Quantum Authentication based on Entangled States

Aymen GHILEN[1], Fatma Hamzaoui[1], Mostafa AZIZI[2], Ridha Bouallegue[3], Hafedh Belmabrouk[1]
[1]Laboratory of electronics and microelectronics of the Faculty of Sciences of Monastir
Tunisia

[2]Department Computer Engineering ESTO
University Mohamed I st Oujda, Morocco

[3]Innov'com Laboratory
Higher School of Communications (Sup'Com)
PO Box: 2083, Technology city, Km 3.5
Road of Raoued of Ariana, Tunisia
{Ghilen06, azizi.mos}@gmail.com, fatma.hamzaoui@yahoo.fr, ridha.bouallegue@supcom.rnu.tn,
hafedh.belmabrouk@fsm.rnu.tn

ABSTRACT: *In this paper, we present a quantum key distribution protocol with quantum authentication. The authentication process is based on the exchange of entangled pairs between a certification center and a communicator looking for being authenticated. The proposed scheme makes use of unitary quantum gates and the shared random number can be reused later for classical encryption after the authentication has succeeded.*

Keywords: Quantum Key Distribution QKD, Entanglement, Authentication, EPR, Bell State Measurement

Received: 1 August 2013, Revised 30 August 2013, Accepted 2 September 2013

1. Introduction

Ideally, quantum cryptography provides unconditionally secure key distribution between two parties. Several quantum key distribution protocols have been proposed. Three main protocols of these are the BB84 protocol [1], B92 protocol [3], and EPR protocol [2].The first QKD was introduced by Bennett and Brassard and uses four non orthogonal states of single photon. In 1991, Ekert [2] proposed a scheme to achieve secure communications. Any eavesdropping attempt will automatically introduce an abnormal high level of quantum bit error and thus be caught by the ligitimate users. QKD is capable to supply a random shared secret key to two users, whose secrecy is guaranteed by the fundamental laws of quantum mechanics. Many works were interested in studying quantum cryptography [4].

Although QKD protocols are seen by their proponents as unconditionally secure to emphasize its difference with computationally secure classical protocols, there still exists a fundamental flaw which is the lack of any authentication mechanism. Otherwise, QKD is vulnerable to man-in-the-middle attacks. Thus, neither BB84 nor Ekert can guarantee Alice that the person she shares the key with is who she thinks he is. In this context, many quantum authentication schemes were proposed. Some protocols use classical cryptography combined with QKD [6, 7]. Some other authentication schemes use the property of quantum entanglement [8, 9, 10, 11, 12, 13]. Ljunggren's protocol [14] performs authentication integrated with quantum key distribution in virtue of an arbitrator. In this paper, we develop a scheme using EPR pairs to create an authentication key between a certification authority, Alice and a user who wants to be authenticated. The two parties will share an entangled two qubits state. Each one owns one of the half of the entangled qubits. Then, randomly Bob will operate with σ_z or $i.\ \sigma_y$ and send back his particle to Alice who performs a Bell states measurement. In this way, Alice makes sure that the particles are indeed from Bob, and by letting both the state Φ^+ represent the binary bit "0" and the state ψ^+ represent the binary bit "1". Consequently, Alice and Bob can also share a key sequence.

The rest of paper is organized as follows. Section 2 introduces the proposed algorithm. Then, a security analysis is developed in Section 3. Finally, a conclusion is given in Section 4.

2. Basic Idea of the Algorithm

Dirac's notation uses vertical bars and angular brackets for a vector [15]. For instance, $| A >$ denotes a vector termed also *ket*. To each ket $|A>$, a *bra* $<A|$ is associated. Thus, using the bra-ket notation, the vectors $| i >$ and $| j >$ describe the states of systems *I* and *J* associated with the corresponding Hilbert spaces *HI* ans HJ. The state of the total system is given by the tensor product $| i > \otimes | j >$ which is commonly written $| ij >$

A Bell state measurement [5] is a proceedings on a two-qubit system in which one uses the Bell states as the basis.

