Entropy **2012**, *14*, 2531-2549; doi:10.3390/e14122531

OPEN ACCESS

entropy

ISSN 1099-4300

www.mdpi.com/journal/entropy

Article

Improving Classical Authentication over a Quantum Channel

Francisco M. Assis [1], Aleksandar Stojanovic [2,3], Paulo Mateus [2,3,*] and Yasser Omar [4,5]

[1] Department of Electrical Engineering, Universidade Federal de Campina Grande, 58.429-970 Campina Grande, Paraíba, Brazil; E-Mail: fmarcos@petri.dee.ufcg.edu.br

[2] Department of Mathematics, IST, Technical University of Lisbon, 1049-001 Lisboa, Portugal; E-Mail: stojanovic.alex1@gmail.com

[3] Security and Quantum Information Group, Instituto de Telecomunicações, 1049-001 Lisbon, Portugal

[4] CEMAPRE, ISEG, Technical University of Lisbon, 1200-781 Lisboa, Portugal; E-Mail: yasser.omar@iseg.utl.pt

[5] Physics of Information Group, Instituto de Telecomunicações, 1049-001 Lisbon, Portugal

* Author to whom correspondence should be addressed; E-Mail: pmat@math.ist.utl.pt.

Received: 28 April 2012; in revised form: 28 July 2012 / Accepted: 26 November 2012 / Published: 11 December 2012

Abstract: We propose a quantum protocol to authenticate classical messages that can be used to replace Wegman–Carter's classical authentication scheme in quantum key distribution (QKD) protocols. We show that the proposed scheme achieves greater conditional entropy of the seed for the intruder given her (quantum) observation than the classical case. The proposed scheme is suitable for situations where the shared symmetric key used in authentication becomes dangerously short (due to noise or eavesdropping), and there is a threat that it might be completely consumed without being replaced. Our protocol is an improvement over a classical scheme by Brassard and takes advantage of quantum channel properties. It is motivated by information-theoretical results. We stress that the proposed authentication protocol can also be used as an independent authentication protocol that is not a part of a QKD. However by adopting it, QKD becomes a fully quantum protocol. We prove that quantum resources can improve both the secrecy of the key generated by the PRG and the secrecy of the tag obtained with a hidden hash function. We conclude that the proposed quantum encoding offers more security than the classical scheme and, by applying a classical result, we show that it can be used under noisy quantum channels.

Keywords: quantum communication; quantum authentication; quantum key maintenance; QKD recovery; entropy bound

1. Introduction

The authentication of public messages is a fundamental problem nowadays for bipartite and network communications. The scenario is the following: Alice sends a (classical) message to Bob through a public channel, together with an authentication tag through a private or public channel. The tag will allow Bob to verify if the message he received via the public channel has been tampered with or if it is indeed the authentic message, originally sent by Alice. A third character, Eve, wants to sabotage this scheme by intercepting Alice's message and sending her own message to Bob, together with a false tag which will convince Bob he is receiving the authentic message. For instance, one could imagine that Alice is sending Bob her bank account number, to which Bob will transfer some money, and Eve wants to interfere in the communication in such a way that Bob will receive her bank account number believing it is Alice's one, thus giving his money to Eve. Authentication tags allow to separate the secrecy problem in message transmission from the authentication problem and they are useful even if a secure communication channel is available [1].

In quantum key distribution (QKD) protocols [2] it is fundamental to authenticate classical messages since the communicating agents need an authenticated channel to publish in which basis they prepared/measured their qubits. For such authentication to happen it is assumed that each pair of agents shares an initial small (classical) key that is given at the startup of the quantum network and allows the QKD protocol to bootstrap. The authentication scheme commonly used in QKD is the Wegman–Carter protocol [1], which requires the authentication key to be used only once, and therefore the key needs to be renewed after being used. Assuming ideal conditions, QKD allows the shared key between two agents to be renovated with perfect security and so the agents can communicate with a high level of security for long time. If for some reason this key is lost, the two agents sharing this key cannot communicate securely anymore. We stress that in a realistic scenario, where the quantum communication channels might lose or modify qubits, it may happen that the shared key between the parties is consumed without being renovated by a new QKD round. There are several ways to address this problem. For instance, the parties might meet physically, rely on asymmetric cryptography or communicate via a trusted service in order to share the authentication key. This situation needs careful analysis, as in many cases it is impossible for parties to meet physically or to have trusted services. Moreover, relying on asymmetric cryptography might be a limitation in the future, as it could be broken with quantum computers.

In this paper we address this problem by proposing a scheme for which the conditional entropy of the intruder knowledge over a random string given her observation is greater than the classical case. To this end, we propose an authentication protocol that does not consume the shared key, at the price of having lower security than the one provided by Wegman–Carter scheme. Two approaches are considered. Firstly, a pseudorandom generator is considered to approximate a fair random generator. Note, that even empowered with a quantum computer, and given current knowledge, it is not possible to attack

in polynomial-time the proposed protocol. For this reason, it should be considered as an alternative to asymmetric cryptography in a situation where the authentication key is about to be lost, and the communication between two agents is threatened. A second approach is to consider almost-random string that consists of a random sequence where ℓ out of k bits, with $\ell << k$, are determined by knowing the seed (or key) and the remaining bits are pure random numbers. The idea is to consider ℓ large enough so that if Eve wants to interfere with the protocol she will be detected with high probability. On the other hand, it should be small enough in order to have small keys. Moreover, by using the proposed protocols, QKD becomes a fully quantum protocol. The proposed protocol will work with noisy channels, assuming that a few blocks of qubits of size k are able to be sent without (or with negligible) noise, even if the majority of these blocks are lost. Our protocol takes advantage of a quantum channel to increase the entropy of the random string, from the intruder's point of view, in the computationally secure scheme by Brassard [3] for classical authentication. This scheme is presently used in classical authentication schemes [4–6]. Note that Brassard's scheme is itself a modification of the Wegman–Carter protocol, and therefore it is a natural candidate for application in QKD. Brassard showed that a relatively short seed of a pseudorandom generator (PRG) can be used as a secret key shared between Alice and Bob that will allow the exchange of at least computationally-secure authentication tags. We extend Brassard's protocol to include quantum-encoded authentication tags, and, as expected, we show that our approach attains higher security than Brassard's scheme by using the fact that quantum encoding scheme has higher entropy from the intruder's point of view.

It is essential to consider PRGs or almost-random generators (ARGs) and not random generators based on thermal noise (or other methods), as the strings generated by the latter cannot be predicted by two physically separated parties, even if they share some kind of key. The security of modern PRG's is based on the alleged hardness of some problems of number theory, e.g., the factorization of a large Blum integer, such as the Blum–Blum–Shub PRG [7]. However, most of the research concerning attacking PRGs has been focused in distinguishing with some advantage the pseudorandom generated string from a uniformly generated one [7] and not to recover the PRG seed (the latter problem is harder than the former [8]). The problem becomes much harder if this generated string is encoded in a quantum channel and the adversary can only access the generated string with a certain level of uncertainty (and might not even know the large Blum integer to factor). In this case, even in the possession of an oracle/quantum computer that is able to solve these hard problems, it is not obvious how to recover efficiently the seed of a PRG given a noisy generated string of polynomial size or to obtain any probabilistic advantage to predict the next bit. There have been several results addressing the use of PRG's and public-key cryptosystems (PKC) together with quantum cryptography [9–11]. It is even well known that there exist PKC's if and only if there exist PRG's [12]. However, as discussed above, for this equivalence to hold, the setup of the PRG must be known by the attacker (for instance the Blum integer must be known by the attacker in the Blum–Blum–Shub PRG), where this setup is the PRG counterpart of the public key in the PKC. In our approach, we assume that this setup is not known by the attacker, which essentially is equivalent to considering that the public key of the cryptosystem is not known by the attacker. By hiding the public key in a PKC, the system becomes a simple symmetric cryptosystem. Thus, the hardness of attacking a PRG where such setup is unknown to the attacker is at the same level of attacking a symmetric cryptosystem.

