Quantum identification system over private quantum channel

J. C. Nascimento, P. Mateus and R. R. Viana

***Abstract*—All proposals for quantum key distribution require that the parties have access to an authenticated channel. Therefore, a key pre-distribution system is needed to provide authentication for the users. In this paper we propose an efficient scheme for key pre-distribution and identification for users with quantum channel. Our proposal uses quantum one-time-pad for implementing a quantum private channel. The quantum identification scheme proposed requires eight times less qubits than the trivial schemed used in other QKD, and moreover, the network initialization with n users requires only $O(n)$ keys.**

***Index Terms*—Quantum key Distribution, quentum cryptography, authentication.**

I. Introduction

RECENTLY, information security techniques based on quantum mechanics have been actively studied because in many important case they are more secure than classical ones. The most famous schemes are quantum key distribution schemes [1], [2], [3] and some of them have been proved to be unconditionally secure [4], [5]. Moreover, if large-scale quantum computers can be built they will be able to solve certain problems much faster than current classical computers. Indeed, Shor proposed a polynomial-time algorithm for prime factorization and discrete logarithm on a quantum computer [6] than can be used to "break" widely used public-key cryptography scheme, such as RSA.

The essence of a quantum channel is to provide a method for encoding bits in quantum states in such a way that any measure taken by an eavesdropper can be discovered by the legitimate users. The security relies on the laws of quantum mechanics, and more specifically on the fact that it is impossible to gain information about non-orthogonal states without disturbing these states [7]. Furthermore, quantum noise also disturbs quantum information in a quantum channel, wherefore one needs error correction and, thus add ancillas qubits. In quantum error correction the total of ancillas is proportional to the total of qubits that we want to correct (although it is possible to perform quantum error correction without ancillas [8], [9], [10]). However, for the sake of clarity and concise exposition, we assume an ideal quantum channel (without noise) because this assumption does not affect the results.

In addition, we assume that a classical channel may be used by the involved parties to exchange classical information. Both channels, classical channels and quantum channels, can be divided into two types: unsecure and secure. Unsecure channels can be actively tampered in such a way that the intruder may insert or modify messages, while secure channels provide data integrity and authentication. Classical secure channels can be implemented through message authentication codes (MAC), such as those proposed by Wegman and Carter [11], and provide unconditional security. In quantum channel the qubit integrity is enabled by a quantum channel privacy method [12].

All proposals of quantum key distribution require that the parties have access to an authenticated channel. Any QKD protocol that does not fulfill this requirement is vulnerable to a man-in-the-middle attack [13]. The reliable relations can be organized hierarchically, which offers the advantage that one does not need to trust everybody in the network, but only to trust a third party – the certification authority (CA). Suppose that the user u_x and CA can identify each other, and they share, at the initial time, a key K_x to be able to implement a secure classical channel. The same situation is valid for any other user, say u_y. In other words, both u_x and u_y have reliable relations with the CA. At the moment that both users want to identify to each other, they ask the CA to send, via the secure channel, a session key. A trivial authentication scheme between user u_x and u_y is the following (see [14]):

1. Since CA and user u_x share a key K_x, they can use the BB84 protocol with an authenticated classical channel in order to agree on a secret key. After, the CA generates and sends the session key K to u_x;
2. CA sends the session key K to user u_y by the same method;
3. Now, both users u_x and u_y can use BB84 with an classical channel authenticated with key K.

Whenever u_x and u_y want to carry out a QKD they have to authenticate with CA. This simple protocol requires $2|K|$ qubits for each quantum key distribution with an ideal quantum channel. We assume that $|K| = |K_y| = |K_x|$ because the authentication protocol between CA and u_x, and between CA and u_y is the same used to authenticate u_x with u_y.

