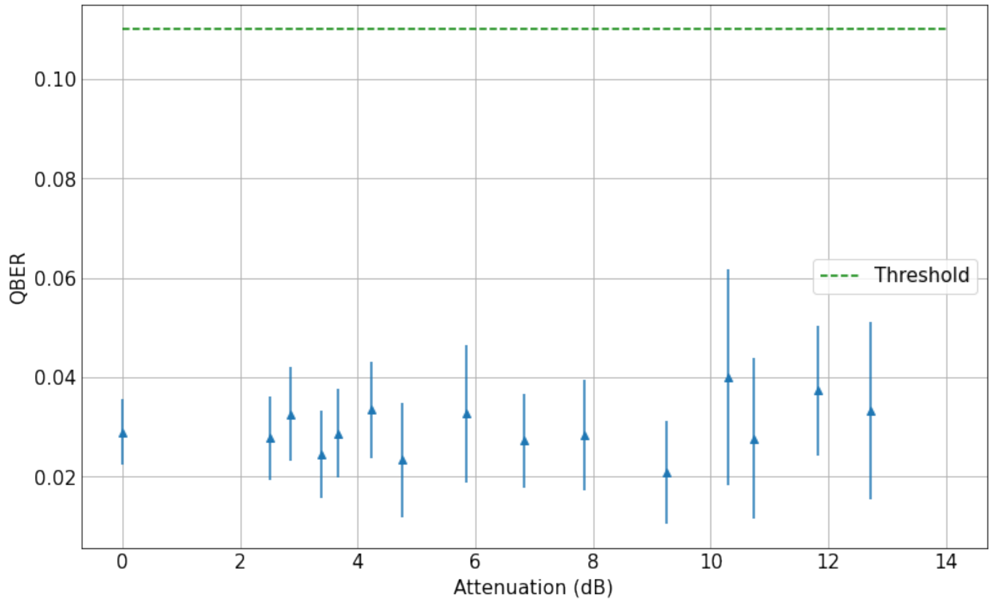

Fig. 5. Measured QBER performance together with the associated standard deviations versus additional link losses in case of honest parties. The green dashed line refers to the standard security threshold value of 11% for the BB84 protocol [16].

the QBER to values less than 1% in the B2B scenario, which would allow us to appreciate with greater detail the gradual increase in QBER with respect to attenuation. In addition, it is observed that the greater the losses, the greater the dispersion of the measured QBER. This is expected due to the limited number of bits used during the QBER estimation influenced by the reduction of the length of Δ_a when increasing the attenuation of the system, since the measurement time duration required to obtain the established Δ_a also increases. In the B2B scenario, the generation of 1 *bit* takes an average time of 0.033 *s*, with a QBER deviation of 0.7% corresponding to the full protocol execution, while for 12.7 *dB* the generation of 1 *bit* takes an average time of 0.465 *s*, giving a standard deviation of 1.8%.

It is worth to point out that the dishonest case has only be executed in a B2B setup to demonstrate the impact in the QBER when a malicious prover who does not know the secret is present during the execution of the QZKP. This corresponds to the best case scenario for the attacker as there is not additional transmission losses due to the increase in the distance during the proof.

4.3.3. Comparison between real and estimated QBER

Finally, given that the QBER used to accept or reject the authentication of a user is an estimate extracted from a fragment of length n of Δ_a and Δ_b, the variation that exists between this estimate and actual value of QBER has been evaluated for the B2B setup and for raw string outcomes from the largest distances: 22.6 *km* to 60.6 *km*. As reported before, the length of the fragment used to estimate the experimented QBER is the 15% of the total segment. To obtain the real value of the QBER, each of the elements of Δ_a and Δ_b have been compared bit by bit, obtaining the results showed in Fig. 6 - blue down triangles. For its part, the estimation is carried out over the values of L_Δ gathered in Table 1, obtaining the results showed in Fig. 6 – red up triangles.

As we can see, the difference between the estimated value and the real one is less than 1% in the best case at 4.75 dB and an underestimation of 25% in the worst case at 9.24 dB, without any negative impact in the authentication test, a behavior that remains constant for all the lengths of $\Delta_{A,B}$ used.