For the results in this paper, we have used several concepts and theorems from information theory (Cover and Thomas [13]), whose notation is adopted in the entire paper. In the following comments about channel models, $H(X)$ and $I(X;Y)$ stand for the entropy of the random variable X and the mutual information between random variables X and Y, respectively. Two different models are considered to set fundamental limits on communication secrecy. In the first model, Alice and Bob share a secret key K used by Alice to create a cipher text C as a function of the message M, and Eve is assumed to receive an identical copy of C (which means she owns a noiseless channel). Unconditional security is defined by $I(M;C) = 0$. The second model, introduced by Wyner [14], assumes noisy channels and no *a priori* secret key. A secrecy capacity is defined to be the largest transmission rate such that Bob's decoding error is arbitrarily small and Eve's equivocation rate [15] is arbitrarily close to the transmission rate. It is noticed that the result due to Shannon for the first model is a very negative result in contrast with the results obtained for the second one, namely the wiretap channel model [14]. Concerning message authentication, only the first (noiseless) model was studied by Simmons's work [16]. However, recently Poor *et al.* [17] introduced new limits for message authentication based on the second (noisy) model. We note that Brassard's proposal concerns the first model (noiseless), whereas our generalization is dealing with the second model. This is because quantum channels are noisy from the point of view of the attacker (Eve cannot read perfectly from a noisy quantum channel).

The paper is organized as follows. In Section 2 we present preliminary results concerning Brassard's protocol. In Section 3 we discuss how quantum encoding increases the equivocation from the adversary's point of view, even when PRG's are used instead of fair coin tossing. In Section 4, we show that by changing the hash function with the generated PRG we improve the security of the scheme, and we finish by discussing the robustness of the proposed authentication scheme under noisy channels.

2. Preliminary Results

In this section we set up basic notation, briefly review Brassard's protocol and describe our proposal. We conclude the section with a negative result on the robustness of an attackable PRG when its output is hidden by a specific quantum coding.

We denote $\mathcal{M}$ the set of messages and $\mathcal{T}$ the set of tags, where $\log|\mathcal{M}| >> \log|\mathcal{T}|$. As hash functions are an important ingredient for all protocols described here we start by presenting their formal definition [18]:

Definition 2.1 (ε − almost strongly universal-2 hash functions) *Let $\mathcal{M}$ and $\mathcal{T}$ be finite sets and call functions from $\mathcal{M}$ to $\mathcal{T}$ hash functions. Let ε be a positive real number. A set $\mathcal{H}$ of hash functions is $\varepsilon-$almost strongly universal-2 if the following two conditions are satisfied*

(1) The number of hash functions in $\mathcal{H}$ that takes an arbitrary $m \in \mathcal{M}$ to an arbitrary $t \in \mathcal{T}$ is exactly $|\mathcal{H}|/|\mathcal{T}|$.

(2) The fraction of those functions that also takes $Y' \neq Y$ in $\mathcal{M}$ to an arbitrary $T' \in \mathcal{T}$ (possibly equal to T) is no more than ε.

The number ε is related to the probability of guessing the correct tag with respect to an arbitrary message Y. Notice that the smaller ε is, the larger $|\mathcal{H}|$ is.

For additional details on universal-2 functions we refer the reader to [1].

Brassard's protocol (see Figure 1) makes use of two secret keys. The first one, $U^{(l)}$, specifies a fixed universal-2 hash function $h \in \mathcal{H}$, where $l = \lceil \log |\mathcal{H}| \rceil$. The second specifies the seed $X^{(n)} \in \mathbb{Z}_2^n$, for a PRG, a sequence of n bits. Observe that Brassard's protocol is a weakening of the Wegnar–Carter protocol [1] where pure random number are replaced by PRG's at the price of loosing perfect security but making the protocol much more practical. The main advantage of our first quantum-enhanced protocol proposed here (see Figure 2) is replacing the classical gate XOR of Brassard's protocol with a quantum coder (QC) similar to that used in the BB84 protocol [2]. As we shall see later on, the key $U^{(l)}$ may be discarded. Assume that Alice and Bob agree on two orthonormal bases B_0 and B_1 for the 2-dimensional Hilbert space,

$$B_0 = \{|0\rangle, |1\rangle\} \quad \text{and } B_1 = \left\{ |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right\}$$

These bases will be used to prepare four quantum states. We shall refer to this preparation process as *quantum coding*. For each bit of the $k = \lceil \log |\mathcal{T}| \rceil$ bits long tag $T_Y = h(Y)$, Alice prepares a quantum state $|\psi\rangle = |\psi\rangle\,(X_i, (T_Y)_i)$ determined by the bit X_i from the PRG and the corresponding bit $(T_Y)_i$ of 2-radix representation of the tag T_Y. Then, if the bit $X_i = 0$, Alice prepares $|\psi\rangle$ using basis B_0, such that

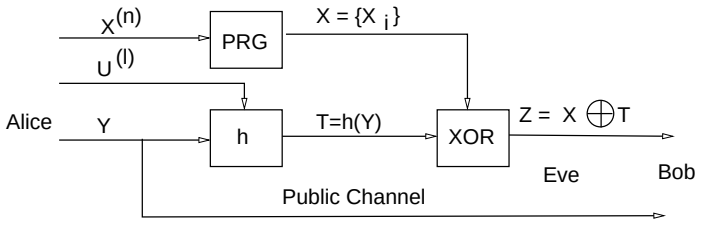
$$|\psi\rangle = \begin{cases} |0\rangle & \text{if } (T_Y)_i = 0 \\ |1\rangle & \text{if } (T_Y)_i = 1 \end{cases} \tag{1}$$

Similarly, if the bit $X_i = 1$, Alice prepares $|\psi\rangle$ using basis B_1, such that

$$|\psi\rangle = \begin{cases} |+\rangle & \text{if } (T_Y)_i = 0 \\ |-\rangle & \text{if } (T_Y)_i = 1 \end{cases} \tag{2}$$

After qubit generation, Alice sends the separable state $|\psi_Y\rangle^{\otimes k}$ to Bob through a noiseless quantum channel and the message Y through an unauthenticated classical channel. At reception, Bob performs measurements to obtain a sequence of k bits from the quantum encoded version of $h(Y)$. For the i-th received qubit, Bob measures it using the basis B_0 or B_1 depending on whether the i-th bit of X is 0 or 1, respectively, in that way a k-bit long string $T' = h'\left(|\psi\rangle^{\otimes k}\right)$ will be recovered.

