Quantum Tags for the Authentication of Classical Public Messages

***Abstract* — In this work we have investigated how quantum resources can improve the security of a protocol for the authentication of classical messages, introduced by Brassard in 1983. In that protocol, the shared key is the seed of a pseudo-random number generator (PNG) and a hash function is used to create the authentication tag of a public message. We have started by showing that the quantum encoding of secret bits offers more security than the classical XOR function introduced by Brassard. Furthermore, we have established the conditions a general PNG must satisfy for our quantum-enhanced protocol to yield information-theoretical security. Altogether, our proposal represents a twofold improvement: first it offers proven information-theoretical security under some assumptions on the PNG; secondly, these assumptions are weaker than the requirements for the PNG in Brassard's protocol. Additionally, our proposal 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 tag's hash function.**

***Index Terms* — Authentication of messages, information security, quantum cryptography, secure telecommunications.**

I. The Problem

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 a private authentication tag. 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 (see general scheme in Fig. 1). For instance, one could imagine that Alice is sending to 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.

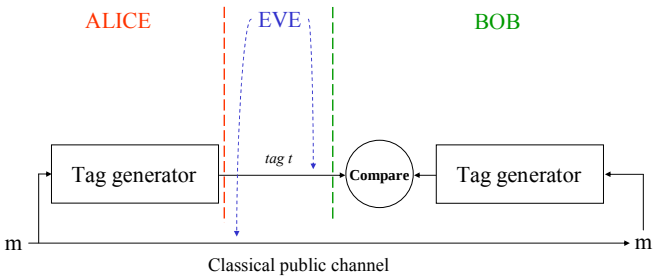

Fig. 1. – General scheme for our authentication problem. Alice wants to send a public classical message *m* to Bob and a private tag *t* that authenticates the message *m* (colour online).

II. The Classical Solutions

In 1983, G. Brassard proposed a computationally secure scheme of classical authentication tags based on the sharing of two short secret keys, shared between Alice and Bob [1]. One key is used as a seed of pseudo-random number generator (PNG) and the other key is used to select a hash function out of a large set. The authentication tag is then given by the XOR of the hash of the message with the pseudo-random bits generated by the PNG. Brassard's scheme is itself an improvement of the Wegman-Carter protocol [2]. The latter protocol offers perfect (informational-theoretical) security using one new hash function for each new message, but this means that the key size grows proportionally to the number of messages and Alice and Bob will need to share a long list of indices to select the same hash function each time. Brassard's scheme yields a much more practical protocol, where the requirements on the seed length grow reasonably with the number of messages we want to authenticate, as opposed to the Wegman-Carter proposal.

III. Quantum Authentication

In this work, we extend Brassard's protocol to include quantum authentication tags, which we prove can offer, under certain conditions, information-theoretical security for the

Manuscript received on 13 June 2008.
F. M. Assis, Departament of Electrical Engineering, Universidade Federal de Campina Grande, Brazil.
P. Mateus, SQIG – Instituto de Telecomunicações and IST, Universidade Técnica de Lisboa, P-1049-001 Lisbon, Portugal.
Y. Omar, SQIG – Instituto de Telecomunicações, P-1049-001 Lisbon and CEMAPRE, ISEG, Universidade Técnica de Lisboa, P-1200-781 Lisbon, Portugal (e-mail: yasser.omar@iseg.utl.pt).

authentication of classical messages. Our main idea is to replace Brassard's XOR operation by a quantum coder (QC). We also show that it is not necessary to have a separate key for the choice of the hash function, as this can be done by the sequence of pseudo-random bits generated by the PNG. Our proposal for a quantum authentication protocol is presented in Fig. 2.

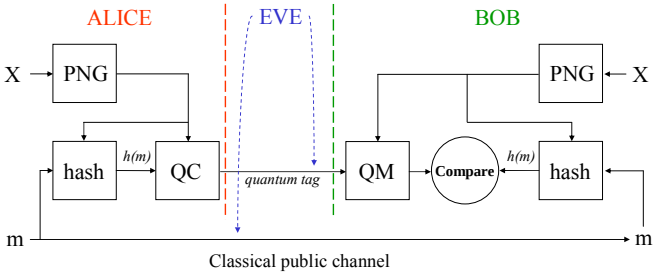

Fig. 2. – Our proposal for a quantum message authentication protocol using only a short key X shared by Alice and Bob. PNG is a pseudo-random number generator, QC is our quantum coder and QM the quantum measurement device (colour online).