An EPR pair is a two qubit system which can take one of the four Bell states:

$$|\phi^+ > = \frac{1}{2}(|00> + |11>)$$

$$|\phi^- > = \frac{1}{2}(|00> - |11>)$$

$$|\psi^+ > = \frac{1}{2}(|01> + |10>)$$

$$|\psi^- > = \frac{1}{2}(|01> - |10>)$$

In the proposed scheme, one party is supposed to play the role of a reliable certification authority, Alice, and another party, Bob, whose identity needs to be authenticated before communicating with Alice. Suppose that Alice will prepare *K* pairs of entangled states in the form:

$|\phi^- > = \frac{1}{2}(|00> - |11>)$, where the first particle is held by Alice and the second one is sent to Bob. Our quantum authentication algorithm follows the steps above:

- After having received his own particle, Bob randomly applies one of two unitary quantum gates σ_z or $i\sigma_y$ on this qubit, where $\sigma_z = \begin{matrix} 1 & 0 \\ 0 & -1 \end{matrix}$ and $\sigma_z = \begin{matrix} 0 & -i \\ i & 0 \end{matrix}$.

- Bob now sends back his particle to Alice.

- Alice receives Bob's qubit, then she makes a Bell state measurement on the particle from Bob and her own particle. If Bob performed the unitary quantum operator σ_z on his particle, then, the state measured by Alice is ϕ^+.

However, if Bob performed $i\sigma_y$, then, the initial state ϕ^- will be transformed into the new state $\psi^+ = \frac{1}{2}(| 01 > + |10 >)$. So, the measurement is either ϕ^+ or ψ^+ if no eavesdropper exists.

- Once the transmission of all the *K* pairs is completed, the two parties consider the state ϕ^+ a binary "0" and consider the state ψ^+ a binary "1".

Consequently, Bob and the certification center, Alice, can at the same time share a key, and authenticate Bob. The table below shows the relation between Bob's operations and Alice's measurement results.

Shared EPR pair	Bob's unitary operation	Bell state measurement	Binary number
$\phi^- = \frac{1}{2}(\|00> - \|11>)$	σ_z	$\phi^+ = \frac{1}{2}(\|00> - \|11>)$	0
	$i\sigma_y$	$\psi^+ = \frac{1}{2}(\|01> - \|11>)$	1

Table 1. Bob's Operations and Alice Measurement Results

3. Security Analysis

The security analysis is necessary to validate our scheme; we analyze the strategy of intercept/resend.

When Alice or Bob sends particle back to each other, an eavesdropper Eve may intercept this particle and resend a fake particle instead according to her measurement result.

For example, when Bob sends his particle back to Alice, Eve intercepts it. Eve can not get any information because the shared state is an entangled state and the state of the particle belonging to Bob is:

$$\rho_B = Tr_A \rho_{\psi^+} = Tr_A \rho_{\phi^+} = \frac{1}{2} |0\rangle\langle 0| + |1\rangle\langle 1|$$

Tr is the partial trace of the density matrix ρ_B which is used to describe the quantum state relative to Bob.

For any EPR pair, the state of just one of the qubits is a maximally mixed state.

Therefore, if Eve intercepts the particle sent back to Alice, then sends a fake one to Alice, this particle is in the state $\phi_E = a\,|0\rangle +$ $b\,|0\rangle$ where *a* and *b* are complex numbers describing the probability law of the superpositioned state and whose squared magnitudes sum to 1: $|a|^2 + |b|^2 = 1$.