Figure 1. Brassard's classical authentication protocol [3].

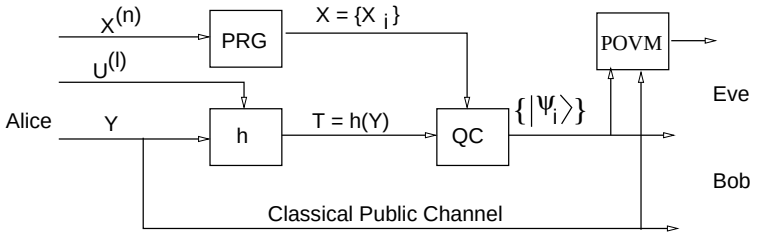


Because the quantum channel is assumed to be perfect, Bob recognizes that the message is authentic if $h' = h(Y_B)$, where Y_B is the message received from the classical channel. Otherwise, Bob assumes that Eve tried to send him an unauthentic message. This concludes the authentication protocol for one message. Throughout this article it is always assumed that the above coding rule is public.

Even though we assume for the moment a noise-free quantum channel, we observe that if the quantum channel is noisy, the only piece of information requiring error-protecting codes is the block of bits $(T_Y)_i$ of the tag T_Y. The sequence of bases to be prepared by Alice and Bob is known a priori, determined locally by the sequence of bits from the PRG. We leave for future work the evaluation of the effects of error-correcting codes on the bits of T_Y.

In a warning against alleged collective attacks, we notice that our analysis allows Eve to make general attacks (suggested in Figure 2 by the block labeled as POVM) without being detected. This assumption agrees with the fact that the channel is noisy and so, we do not distinguish between noise and Eve's interference. Our results are robust to such powerful assumptions for the attacker. Note that our quantum scheme aims at minimizing the key length for one-way transmission. Another example of such approach is given in [19]. Next we focus on crucial aspects of the PRGs.

Figure 2. First proposal of quantum-enhanced authentication scheme.

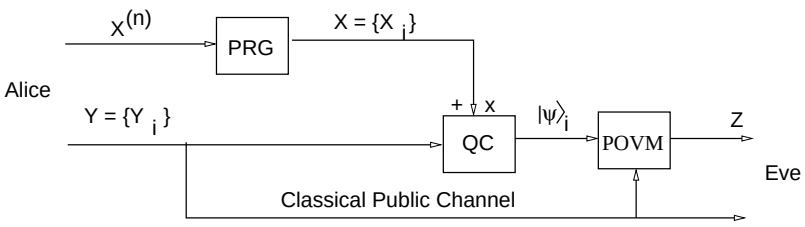


Weak Pseudorandom Generators

Clearly, it is important to understand how secure the authentication code described above is. As we shall see, the security of the authentication code is deeply related to the quality of the pseudorandom generator. The quality of a pseudorandom generator is evaluated by the hardness to discriminate its pseudorandom sequence output from a truly random sequence or by the hardness to find its seed. The first quality evaluation relates to the PRG's robustness against *distinguishing attacks*, the second relates to the so-called *state recovery attacks*. In [8] it is shown that state recovery attacks are harder than distinguishing attacks.

As a matter of fact, if the pseudorandom generator can be attacked by a quantum computer, so does the authentication code. To set this result we refer to Figure 3, which describes a simple scheme to assist us the proof. In this scheme, we simply allow Eve to compare a sequence $\{Y_i\}$ of classical bits with the corresponding sequence $\{Z_i\}$ obtained from the measurement apparatus POVM.

Figure 3. Scheme for Theorem 2.3.



Recall that a pseudorandom generator is a polynomial-time family of functions $G = \{G_n : \mathbb{Z}_2^n \times \mathbb{N} \to \mathbb{Z}_2\}_{n\in\mathbb{N}}$ where $\mathbb{Z}_2$ is the set $\{0,1\}$ and G_n is the pseudo-generator for seeds with n-bit size, that is, $G_n(X^{(n)}, i)$ returns the i-th bit generated from n bits long seed $X^{(n)}$. Pseudorandom generators are expected to be indistinguishable from fair coin tossing by a polynomial-time algorithm (more details in [20]). In the following definition we write $B^{p(n)} = \left(G(X^{(n)}, i_1), G(X^{(n)}, i_2), \ldots, G(X^{(n)}, i_{p(n)})\right)$ to denote a subsequence of $p(n)$ (not necessarily contiguous) bits generated by G.

Definition 2.2 We say that a pseudorandom generator G is *attackable in (quantum/probabilistic) polynomial time* if there exists a (quantum/probabilistic) polynomial time algorithm P and polynomial p such that if P is fed with a subsequence of $p(n)$ (not necessarily contiguous) generated bits $X^{p(n)}$ of G we have that:

$$H(X^{(n)} - P(B^{p(n)})) \in O(2^{-n}).$$

For a pseudorandom generator to be attackable, there must exist an algorithm (quantum or probabilistic) that receives a subsequence of $p(n)$ generated bits (not necessarily contiguous) and is able to compute the seed up to a negligible uncertainty. We observe that the security/randomness of the pseudorandom generator cannot be grounded in the fact that the attack can only be performed to a contiguous subsequence of generated bits, since the attacker may have access just to a particular set of generated bits. Indeed, if the attack required say, a contiguous subsequences of bits, a simple defense would consist of discarding some generated bits. A simple example of pseudorandom generators that can be attackable in polynomial time is the pseudo-number generator based on linear congruence [8].

Theorem 2.3 If a pseudorandom generator G is *attackable in (quantum/probabilistic) polynomial time* then the scheme presented in Figure 3 is not secure in polynomial-time for a quantum adversary that has access to $Y = \{Y_i\}$.

Proof. Since G is attackable, there exists a quantum polynomial time algorithm P and a polynomial p such that if P is fed with $p(n)$ bits of the string X generated by G, then P computes (up to negligible uncertainty) the seed $X^{(n)}$ of G. So it is enough to show that Eve, upon capturing the qubits generated by $\mathbb{QC}$ (the quantum coder in page 5), is able to recover (with non-negligible probability) $p(n)$ bits of X.

Indeed, assume that Eve has captured $8p(n)$ qubits $|\psi\rangle_i, i : 1 \ldots 8p(n)$ and has measured them in a random basis (that is, either the computational or the diagonal basis). Eve can now verify if $Z_i = Y_i$. If this occurs, Eve does not know if the basis chosen to encode the Y_i bit was the basis she measured or if she got with $\frac{1}{2}$ probability the correct bit due to encoding in the wrong basis. However, if the outcome is different (that is, $Y_i \neq Z_i$), then she knows that the basis at the i-th bit is the basis she did not choose to measure, because no mismatch would be possible if the encoding was performed with the same basis. In the latter case, she knows that X_i is either 0 or 1 depending if she measured in the diagonal or the computational basis, respectively. Moreover, this happens with $1/4$ probability. So the probability of Eve not to obtain $p(n)$ elements of X y measuring $8p(n)$ qubits is given by the cumulative function of a binomial distribution with $1/4$ Bernoulli trial; $8p(n)$ trials and success of at most $p(n)$. By Hoeffding's inequality this probability is upper-bounded by $\exp\left(-2\frac{(8p(n)/4-p(n))^2}{p(n)})\right) = \exp(-2p(n))$ which decreases exponentially with n. In other words, Eve has an exponentially increasing probability

of obtaining $p(n)$ bits of X with $8p(n)$ qubits measurements. Since G is attackable by knowing $p(n)$ bits of X, Eve is able to perform this attack up to negligible probability. □

Corollary 1 If a pseudorandom generator G is attackable, then the scheme presented in Figure 2 is not secure in polynomial-time for a quantum adversary that has access to hash function h.