Our protocol works in the following way. Alice uses the QC to encode the bits of the hash of the message in one of two mutually-unbiased bases [3]:

$$B_0 = \{|0\rangle, |1\rangle\}$$
$$B_1 = \{|+\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$$

according to the following public rule, depending on the value of each pseudo-random bit x:

$$\begin{aligned}
&\text{If } x = 0 \text{ and } h(m) = 0, \ |\psi\rangle = |0\rangle \\
&\text{If } x = 0 \text{ and } h(m) = 1, \ |\psi\rangle = |1\rangle \\
&\text{If } x = 1 \text{ and } h(m) = 0, \ |\psi\rangle = |+\rangle \\
&\text{If } x = 1 \text{ and } h(m) = 1, \ |\psi\rangle = |-\rangle
\end{aligned}$$

This quantum tag is then sent to Bob through a quantum (noiseless) channel. Finally, Bob chooses to measure this tag in basis B_x according to the pseudo-random bit x and should then obtain exactly $h(m)$.

The use of quantum bits for the authentication tags hides more information and thus protects the pseudo-random number generator much better from Eve's attacks. In fact, we were able to prove the following theorem, for the case of blocks of size k [4]:

Theorem 1

Given a PNG with a seed of length n, let $\mathbf{p}$ be the probability distribution of a pseudo-random block of bits, with length k, and $\mathbf{q}$ be the uniform probability distribution.

Let ρ_k be the density matrix describing the state of the quantum tag obtained from the PNG and σ_k the density matrix of the quantum tag in the case we had a purely-random number generator, associated respectively to $\mathbf{p}$ and $\mathbf{q}$.

Let also D be the trace distance and S the von Neumann entropy.

Finally, let $f(k,n)$ and $g(n)$ positive functions such that:

- $\lim_{n\to\infty} g(n) = +\infty$
- $\lim_{n\to\infty} g(n) f(g(n), n) = 0.$

Then, if $D(\mathbf{p},\mathbf{q}) \leq f(k,n)$ and $k \leq g(n)$
we have: $\lim_{n\to\infty} |S(\rho_{g(n)}) - S(\sigma_{g(n)})| = 0.$

This important result establishes the conditions under which the PNG will yield pseudo-random quantum tags that are indistinguishable from purely-random quantum tags. From it we can conclude:

Theorem 2

If the PNG satisfies the conditions of Theorem 1, then the key X in the quantum authentication protocol presented in Fig. 2 is perfectly secure for blocks up to length k.

This establishes the conditions on the PNG for our quantum authentication protocol to offer perfect security for blocks of length k, which can be a very large number. And if the PNG is such that the above function g satisfies $g(n) < 2^n$, then our protocol offers informational-theoretical security without any limitations. To find such a PNG remains an open question, but in any case we have established a quantum protocol for the authentication of publical classical messages which requires only one short key shared between Alice and Bob and which can offer perfect security under the right conditions, defined precisely in Theorem 1.

ACKNOWLEDGMENT

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. P. Mateus and Y. Omar thank the support from Fundação para a Ciência e a Tecnologia (Portugal), namely through programs POCTI/POCI/PTDC and projects PTDC/EIA/67661/2006 QSec and POCI/MAT/55796/2004 QuantLog, partially funded by FEDER (EU).

REFERENCES

[1] G. Brassard, "On computationally secure authentication tags requiring short secret shared keys", in *Advances in Cryptology*, Springer-Verlag, pp. 79-86 (1983).

[2] M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality", *J. Comput. Syst. Sci.* **22**, 265-279 (1981).

[3] C. H. Bennett and G. Brassard, "Quantum cryptography: public-key distribution and coin tossing", in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, IEEE Press, New York, pp. 175-179.

[4] F. M. Assis, P. Mateus and Y. Omar, "*Quantum Authentication of Classical Messages with Perfect Security*", in preparation (2008).