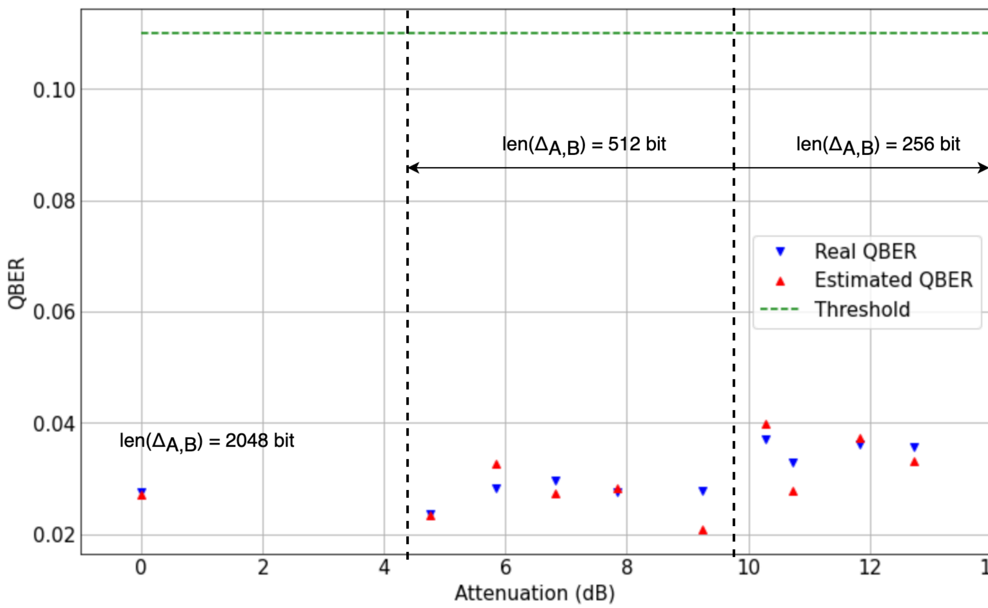

Fig. 6. Comparison of the real QBER of (Δ_a, Δ_b), blue down triangles, versus the estimated QBER obtained from the fragments (δ_a, δ_b), red up triangles, for different string lengths.

5. Conclusions

To benefit from the advantages provided by QKD, the design of an end-to-end secure cryptographic system is required, where the demonstration of the identity of the two communicating users is one important step to achieve this goal. For this aim, the proposed QZKP is a tool that allows the authentication of users in networks that already have a quantum communications infrastructure without disclosing any personal information about the user or his secret. Based on purely quantum processes the tool provides a quantum-safe authentication mechanism that, not only adds another layer of security to the entire ecosystem, but is also easily implementable with the technology available for QKD and more efficient because it does not require full error correction steps. Regarding the security of the protocol, the increase in the order of 25% produced in QBER has been demonstrated, both theoretically and experimentally in a back-to-back scenario, between an honest case, where $QBER = (2.9 \pm 0.7)\%$, and an attempt by a malicious prover to guess the bases associated with the derived h_1 function from the secret, where $QBER = (26.6 \pm 1.5)\%$. In addition, the proof is also valid for long distances, being demonstrated for metropolitan areas ($\approx 60\,km$), where the increase in the QBER is appreciated as well as a greater dispersion of the data. It is worth to point out that the QZKP has not presented a false positive or false negative, thus demonstrating the robustness of the proof. The QZKP has been tested and guarantees completeness, soundness and zero-knowledge, against different strategies from a malicious player. Finally, we have demonstrated that, for lengths of 2048 *bit*, 512 *bit* and 256 *bit*, an error estimation using 15% of Δ_a and Δ_b, provides us with a reliable QBER value that can be used to validate or not the QZKP.

Funding. EIT Digital; Digital Europe Programme (EuroQCI Spain-101091638); Horizon 2020 Framework Programme (QuantERA II - 101017733); Agencia Estatal de Investigación (PCI2022-133009); NextGenerationEU (PRTR-C17.I1);

Optics EXPRESS

Comunidad de Madrid - Programa de Acciones Complementarias (Madrid Quantum); HORIZON EUROPE Framework Programme (QSNP-101114043).