Proof. Eve is able to calculate $h(Y)$ from Y that is public. Therefore she can apply Theorem 2.3 by observing a number N of tags such that $N \log |\mathcal{T}| \geq 8p(n)$. □

Although Theorem 2.3 points that the quantum coding of Figure 3 is not better asymptotically than the classical coding (where we simply replace the quantum coder QC by a XOR gate), it seems harder to attack the quantum scheme. We will now show that this is true for the simple case where the encoder is fed by an independent and identically distributed (i.i.d.) fair Bernoulli sequence (a pure random sequence generated by fair coin tossing). The following example illustrates that this is true even for a very simple generator.

Example 2.4 (State Recovery Attack for Linear Congruential Generator(LCG)) *Let A be a positive integer and $\mathbb{Z}_A$ the set of integers modulo A. The seed of the LCG is the vector $X^{(n)} = (A, s_0, a, b)$, where $s_0, a, b \in \mathbb{Z}_A$. The length of the seed is $n = 4\lceil \log A \rceil$. A binary pseudorandom sequence with length $N \times \lceil \log A \rceil$ bits is obtained from the 2-radix expansion of the sequence $\mathbf{s} = \{s_1, s_2, \ldots, s_N\}$ created by the following recursion:*

$$s_i = as_{i-1} + b \mod A, \quad i = 2, 3, \ldots, N \tag{3}$$

It is well known (see [8]) that for all $i, i = 1, 2, \ldots, N-3$, the numbers

$$\delta_i = \det \begin{bmatrix} s_i & s_{i+1} & 1 \\ s_{i+1} & s_{i+2} & 1 \\ s_{i+2} & s_{i+3} & 1 \end{bmatrix}$$

are multiple of A. As a consequence, the greatest common divisor GCD *of some $\delta_i's$ gives the value of A. The rest of the seed, that is a, b and s_0, follow then from a system of linear equations. In practice five values of δ_i are enough.*

Figure 4 (right) displays a simplified version of the scheme shown in Figure 3, where X stands for the pseudorandom sequence from the output of the PRG. The left side of Figure 4 displays the situation when a gate XOR is utilized. We notice that the state recovery attack is applicable without change to the XOR-based scheme. It is enough to compute $X = Z \oplus Y$ before applying the algorithm. In contrast, for the quantum scheme, Eve has an irreducible uncertainty on the X values due to quantum coding. In particular, if she employs the procedure described in the proof of the Theorem 2.3 it is expected only one fourth of the X's to be correct. The problem from Eve's point of view is how to solve the seed from a degraded version of the algorithm input X.

3. Comparing XOR with Quantum Coding

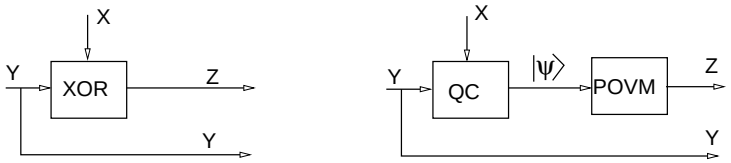
In the last section we have considered the problem of the state recovering attack and defined the weakness of a PRG. In this section we make a rigorous comparison between the XOR and the quantum coding performances using information-theoretical measures.

To this end, consider Figure 4 where both classical and quantum encodings are displayed. The QC denotes the quantum encoder defined before, in (1) and (2), where X is the variable that sets the basis. The block POVM stands for the measurement apparatus defined by the positive operator-valued measure

$$Z = \{E_m(Y)\}_{m \in O}$$

where O is the set of outcomes. Observe that the measurement may depend on the message Y, which is public. The goal of Eve is to maximize the knowledge of X, that is, minimize the entropy $H(X|Y,Z)$.

Figure 4. XOR (left) and quantum coding (right).



We consider the classical and quantum scheme presented in Figure 4 in two ways: firstly, we will assume that X is a sequence of fair and independent Bernoulli random variables, that is, the PRG describing X is perfect; secondly, we consider a biased PRG (unfair) to describe X and introduce blocks of random variables into the analysis.

3.1. Fair Input Single-Sized Block

We start with the simple case of a single-sized block and where $X \sim \text{Ber}\left(\frac{1}{2}\right)$. In the classical XOR encoding case we have that $Z = X \oplus Y$ and thus $H(X|Y,Z) = 0$. So, Eve has no doubt about X. In the quantum encoding case, we begin by observing that one can compute easily the von Neumann entropy of $S(\rho(Y)) = S(\rho(0)) = S(\rho(1))$. Therefore we have:

$$S^* = S(\rho(Y)) \quad = \quad -2\cos^2\left(\frac{\pi}{8}\right)\log\left(\cos\left(\frac{\pi}{8}\right)\right) - 2\log\left(\sin\left(\frac{\pi}{8}\right)\right)\sin^2\left(\frac{\pi}{8}\right) \tag{4}$$

Theorem 3.1 Following the notation in Figure 4 (right), the minimum uncertainty for X given Z and Y is

$$H(X|Z,Y) = 1 - S^* \tag{5}$$

where S^* is given by (4).

Proof. The Holevo bound states that

$$I(X;Z|Y) \leq S(\rho(Y)) - \sum_{i=0}^{1} \frac{1}{2} S(|\phi_i(Y)\rangle\langle\phi_i(Y)|) \tag{6}$$

where $\rho(Y)$ is the density operator that describes the encoding done by QC in the following way:

$$\rho(Y) = \frac{1}{2}|\phi_0(Y)\rangle\langle\phi_0(Y)| + \frac{1}{2}|\phi_1(Y)\rangle\langle\phi_1(Y)| \tag{7}$$

where $|\phi_0(0)\rangle = |0\rangle$, $|\phi_1(0)\rangle = |+\rangle$, $|\phi_0(1)\rangle = |1\rangle$ and $|\phi_1(1)\rangle = |-\rangle$. Since there are only pure states in the sum of (6) we can simplify that to

$$I(X;Z|Y) \leq S(\rho(Y)) \tag{8}$$

However, it is easy to verify that the Holevo bound can be achieved by a simple von Neumann measurement ([21], p. 421) described by the Hermitian operator

$$A = \mathbf{0}|\psi_\theta\rangle\langle\psi_\theta| + \mathbf{1}|\psi_\theta^\perp\rangle\langle\psi_\theta^\perp| \tag{9}$$

with $\psi_\theta = \cos(\theta)|0\rangle + \sin(\theta)|1\rangle$, $\psi_\theta^\perp = \sin(\theta)|0\rangle - \cos(\theta)|1\rangle$ and $\theta = -\frac{\pi}{8}$. Therefore we have indeed

$$I(X;Z|Y) = S(\rho(Y)) \tag{10}$$

yielding the maximum accessible information to Eve. Therefore, since $H(X|Z,Y) = H(X|Y) - I(X;Z|Y)$ and $H(X|Y) = 1$, the minimum uncertainty that Eve may attain about X is given by

$$H\left(X|Y,Z\right) = 1 - S(\rho(Y)) \tag{11}$$

$$= 1 - S^* \tag{12}$$

□

3.2. Fair Input k-Blocks

First, consider the classical setup, then $H(X^k|Y^k,Z^k) = 0$, since the block X^k is completely determined from the knowledge of Y^k and Z^k.