According to Dirac's notation, the $|\phi_E\rangle$ system has the probability $|a|^2$ to be in the state $|0>$ and the probability $|b|^2$ to be in the state $|1>$.When Alice receives the fake particle from Eve, she makes a Bell state measurement on this latter and her own one. The state of these particles is:

$$\rho_{AE} = \frac{1}{2}\{|0\rangle\langle 0| + |1\rangle\langle 1| \otimes a^2|0\rangle\langle 0| + ab^*|0\rangle\langle 1| + a^* b|1\rangle\langle 0| + b^2|1\rangle\langle 1|\}$$

Alice's Bell state measurement of the two particles should be one of the four Bell states with equal probability. That is means when the certification authority (Alice) gets the result state ψ^- or ϕ^-, she believes that these particles are not from Bob and then aborts this communication. That is, for one shared state, the probability of not being capable to detect Eve is 1/2 , thus for *k* states, the probability to detect Eve is $(1-(1/2)^k)$. When *k* becomes large enough, the probability of detection of Eve becomes approximatively 100% and Eve can't impersonate Bob and disrupt the key distribution process.

In conclusion, our proposed scheme is secure if the error-free channel is used. The above analysis confirms our result.

4. Conclusion

An authentication algorithm with QKD was proposed.

This scheme helps a certification authority to authenticate an external user by sharing an entangled EPR pairs between the two parties and performing some unitary operators and the Bell state measurement. Furthermore, the security analysis show that for a large number of shared pairs, the probability of detection of the eavesdropper rises and the scheme becomes more secure.

The greatest contribution of this scheme is the needless of any classical communication and the simplicity thanks to the reduced number of steps needed to share the authentication key. The major challenges of this scheme are the quantum decoherence effects that may affect the entanglement between the particles and cause a loss of coherence along with the time. So soon, there are no correlations between the qubits and our scheme will no longer work. We can focus in a subsequent work on the impact of adding an extra initial state on the authentication mechanism and the level of security.

5. Acknowledgment

The authors would like to thank Mr. Rached Tourki as well as Mr. Mohamed Boukhari for their help throughout and for encouragement.

References

[1] Bennett, C. H., Brassard, G. (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing, *In*: Proceedings of IEEE International Conference on Computers, *System and Signal Processing*, Bangalore, India (IEEE, New York), p. 175-179.

[2] Ekert, A. K. (1991). *Phys. Rev. Lett*. 67, 661.

[3] Bennett, C. H. (1992). Quantum cryptography using any two nonorthogonal states, Physical Review Letters, 68 (21) 3121 – 2124, 25 May.

[4] Crépeau, C. (1996). Theory and Applications of Cryptology, *In*: Proceeding of 1*st* Intl. Conf., Pragocrypt ’96, Prague (CTU Publishing, Prague), p. 193.

[5] Kim, Y. H., Kulik, S. P., Shih, Y. (2001). Quantum Teleportation of a Polarization State with a Complete Bell State Measurement, *Physical Review Letters*, 86, p.1370-1373.

[6] Miloslav Dusek *et al*. (1999). Quantum identification system, *Physical Review A*, 60, p. 149-156.

[7] Kuhn, D. R. (2003). A hybrid authentication protocol using quantum entanglement and symmetric cryptography, quant-ph/0301150.

[8] Barnum, H. N. (1999). Quantum secure identification using entanglement and catalysis, quant-ph/9910072.

[9] Curty, M., Santos, D. J. (1999). Quantum authentication of classical messages, *Physical Review A*, v. 64.

[10] Xiaoyu Li, Dexi Zhang. (2006). Quantum authentication protocol using entangled states, *In*: Proceedings of the 5*th* WSEAS International Conference on Applied Computer Science, Hangzhou, China, April 16-18, (p. 1004-1009)

[11] Zeng, G., Guo, G. (2000). Quantum authentication protocol, quant-ph/0001046.

[12] Zhang, Y., Li, C., Guo, G. (2000). Quantum authentication using entangled state, quant-ph/0008044.

[13] Zeng, G., Zhang, W. (2000). Identity verification in quantum key distribution, *Physical Review A*, v. 61, 022303.

[14] D. Ljunggren, M. Bourennane and Anders Karlsson, Authority-based user authentication in quantum key distribution *Physical Review A*, vol. 62, 2000, 022305.

[15] PAM Dirac. A new notation for quantum mechanics, *Mathematical Proceedings of the Cambridge Philosophical Society*, 35 (3) 416–418.