A common and realistic restriction is to assume that the classical channel between u_x and CA is open only once (and

Manuscript submited at March 20, 2009

J. C. Nascimento Department of Teleinformatic Engineering, Federal University of Ceará, Fortaleza, CE, Brazil. e-mail: claudio@deti.ufc.br

P. Mateus Departament of Mathematic, SQIG - IT and IST, Av. Rovisco Pais 1049-001, Lisboa, Portugal Tel. +351 21 8417149 Fax. +351 21 8417048

R. R. Viana Department of Teleinformatic Engineering, Federal University of Ceará, Fortaleza, CE, Brazil. e-mail: rubens@deti.ufc.br

the same for the channel between u_y and CA), and moreover, that there is not, at the same time, a channel open between u_x, CA, and u_y. Since a quantum network needs to pre-distribute secret keys to perform the first rounds of authentication, the CA needs to generate distinct keys for each pair among the n users and distribute to each user its $n-1$ keys appropriately labeled. The keys are stored in classical memory for later authentication. Hence the initialization of a network of n users requires the pre-distribution of $n(n-1)/2$ pairs of secret keys a priori.

A quantum identification system was first proposed by C. Crpeau and L. Salvail in [15]. Alice and Bob mutually check their knowledge of a common secret string without disclosing it. In [16], Alice and Bob check their common secret string in a classical way. To prevent from a later misuse, each identification sequence is used only once and the distribution of a new common secret string is achieved by means of quantum key distribution. In [17], Barnum considers the use of entanglement between two parties to enable one to authenticate her identity to another over a quantum communication channel. In [18], a quantum password is a quantum state analogue of the classical password. Their proposal, the information is stored and manipulated classically. However, to identify several agents, the password systems need one different password to each agent.

The purpose of this paper is to propose a scheme of key pre-distribution and identification to users of quantum channel. Our goal is to propose with unconditionally security a network management service with complexity $O(n)$ for a network with n nodes (users). The quantum identification scheme proposed requires eight times less qubit than the trivial protocol presented before.

The article is organized as follows: In section II we present some notation and two quantum one-time-pad codes. In section III we propose the scheme for key pre-distribution and users identification with the certification authority to provide security over a network of QKD links. Finally in section IV some conclusion are draw.

II. Preliminaries

Let u_x be any of the n users of network that trust in CA. The key shared between CA and user u_x is divided in three parts $K_x = (a_x, b_x, c_x)$ such that $2|a_x| = 2|b_x| = |c_x| = 2m$. In our notation the state $|\psi_{b_{xi}}^{a_{xi}}\rangle$ is in two dimensional Hilbert space and, a_{xi} and b_{xi} are the i-th bit of the sequences a_x and b_x, , respectively. Bit b_{xi} represents the basis (0 for $\{|0\rangle, |1\rangle\}$ and 1 for $\{|+\rangle, |-\rangle\}$) and a_{xi} represents the data logic value (0 if the state is $|0\rangle$ or $|+\rangle$ and 1 if the state is $|1\rangle$ or $|-\rangle$). The quantum state $|\psi_{b_{xi}}^{a_{xi}}\rangle$ is represented in Table I for every possible bit value of a_{xi} and b_{xi}. The states $|+\rangle$ and $|-\rangle$ denote the following superposition: $|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$ and $|-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. The quantum state $|\psi_{b_x}^{a_x}\rangle = \overset{m}{\underset{i=1}{\otimes}} |\psi_{b_{xi}}^{a_{xi}}\rangle$ is in the Hilbert space of dimension 2^m.

The quantum state ρ is a density matrix represent by a non-negative Hermitian matrix with trace $Tr(\rho) = 1$. We use $I_{2^m} = \frac{1}{2^m}\sum_{i=1}^{2^m} |i\rangle\langle i|$ to denote the totally mixed state.

a_{xi}	b_{xi}	$\|\psi_{b_{xi}}^{a_{xi}}\rangle$
0	0	$\|0\rangle$
0	1	$\|+\rangle$
1	0	$\|1\rangle$
1	1	$\|-\rangle$

TABLE I
The state $|\psi_{b_{xi}}^{a_{xi}}\rangle$ according to the bit values of a_{xi} and b_{xi}.