Disclosures. MIGC: Indra Sistemas S.A. (E), DB: Cohaerentia S.r.l (E).

Data availability. All data generated and analyzed are presented in the main text. No additional data were generated or analyzed in the presented research.

References

1. S. Goldwasser, S. Micali, and C. Rackoff, *The knowledge complexity of interactive proof-systems* (Association for Computing Machinery, 2019).
2. A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems," *Proceeding of Advances in Cryptology*, A. M. Odlyzko, ed. (Springer, 1986), pp. 186–194.
3. D. Gabay, K. Akkaya, and M. Cebe, "Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs," IEEE TVT **69**(6), 5760–5772 (2020).
4. M. Backes, J. Camenisch, and D. Sommer, "Anonymous yet accountable access control," *Proceedings of the ACM Workshop on Privacy in the Electronic Society* (ACM, 2005), pp.40–46.
5. M. Blum, P. Feldman, and S. Micali, *Non-interactive zero-knowledge and its applications* (ACM, 2019).
6. E. B. Sasson, A. Chiesa, C. Garman, *et al.*, "Zerocash: decentralized anonymous payments from bitcoin," *Proceeding of IEEE Symposium on Security and Privacy* (IEEE, 2014), pp. 459–474.
7. C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Theor. Comput. Sci. **560**(1), 7–11 (2014).
8. P. Wallden, V. Dunjko, A. Kent, *et al.*, "Quantum digital signatures with quantum-key-distribution components," Phys. Rev. A **91**(4), 042304 (2015).
9. M. I. Garcia-Cid, L. O. Martín, D. D. Martín, *et al.*, "A Feasible Hybrid Quantum-Assisted Digital Signature for Arbitrary Message Length," arXiv, arXiv.2303.00767, (2023).
10. C. H. Bennett, G. Brassard, C. Crépeau, *et al.*, "Practical quantum oblivious transfer," *Proceeding of Advances in Cryptology*, J. Feigenbaum, ed. (Springer, 1992), pp. 351–366.
11. Y. Kurochkin, "Quantum cryptography with floating basis protocol," Proc. SPIE **5833**, 213–221 (2005).
12. V. Kurochkin and Y. Kurochkin, "Principles of the new quantum cryptography protocols building," Phys. Part. Nuclei Lett. **6**(7), 605–607 (2009).
13. Z. Wei, W. Wang, Z. Zhang, *et al.*, "Decoy-state quantum key distribution with biased basis choice," Sci. Rep. **3**(1), 2453 (2013).
14. A. S. Trushechkin, P. A. Tregubov, O. Evgeniy, *et al.*, "Quantum-key-distribution protocol with pseudorandom bases," Phys. Rev. A **97**(1), 012311 (2018).
15. E. Barker, L. Chen, and R. Davis, "Recommendation for key-derivation methods in key-establishment schemes," Standard NIST SP 800-56C (r2), (2020).
16. P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Phys. Rev. Lett. **85**(2), 441–444 (2000).
17. R. Renner, N. Gisin, and B. Kraus, "Information-theoretic security proof for quantum-key-distribution protocols," Phys. Rev. A **72**(1), 012332 (2005).
18. H. Krawczyk and P. Eronen, "HMAC-based Extract-and-Expand Key Derivation Function (HKDF)," RFC 5869 (2010).
19. H. K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," J Cryptology **18**(2), 133–165 (2005).
20. A. Gatto, M. Brunero, M. Ferrari, *et al.*, "A BB84 QKD field-trial in the Turin metropolitan area," *Photonics in Switching and Computing Conference*, Vol. 2 of 64 OSA Technical Digest, (Optica Publishing Group, 2021), paper Tu1A.
21. X. Ma, B. Qi, Y. Zhao, *et al.*, "Practical decoy state for quantum key distribution," Phys. Rev. A **72**(1), 012326 (2005).
22. A. Gatto, J. P. Brito, M. Brunero, *et al.*, "Quantum technologies for future quantum optical networks," *Proceeding of International Conference on Optical Network Design and Modeling* (IEEE, 2021), pp. 1–5.