For the quantum setup, the subsystem that Eve owns is described by

$$\rho_{Y^k} = \bigotimes_{i=1}^{k}\left(\frac{1}{2}|\phi_0(Y_i)\rangle\langle\phi_0(Y_i)| + \frac{1}{2}|\phi_1(Y_i)\rangle\langle\phi_1(Y_i)|\right) \tag{13}$$

By the Holevo bound we get that

$$H\left(X^k|Y^k,Z^k\right) \geq H(X^k) - S(\rho_{Y^k}) \tag{14}$$

Example 3.2 *Table 1 illustrates the scenario for $k = 2$. Rows are indexed by the four possible values of Y^2 and columns are indexed by the bases corresponding to the four values of X^2. Notice that Eve is not able to distinguish which column is being used. Then, her uncertainty is lower bounded by the von Neumann entropy of the quantum system formed by states listed in row indexed by the values of Y^2 that she can access.*

Table 1. Encoding for blocks of length 2.

Y^2	Bases			
	B_0B_0	B_0B_1	B_1B_0	B_1B_1
00	$\|00\rangle$	$\|0+\rangle$	$\|+0\rangle$	$\|++\rangle$
01	$\|01\rangle$	$\|0-\rangle$	$\|+1\rangle$	$\|+-\rangle$
10	$\|10\rangle$	$\|1+\rangle$	$\|-0\rangle$	$\|-+\rangle$
11	$\|11\rangle$	$\|1-\rangle$	$\|-1\rangle$	$\|--\rangle$

In order to get a bound for $S(\rho_{Y^k})$ in Equation (14), we need to recall the following property concerning the von Neumann entropy [22].

Property 3.3 Let ρ and σ be quantum states; then $S(\rho \otimes \sigma) = S(\rho) + S(\sigma)$.

As a consequence of Equation (13) and Property 3.3, for a sequence of fair Bernoulli trials we have

$$S(\rho_{Y^k}) = kS^* \tag{15}$$

where S^* is given by (11). So, from Equation (14), we have that

$$H\left(X^k|Y^k, Z^k\right) \geq k - kS^* \tag{16}$$

Again, the equality can be achieved by a simple von Neumann measurement, namely that defined by $A^{\otimes k}$. We summarize the results from the prior discussion in the following theorem.

Theorem 3.4 (Generalization of Theorem 3.1) Following the notation in Figure 4 (right), the minimum uncertainty for k-blocks X^k given Z^k and Y^k is

$$H\left(X^k|Y^k, Z^k\right) = k\left(1 - S^*\right) \tag{17}$$

This is the best scenario one can imagine to defeat Eve. However, for the protocol to be practical, the $X's$ should be generated by a PRG, which is the case we examine next.

3.3. Unfair Input k-Blocks

The results above were obtained assuming that $\{X_i\}$ was a sequence of i.i.d. fair Bernoulli random variables. In this section we study the general case, with the purpose of clarifying how the use of a real PRG affects the uncertainty about X. Our main point is to stress that even when using PRG, the uncertainty given by $H\left(X^k|Y^k, Z^k\right)$ remains positive, contrarily to the classical XOR encoding case where $H(X^k|Y^k, Z^k) = 0$ (since $Z^k = X^k \oplus Y^k$). As expected, we show that the uncertainty is directly proportional to the size of the seed of the PRG under reasonable assumptions.

Consider k-length blocks X^k, Y^k and Z^k, where $X^k = X_{i+1}, X_{i+2}, \ldots, X_{i+k}$ is a contiguous subsequence of $\{X_i\}$ and similarly to Y^k and Z^k. Note that, to ease notation, we omit the index i

in defining X^k. However, it is crucial to remark that the probability distribution of X^k is, in general, dependent on i. As a matter of fact, $\mathbf{p}_{X^k} = (p_0, p_1, \ldots, p_{2^k-1})$ can even degenerate to a distribution with a single component equal to 1, depending on the robustness of the PRG. We shall simplify the notation denoting $\mathbf{p}_{X^k}$ by $\mathbf{p}$. We consider that a PRG is as robust as possible, that is, with a seed of size s the PRG generates precisely 2^s blocks of size k with $k \geq s$. Note that this assumption is more than acceptable as k should be much larger than s. Thus, $p_{i_j} = 1/2^s$ for some indexes $i_1 \ldots i_{2^s}$ and $p_j = 0$ if $j \notin \{i_1 \ldots i_{2^s}\}$. Thanks to the fact that only 2^s sequences are generated by the PRG among the possible 2^k sequences, we can rewrite, by change of basis, ρ_{Y^k} as

$$\rho_{Y^k} = \sum_{j=0}^{2^s-1} 1/2^s |\phi_j 0 \ldots 0\rangle\langle\phi_j 0 \ldots 0| \tag{18}$$

where the states

$$|\phi_j 0 \ldots 0\rangle = \left(\bigotimes_{i=1}^{s} |\phi_{j_i}(Y_i)\rangle \right) \otimes \left(\bigotimes_{i=1}^{k-s} |0\rangle \right),$$

and j_i is the i-th bit of the binary representation of j. Observe that in this case we have

$$H\left(X^k|Y^k, Z^k\right) = H\left(X^s|Y^s, Z^s\right)$$

since in this basis, by knowing Y^k and Z^k, there is no uncertainty in the last $k-s$ qubits. So if the PRG has a seed of size s, we can see the pseudorandom string of size k as one string where the first s bits are completely random and the last $k-s$ bits are fixed. Then, by Theorem 3.4 we have that

$$H\left(X^k|Y^k, Z^k\right) = s(1-S^*) > 0 \; and \; I(X^k; Z^k|Y^k) = sS^* < s \tag{19}$$

Therefore, we can conclude that the quantum encoding protects better the secret than the classical one, even in the presence of PRG's. In the next section we further improve the scheme by exploiting the uncertainty derived above. As we shall see, the entropy given in (19) is the upper-bound for the equivocation caused by the noise in the channel between Alice an Bob (which includes Eve's intervention) for the proposed scheme to work in practice.