A unitary transformation U is a Hermitian matrix with $U = U^\dagger$ and $U^{-1} = U^\dagger$. The unitary transformation U applied to the pure state $|\psi_{b_x}^{a_x}\rangle$ results in the pure state $U|\psi_{b_x}^{a_x}\rangle$ and when the unitary transformation is applied to a mixed state ρ results in the mixed state $U\rho U^\dagger$. We denote by p_i the probability of the unitary transformation U_i to be applied and we denote the superoperator $E = \{\sqrt{p_i}U_i | 1 \le i \le 2^{2m}\}$ (where $\sum_i p_i = 1$). The following unitary transformations are known as the Pauli transformations:

$$\sigma_0 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ \sigma_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$\sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \text{ and } \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Let us sketch the scenario for the quantum version of the one-time-pad know as quantum one-time-pad (QOTP). There are 2^{2m} key and each key c_x corresponds to a unitary transformation U_{c_x}. CA and u_x are connected by a quantum channel where the CA want to transmit to user u_x the quantum state ρ without allowing an eavesdropper to obtain any information about ρ. Let ρ be a pure state without entanglement in form of density matrix then the quantum channel is called a private quantum channel if $E(\rho) = \sum_{c_x=1}^{2^{2m}} p_{c_x} U_{c_x} \rho U_{c_x}^\dagger = \tilde{I}_{2^m}$. Thus, the eavesdropper Eve has no information about ρ encoded with the key c_x apart from the distribution p_{c_x}.

The first proposed quantum one-time-pad code consists of simply applying a random Pauli matrix to each qubit individually. For $c_x \in \{0,1\}^{2m}$ we denote $c_{xi} \in \{00, 01, 10, 11\}$ for its i-th entry and we define the m-qubit unitary transformation by $\bar{\sigma}_{c_x} = \sigma_{c_{x1}} \otimes \sigma_{c_{x2}} \otimes \cdots \otimes \sigma_{c_{xm}}$, then the associated superoperator is $E = \{\frac{1}{\sqrt{2^{2m}}}\bar{\sigma}_{c_x} | c_x \in \{0,1\}^{2m}\}$. For this quantum one-time-pad code one can easily verify that applying the operator E in the state with m qubits result in I_{2^m} (see ref [12]).

The second proposed quantum one-time-pad code uses only two Pauli matrices, σ_0 and σ_1. Associating σ_0 to the bit 0 and σ_1 to the bit 1 then to $c_i \in \{0,1\}$ follows that $\sigma_{c_i}|\psi_{b_{xi}}^{a_{xi}}\rangle = (-1)^\tau |\psi_{b_{xi}}^{a_{xi}\oplus b_{xi}\oplus \bar{ci}}\rangle$. Where $\bar{ci}$ represents the logic operation NOT(ci). Observe that the global phase factor $(-1)^\tau$ does not affect the measurement results, and therefore we will not consider it. Table II provides result for the logical equation $a_{xi} \oplus b_{xi} \oplus \bar{ci}$ in the quantum state and note that $\tau = a_{xi} \wedge (b_{xi} \oplus ci)$ where $\wedge$ denotes the logical

a_{xi}	b_{xi}	c	$\sigma_{ci}\|\psi_{b_{xi}}^{a_{xi}}\rangle$	$(-1)^{\tau}\|\psi_{b_{xi}}^{a_{xi}\oplus b_{xi}\oplus\bar{ci}}\rangle$
0	0	0	$\sigma_0\|0\rangle$	$\|1\rangle$
0	1	0	$\sigma_0\|+\rangle$	$\|+\rangle$
1	0	0	$\sigma_0\|1\rangle$	$\|0\rangle$
1	1	0	$\sigma_0\|-\rangle$	$-\|-\rangle$
0	0	1	$\sigma_1\|0\rangle$	$\|0\rangle$
0	1	1	$\sigma_1\|+\rangle$	$\|-\rangle$
1	0	1	$\sigma_1\|1\rangle$	$-\|1\rangle$
1	1	1	$\sigma_1\|-\rangle$	$\|+\rangle$

TABLE II
THE STATE $\sigma_{ci}|\psi_{b_{xi}}^{a_{xi}}\rangle$ ACCORDING BITS VALUES a_{xi}, b_{xi} AND ci.

operation AND. For $c \in \{0,1\}^m$ we define the m-qubit unitary transformation by $\tilde{\sigma}_c = \sigma_{c1} \otimes \sigma_{c2} \otimes \cdots \otimes \sigma_{cm}$.