Note that in the original scheme by Brassard (see Figure 1) the stream Y is hashed before being XORed and so, if we consider the full encryption scheme, the total entropy for the eavesdropper is

$$H\left(X^k|Y^k; Z^k\right) = \log|\mathcal{H}| - \epsilon \;\; and \; I(X^k; Z^k|Y^k) = s - \log|\mathcal{H}| + \epsilon \tag{20}$$

for s large enough. For the quantum scheme, (see Figure 2) the stream Y is also hashed before being quantum encoded. In this case the total entropy for the eavesdropper is

$$H\left(X^k|Y^k; Z^k\right) = s(1-S^*) + \log|\mathcal{H}| - \epsilon \;\; and \; I(X^k; Z^k|Y^k) = sS^* - \log|\mathcal{H}| + \epsilon \tag{21}$$

for s large enough. Note that we are able to make the equivocation (conditional entropy) dependent on the size of the seed of the PRG and, in the quantum case the equivocation is greater than in the classical case.

3.4. Almost Fair Input k-Blocks

The above unfair case renders the authentication to be only computationally secure, as its security relies only on the size of the seed. In order to improve this result we have considered almost-random sequences instead of pseudorandom sequences. In an almost-random sequence of size k all the bits are random with exception of ℓ control bits. So, contrarily to a pseudorandom generator where all the k-long sequence depends on the seed, in almost-random sequences only some control bits depend on the key. Indeed, to represent ℓ bits in a k long almost-random sequence we need a key with $\ell \times \log(k)$ bits.

Our aim is to estimate the minimal uncertainty of the eavesdropped in the case that X is an almost-random sequence. When Alice and Bob use the scheme in Figure 3 with an almost-random sequence X, a full message of size k is authenticated, but only ℓ control bits are used to check whether the message is authentic. Since the eavesdropper does not know in which positions the control bits are, if he randomly changes the sequence he would alter, with very high probability, at least one of these bits and therefore, he will be detected. The good thing is that the entropy of the almost-random sequence is much higher than the entropy of the pseudorandom sequence, since only ℓ bits are constrained given the key.

Actually, an almost fair random sequence is a sequence produced as an output of random-number generator in a way that if we compare its two output sequences from the same key, only ℓ out of total k bits ($\ell << k$) are going to be the same and other $k-\ell$ are going to be totally uncorrelated (which means that from knowing the key we are able to get the values of only ℓ bits as well as their positions). Thus, if Eve has no knowledge about the seed, then her uncertainty concerning X^k given Y^k and Z^k is precisely the same as that in the case of fair random sequences. This is so because all generated bits of X^k are random, and not pseudorandom, even for the ℓ control bits that used to authenticate, and so we have that the minimum conditional entropy is given by

$$H\left(X^k|Y^k,Z^k\right) = k\left(1-S^*\right) \tag{22}$$

Note, however, that this result comes with the price of Eve being able to change several qubits without being detected. She does not know a priori in which position control qubits are going to occur; and so, if she risks too much then she will be detected. It remains to understand what is the probability that Eve can modify the quantum channel without being detected. Indeed, if we assume that Eve needs to modify s bits in order to make the attack, then the probability of her not being detected can be computed by

$$\prod_{i=0}^{s}\left(1-\frac{\ell}{k-i}\right) \tag{23}$$

where $k >> s$ and $k >> \ell$. First we notice that by applying McLauren approximation to (23)

$$\ln(1+x)\approx x \tag{24}$$

for a positive x close to zero, we have

$$\ln\prod_{i=0}^{s}\left(1-\frac{\ell}{k-i}\right) = \sum_{i=0}^{s}\ln\left(1-\frac{\ell}{k-i}\right) \approx \sum_{i=0}^{s}\frac{(-\ell)}{k-i} = (-\ell)\sum_{i=0}^{s}\frac{1}{k-i} \tag{25}$$

Introducing the substitution $k-i=t$, we obtain:

$$(-\ell)\sum_{i=0}^{s}\frac{1}{k-i}=(-\ell)\sum_{t=k}^{k-s}\frac{1}{t}=\ell\sum_{t=k-s}^{k}\frac{1}{t}=\ell(H_k-H_{k-s-1}) \tag{26}$$

where H_k is the k-th harmonic number. By using the approximation for the harmonic sum $H_N \approx \ln(n)+\gamma-\frac{1}{2n}$ (where γ is the Euler–Mascheroni constant), we obtain the final expression

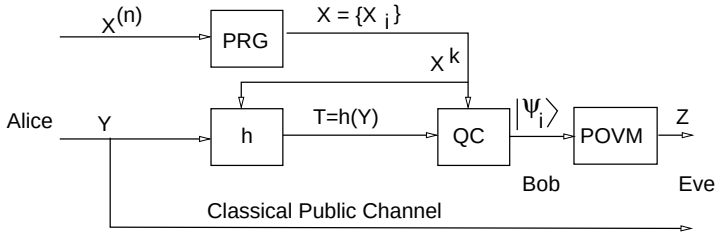
$$\prod_{i=0}^{s}\left(1-\frac{\ell}{k-i}\right)\approx e^{(-\ell)\left(\left(\ln\frac{k}{k-s-1}\right)+\frac{s+1}{2k(k-s-1)}\right)} \tag{27}$$

This expression states that the probability for an eavesdropper not to be detected decreases exponentially with ℓ.

4. Improving Key-Tag Secrecy

In the last section we compared Eve's equivocation on X for the XOR and QC schemes when she has access both to the message Y and its quantum encoded version, which she observes from the quantum channel. We concluded that the equivocation is kept above some lower bound depending on the size of the seed of the PRG. In this section we include a hash function h in the scheme (see Figure 5) in such a way that Eve only accesses the public message Y and the quantum encoded version of the tag $T=h(Y)$. Thanks to that modification we shall demonstrate that is feasible to improve the secrecy of the key and of the tag simultaneously. Note that if the random string was truly random (and not pseudorandom) then the whole construction yields perfectly secure authentication even if the secret almost strong 2-universal function is used many times [1]. However, we are not using truly random strings, and as we shall see, by changing the hash function as the pseudorandom string is generated we improve the security of the scheme.

Figure 5. Authentication scheme with a single key $X^{(n)}$.



By information-theoretic secrecy, as usually, we mean $I(W;V)=0+O(2^{-n})$ or equivalently, the equivocation $H(W|V)=H(W)-O(2^{-n})$, where W is the secret to be protected and V is the piece of data available to the eavesdropper. Our derivations will focus on the equivocation $H(W \mid V)$ to measure the quality of the scheme. Then, the information to be protected is $W=\left(T,X^k\right)$ and the information available, from Eve's viewpoint, is $V=(Y,Z)$. We investigate the uncertainty of the tag $H(T \mid Y,Z)$ and the uncertainty of the key $H(X^k \mid Y,Z)$.

We assume that X^k is independent of the message Y and that the hash function is selected from the $\varepsilon-$almost strongly universal-2 class of hash functions, which we refer in the following just as *hash functions*.

4.1. Modified Classical Case

Consider a simple modified setup where a XOR gate is taken in place of the QC block in the scheme displayed in Figure 5.

If $\{X_i\}$ is a fair Bernoulli sequence and a k-block of bits such that

$$k = \max\{\lceil \log |\mathcal{T}| \rceil, \lceil \log |\mathcal{H}| \rceil \}$$

it is utilized per message, then the scheme turns to be equivalent to the Wegman–Carter scheme. Indeed, in this situation h is in fact drawn uniformly from $\mathcal{H}$. Then we have

$$\begin{aligned} H\left(T, X^k|Y, Z^k\right) &\overset{(a)}{=} H(T|Y, Z^k) + H(X^k|T, Y, Z^k) && (28)\\ &\overset{(b)}{=} H(T|Y, Z^k) && (29)\\ &\overset{(c)}{=} H\left(T|Y\right) && (30)\\ &\overset{(d)}{=} \log \mid \mathcal{T} \mid && (31) \end{aligned}$$

Equality (a) is due to the chain rule for Shannon entropy, (b) is due to the fact that in the classical setup it is known that $X^k = T \oplus Z^k$. The equality (c) is harder to obtain, indeed it follows from the properties of the $\varepsilon-$almost universal-2 class of hash function. Note that $T = h_{X^k}(Y)$ has a uniform distribution. Moreover $T|_{x_k} = h_{x^k}(Y)$ has also uniform distribution, and therefore, T is independent of X^k. Since $Z^k = f(X^k, Y)$ we have that $H(T|Y, Z^k) = H(T|Y)$. Equality (d) is also due to the properties of hash functions. On the other hand, if $\{X_i\}$ comes from a PRG, the Eve's uncertainty on the tag can, eventually, decreases by observing the random variable Z^k. Indeed, in general, $H\left(T|Y, Z^k\right) < H\left(T|Y\right)$. Consequently, unconditional secrecy relative to T, $H(T|Y, Z^k) = \log |\mathcal{T}|$ cannot be assured.

4.2. Uncertainty of the Tag in the Quantum Case

We start by giving a condition to attain unconditional security of the tag in terms of the conditioned mutual information between T and the $k-$block of bits of the key. This condition will motivate our final proposal for the authentication protocol.

Theorem 4.1 If $I\left(T; X^k|Y, Z^k\right) = H(T)$ then the tag is secure in the information theoretical sense, that is, $H(T|Y, Z^k) = H(T)$.

Proof.

From the standard chain rule for Shannon entropy we have:

$$\begin{aligned} H\left(T, X^k \mid Y, Z^k\right) &= H\left(X^k \mid Y, Z^k\right) + H\left(T \mid X^k, Y, Z^k\right) && (32)\\ &= H\left(T|Y, Z^k\right) + H\left(X^k|T, Y, Z^k\right) && (33) \end{aligned}$$

Then, comparing (32) and (33) we obtain

$$\begin{aligned} H\left(T|Y, Z^k\right) &\overset{(a)}{=} H\left(T|X^k, Y, Z^k\right) + \\ &\quad H\left(X^k|Y, Z^k\right) - H\left(X^k|T, Y, Z^k\right) && (34)\\ &\overset{(b)}{=} H\left(T|X^k, Y, Z^k\right) + I\left(T; X^k|Y, Z^k\right) && (35)\\ &\overset{(c)}{=} I\left(T; X^k|Y, Z^k\right) && (36) \end{aligned}$$

Equality (a) is due to a simple manipulation of (32) and (33), (b) is definition of mutual information and (c) follows because the hash function is determined by X^k and so, then $T = h(Y)$ is immediately calculated. That is, $H(T|X^k, Y, Z^k) = H(T|X^k, Y, T = h(Y)) = 0$. The results follows from (36). □

Observe that Equation (36) clearly indicates that in order to increase Eve's uncertainty about T, we must maximize the mutual information between the block X^k and the tag T. This is the *information-theoretical* intuition that motivates the scheme presented in Figure 5. Note that in this case we make the tag T dependent of X^k, thus increasing their mutual information. In Brassard scheme (see Figure 1) the hash function is fixed in the beginning, and therefore $I\left(T; X^k|V'\right) = 0$ where V' is the observation that Eve can perform in Brassard's scheme.

Now we can compare the scheme from Figure 5 with that in Figure 2. For the latter recall Equation (21) and note that the key for Alice and Bob is the seed s together with a chosen hash function, which has to be encoded in $\log(|\mathcal{H}|)$ bits. However for the scheme in Figure 5 we only have one key and for this key it is straightforward to derive the following entropy bounds following the same reasoning as in Section 3

$$H\left(X^k|Y^k; Z^k\right) = s(1 - S^*) - \epsilon \ \ and \ I(X^k; Z^k|Y^k) = sS^* + \epsilon \tag{37}$$

which improve those in (21) since $S^* < 1$.

4.3. Robustness of the Protocol under Noisy Quantum Channels

As we discussed in the introduction, one of the points of the protocol proposed in Figure 5 is to address the scenario where the quantum communication channels have noise. In this case, the shared key might be lost and therefore there is no way to bootstrap a new QKD round. Considering noise, we now discuss how the protocol copes with the quantum channel erasing qubits or modifying them.

When qubits are removed from the channel, Bob will lose the corresponding message authentication tag for a given message, and therefore the authentication will be lost. As usual, to avoid this problem Alice and Bob have to make synchronous emissions of qubits in such a way that Bob knows the time each qubit should arrive. This measure requires Alice and Bob to have a synchronous clock. If a qubit is lost, Bob can disregard it (assuming the message has enough redundancy) and tell this fact afterwards to Alice. Another option is to send through the public channel the list of qubits that were not received (authenticated with those that were). If qubits are added by an attacker, then Bob can also disregard them if they arrive out of schedule.

In the case qubits are modified by the channel, it is well known that if the attacker Eve has access to a degraded version of the channel between Alice and Bob, even when this channel is not perfect, it is possible to exchange perfectly secure messages between Alice and Bob [14,23]. By the results established in Section 3 and Section 4, namely Equation (37), if the mutual information between messages sent by Alice and received by Bob is higher than $sS^* + \epsilon$, then Alice and Bob can communicate securely regarding Eve, where s is the number of bits of the seed of the PRG that Eve does not known. We formalize this statement in the following result, which follows immediatly from [23] (namely Corollary 2 page 341) and Equation (37).

Corollary 2 *Let W^k be the degraded version of X^k observed by Bob caused by noise and let s be the number of bits from the seed of the PRG that Eve does not know. Then, if $I(X^k;W^k|Y^k) > sS^* + \epsilon$ then Alice and Bob can exchange tags with perfect security at rate smaller than $I(X^k;W^k|Y^k) - sS^* - \epsilon$.*

Note however that this does not imply that this scheme is perfectly secure, as s decreases while messages are exchanged between Alice and Bob. So, in practice our authentication protocol can be used as follows: (i) estimate the mutual information between messages exchanged between Alice and Bob (that is the noise of the channel); (ii) estimate the information gain concerning the PRG seed that Eve can obtain by analysing blocks of exchanged tags; (iii) choose s large enough such that the mutual information between the message sent by Alice and that received by Bob is always greater than $s_{\min}S^* + \epsilon$, where $s_{\min}$ is the minimum number of bits of the seed of the PRG that Eve will never known, taking into account (ii) and the number of tags exchanged.

5. Summary

In this work, we have investigated how quantum resources can improve the security of classical message authentication protocols. We have started by showing that a quantum coding of secret bits offers more security than the classical XOR function. Then, we have used this quantum coding to propose a quantum-enhanced protocol to authenticate classical messages, with improved security with respect to the classical scheme introduced by Brassard in 1983. Our protocol is also more practical in the sense that it requires a shorter key than the classical scheme by using the pseudorandom bits to choose the hash function. Finally, we prove that quantum resources can improve both the secrecy of the key generated by the PRG and the secrecy of the tag obtained with a hidden hash function.