III. Quantum identification system over a private quantum channel

As usual, we consider that each communicating agent of the network share a secret key with the CA . Recall that in Section II, the common key between CA and user u_x is divided in three parts $K_x = (a_x, b_x, c_x)$ such that $2|a_x| = 2|b_x| = |c_x| = 2m$. Thus the initialization requires only n keys (one key to each user). Figure 1 shows the initialization of a network QKD links.

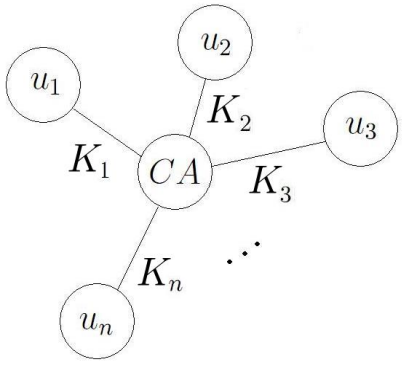

Fig. 1. Initialization of a QKD network of n nodes

The authentication protocol proposed in this article is describe as follows:

Protocol III.1:

1. User u_x requests from the CA the quantum state needed to identify user u_y. CA sends to the u_x the quantum state with m qubits $|\psi_{b_y}^{a_y}\rangle$ coded as in Table I by quantum one-time-pad using the challenge c_x of user u_x, $\bar{\sigma}_{c_x}|\psi_{b_y}^{a_y}\rangle$.
2. User u_x decodes the quantum state sent by the CA, $\bar{\sigma}_{c_x}\bar{\sigma}_{c_x}|\psi_{b_y}^{a_y}\rangle$, and next he uses the unitary transformation of the second presented quantum one-time-pad to write a challenge c randomly chosen by him. Then he sends $|\psi_{b_x}^{a_y\oplus b_y\oplus\bar{c}}\rangle$ to the user u_y.
   (a) User u_x sends $|\psi_{b_y}^{a_y\oplus b_y\oplus\bar{c}}\rangle$ to u_y.
   (b) User u_y correctly measures $|\psi_{b_{xi}}^{a_{yi}\oplus b_{yi}\oplus\bar{c}}\rangle$ because he knows the string b_y. He can calculate the challenge string c because he knows b_y and a_y (NOT$(b_y \oplus a_y \oplus a_y \oplus b_y \oplus \bar{c})$=$c$).
   (c) Finally, u_y send a message signed with a message authentication code (M, MAC(M, c)) to prove his identity to u_x.

Note that the user u_y has shown his identity to u_x without revealing his key. For mutual identification, user u_y requests to CA the quantum state to identify user u_x using the same protocol. Finally, after this process both users can perform a quantum key distribution. A simple count on the number qubits used shows an improvement of eight times less.

IV. Conclusion

For quantum key distribution protocols to be robust to the man-in-the-middle attack, users need to authenticate themselves. In order to do so (in an unconditionally secure manner) they need to used Message Authentication Codes, with a small shared key that the system needs to pre-distribute. This step is called the network initialization, and, if after all agents are authenticated to each other the quantum network never goes off, each communication keeps to be perfectly secure. Thus, it is important to have efficient pre-distribution key protocols, since a node might get off and needs to re-authenticate itself to the network.

In this papaer we consider an ideal quantum channel and an initial common key K (remember $K = |Kx| = |Ky| = 4m$) between certification authority and any user. The trivial proposal requires $4|K|$ qubits to provide identification to each pair of users while ours requires $2m = 2(|K|/4)$ qubits. Therefore, the proposed protocol needs eight times less qubits than the trivial one, that uses QKD between CA and u_x (and between CA and u_y) to create one common key between u_x and u_y. Due to the large number of qubits in the trivial proposal, the CA prefers to generate distinct keys for each pair among the n users and, initially distribute to each user its $n-1$ keys appropriately labeled. The keys are stored in classical memory for later authentication. Hence, the initialization of a network with n users requires the pre-distribution of $n(n-1)/2$ pairs of secret keys. Due to reduction number of qubits in our proposal CA can pre-ditribute only n keys and with them, the CA provides the identification of any pair of users. Thus, the protocol proposed in this article is an important improvement for the management of quantum key distribution in a network.

In this paper, we propose a sophisticated quantum key pre-distribution protocol that requires eight times less qubits than the standard one. Better protocols can be devised, assuming that the nodes are always honest, and that the attacking parties do not belong to the network. We let this improvements for future work, as well as a detailed

analysis of the security of the proposed protocol.

V. ACKNOWLEDGMENTS

This research was suported by Brazilian agency FUNCAP in the period from November 2006 until November 2008, it was suported by Brazilian agency CAPES in the period from December 2008 until March 2009, now this work has been suported by SQIG-IT, QSec project PTDC/EIA/67661/2006.

REFERENCES

[1] C. H. Bennett and G. Brassard, "Quantum cryptography: Public-key distribution and coin tossing," *Advances in Cryptology: Proceedings of Crypto 84*, pp. 475 – 480, August 1984.
[2] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug 1991.
[3] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, no. 21, pp. 3121–3124, May 1992.
[4] H.-K. Lo and H. F. Chau, "Unconditional security of quantum key distribution over arbitrarily long distances," *Science*, vol. 283, no. 5410, pp. 2050 – 2056, March 1999.
[5] D. Mayers and A. Yao, "Quantum cryptography with imperfect apparatus," in *FOCS '98: Proceedings of the 39th Annual Symposium on Foundations of Computer Science*. Washington, DC, USA: IEEE Computer Society, 1998, p. 503.
[6] P. W. Shor, "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer," *SIAM Journal on Computing*, vol. 26, no. 5, pp. 1484–1509, 1997.
[7] A. Peres, "How to differentiate between non-orthogonal states," *Physics Letters A*, vol. 128, p. 19, 1988.
[8] D. Kalamidas, "Single-photon quantum error rejection and correction with linear optics," *Physics Letters A*, vol. 343, pp. 331–335, 2005.
[9] D. B. B. de Brito, J. C. do Nascimento, and R. V. Ramos, "Quantum commnunication with polarization-encoded qubit using quantum error correction," *IEEE Journal of Quantum Electronics*, vol. 44, pp. 113–118, 2008.
[10] J. C. do Nascimento, F. A. Mendona, and R. V. Ramos, "Linear optics setup for active and passive quantum error correction in polarization encoded qubits," *Jounal of Modern Optics*, vol. 54, pp. 1467 – 1479, 2007.
[11] M. N. Wegman and L. Carter, "New hash functions and their use in authentication and set equality," *Journal of Computer and System Sciences*, vol. 22, pp. 265 – 279, 1981.
[12] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf, "Private quantum channels," *Foundations of Computer Science, Annual IEEE Symposium on*, vol. 0, p. 547, 2000.
[13] G. Gilbert and M. Hamrick, "Practical quantum cryptography: A comprehensive analysis (part one)," 2000. [Online]. Available: arXiv.org:quant-ph/0009027
[14] D. Ljunggren, M. Bourennane, and A. Karlsson, "Authority-based user authentication in quantum key distribution," *Phys. Rev. A*, vol. 62, no. 2, p. 022305, Jul 2000.
[15] C. Crepau and L. Salvail, "Quantum oblivious mutual identification," *Advances in Cryptology - EUROCRYPT '95*, vol. 921, pp. 133–146, May 1995.
[16] M. Dušek, O. c. v. Haderka, M. Hendrych, and R. Myška, "Quantum identification system," *Phys. Rev. A*, vol. 60, no. 1, pp. 149–156, Jul 1999.
[17] H. N. Barnum, "Quantum secure identification using entanglement and catalysis," 1999. [Online]. Available: arXiv.org:quant-ph/9910072
[18] M. Gu and C. Weedbrook, "Quantum passwords," 2005. [Online]. Available: arXiv.org:quant-ph/0506255