The usefulness of our proposal follows from three facts. Firstly, the shared key between Alice and Bob is not consumed while generating the pseudorandom sequence [24], which allows for tentative recovery of the system under noisy channels.

Secondly, even empowered with a quantum computer, it is not known how to attack our protocol in polynomial-time. The latter fact follows since it is very hard to attack a PRG if the generated string is encoded in a quantum channel and the adversary can only access each pseudorandom bit with 1/4 probability, that is, the attacker only knows the pseudorandom sequence with a high level of uncertainty. Moreover, if one assumes the Blum–Blum–Shub PRG and consider that the Blum integer is kept secret between Alice and Bob (which is not assumed in the classical reduction to the quadratic residuosity in [7]), then the attacker would also need to guess this integer, making the attack much harder than if the integer is known. As far as the authors know, there are no results on attacking PRG's in this case. Moreover, by taking into account the equivalence between the existence of PRG's and public key cryptosystems, such attack is equivalent to attacking a public-key cryptosystem without having access to the public key, which essentially consists of attacking a symmetric key encryption. Such attack is believed to be much harder than attacking a public-key cryptosystem. The same argument can be used for other PRG's based on hardness assumptions [25]. In the setting of our protocol, where Alice and Bob start with a shared symmetric private key, there is no reason to assume that such information is known by Eve, since Alice and Bob could privately and secretly choose the Blum integer in the same way they choose the initial shared symmetric key.

Thirdly, by taking into account the noise of the quantum channel, it is possible to choose the size of the seed of the PRG to be large enough so that the equivocation of the attacker (due to the quantum encoding) is larger than that equivocation caused by the noise between Alice and Bob (and assuming the attacker has access to the channel near Alice, that is, without noise). In such a case, and while the attacker cannot discover enough bits of the PRG, the communication between Alice and Bob remains perfectly secret according to [23].

Finally, we stress that by using the proposed protocol, QKD becomes a fully quantum protocol.

Acknowledgments

F. M. Assis acknowledges partial support from Brazilian National Council for Scientific and Technological Development (CNPq) under Grants No. 302499/2003-2 and CAPES-GRICES No. 160. A. Stojanovic, P. Mateus and Y. Omar thank the support from project IT-QuantTel, as well as from Fundação para a Ciência e a Tecnologia (Portugal), namely through programs POCTI/POCI/PTDC and projects PTDC/EIA/67661/2006 QSec and PTDC/EEA-TEL/103402/2008 QuantPrivTel, partially funded by FEDER (EU).

References and Notes

1. Wegman, M.N.; Carter, J.L. New hash functions and their use in authentication and set equality. *J. Comput. Syst. Sci.* **1981**, *22*, 265–279.
2. Bennett, C.H.; Brassard, G. Quantum cryptography: Public-key distribution and coin tossing. In Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984; pp. 175–179.
3. Brassard, G. On computationally secure authentication tags requiring short secret shared keys. In *Advances in Cryptology*; Springer-Verlag: New York, NY, USA, 1983; pp. 79–86.
4. Krawczyk, H. LFSR-based hashing and authentication. In *Advances in Cryptology*; Springer-Verlag: New York, NY, USA, 1994; pp. 29–42.
5. Rogaway, P. Bucket hashing and its application to fast messages authentication. In *Advances in Cryptology*; Springer-Verlag: New York, NY, USA, 1995; pp. 29–42.
6. Shoup, V. On fast and provably secure message authentication based on universal hashing. In *Advances in Cryptology*; Springer-Verlag: New York, NY, USA, 1996; pp. 313–328.
7. Blum, L.; Blum, M.; Shub, M. A simple unpredictable pseudo random number generator. *SIAM J. Comput.* **1986**, *15*, 364–383.
8. Sidorenko, A.; Shoenmakers, B. State recovery attacks on pseudorandom generators. In *Western European Workshop on Research in Cryptology, Lectures Notes in Informatics (LNI)*; GI: Bonn, Germany, 2005; Volume 74, pp. 53–63.
9. Alleaume, R.; Bouda, J.; Branciard, C.; Debuisschert, T.; Dianati, M.; Gisin, N.; Godfrey, M.; Grangier, P.; Langer, T.; Leverrier, A.; *et al*. SECOQC white paper on quantum key distribution and cryptography. *arXiv* **2007**, arXiv:quant-ph/0701168.
10. Ioannou, L.M.; Mosca, M. A new spin on quantum cryptography: Avoiding trapdoors and embracing public keys. *Post-Quantum Cryptography* **2011**, *7071*, 255–274.

11. Kunz-Jacques, S.; Jouguet, P. Using hash-based signatures to bootstrap quantum key distribution. *arXiv* **2012**, arXiv:1109.2844v2.
12. Goldreich, O. *Modern Cryptography, Probabilistic Proofs and Pseudorandomness*; Springer: Berlin, Germany, 1999.
13. Cover, T.M.; Thomas, J.A. *Elements of Information Theory*; Jonh Wiley & Sons: Hoboken, NJ, USA, 2006.
14. Wyner, A.D. The wire-tap channel. *Bell Syst. Tech. J.* **1975**, *54*, 1355–1387.
15. Maurer, U.M. Secret key agreement by public discussion from common information . *IEEE Trans. Inform. Theor.* **1993**, *39*, 733–742.
16. Simmons, G.J. Authentication theory/coding theory. In Proceedings of the CRYPTO 84 on Advances in Cryptology, Santa Barbara, CA, USA, 1984; Springer-Verlag: New York, NY, USA, 1975; pp. 411–431.
17. Lai, L.; El Gamal, H.; Poor, H.V. Authentication over noisy channels . *IEEE Trans. Inform. Theor.* **2009**, *55*, 906–916.
18. Cederlörf, J.; Larsson, J. Security aspects of the authentication used in quantum cryptography. *IEEE Trans. Inform. Theor.* **2008**, *54*, 1735–1741.
19. Damgaard, I.; Pedersen, T.; Salvail, L. On the key-uncertainty of quantum ciphers and the computational security of one-way quantum transmission. *arXiv* **2004**, arXiv:quant-ph/0407066.
20. Goldreich, O. *Foundations of Cryptography: Volume I Basic Tools*; Cambridge University Press: Cambridge, UK, 2001.
21. Paris, M.G.A.; Rehácek, J. *Lectures Notes in Physics, Quantum State Estimation*; Springer: Berlin, Germany, 2004.
22. Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Information*; Cambridge University Press: Cambridge, UK, 2000.
23. Csiszar, I.; Korner, J. *Broadcast channels with confidential messages. IEEE Trans. Inform. Theor.* **1978**, *24*, 339–238.
24. Although this sequence is cyclic, the cycle is exponential in the size of the seed, and so the standard QKD key maintenance will eventually be restored before the cycle ends.
25. A similar analysis can be made to the Blum-Micali PRG assuming the large prime is kept secret [26].
26. Blum, M.; Micali, S. How to generate cryptographically strong sequences of pseudorandom bits. *SIAM J. Comput.* **1984**, *13*, 850–864.