Vol 18 No 8, August 2009
1674-1056/2009/18(08)/3189-04

Chinese Physics B

© 2009 Chin. Phys. Soc.
and IOP Publishing Ltd

Secure authentication of classical messages with single photons*

Wang Tian-Yin(王天银)[a)b)†], Wen Qiao-Yan(温巧燕)[a)], and Zhu Fu-Chen(朱甫臣)[c)]

[a)] *State key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*
[b)] *School of Mathematical Science, Luoyang Normal University, Luoyang* 471022, *China*
[c)] *National Laboratory for Modern Communications, P.O.Box 810, Chengdu* 610041, *China*

(Received 27 October 2008; revised manuscript received 31 October 2008)

This paper proposes a scheme for secure authentication of classical messages with single photons and a hashed function. The security analysis of this scheme is also given, which shows that anyone cannot forge valid message authentication codes (MACs). In addition, the lengths of the authentication key and the MACs are invariable and shorter, in comparison with those presented authentication schemes. Moreover, quantum data storage and entanglement are not required in this scheme. Therefore, this scheme is more efficient and economical.

Keywords: message authentication codes, single photons, hash function
PACC: 0365, 4230

1. Introduction

Reliably ensuring that a communication comes from its purported sender, or that stored data have not been tampered with, is an important problem in classical communication networks and data storage systems. Classical cryptography provides data authentication by means of two general techniques: digital signatures[1] and message authentication codes (MACs).[2,3] In both cases, the authentication process is specified by two main algorithms: an encoding, or tagging algorithm (possibly stochastic), and a decoding or verification algorithm. When the sender (Alice) wants to send a certified message to a recipient (Bob), she generates, employing the encoding algorithm, a digital signature or an authentication tag (a function of the message and a secret encoding-key) and appends it to the message. On the reception side, Bob verifies the authenticity of the message by means of the decoding algorithm, which depends on the message, the tag, and a decoding-key. This algorithm returns a bit indication when Bob must regard the message as authentic and accept it as coming from Alice, and when he must discard it. However, in classical signature schemes, the decoding-key is public, and the degree of security provided by classical signature schemes depends on certain unproven assumptions related to the intractability of certain difficult mathematical problems, such as the prime-factorization problem[4] and discrete logarithm problem.[5] Therefore, if a quantum computer is ever built, classical signature schemes will be broken easily.[6] Though information-theoretic secure MACs can be performed by techniques based on hashed functions,[2] the security of the resulting schemes depends on the selection of appropriate hashed functions, and on the use of long authentication keys.

The security of quantum cryptography is based on fundamental properties of quantum mechanics, instead of an unproven assumption concerning the computational complexity of some algorithms, and therefore brings a whole new dimension to security in communications. Since the first quantum key distribution (QKD) protocol was proposed by Bennett and Brassard,[7] quantum cryptography has attracted a great deal of attention and various quantum cryptographic protocols have been proposed.[8−16] Also, several proposals of message authentication using quan-

*Project supported by the National Natural Science Foundation of China (Grant Nos 60873191 and 60821001), the Specialized Research Fund for the Doctoral Program of Higher Education (Grant No 200800131016), Beijing Nova Program (Grant No 2008B51), Key Project of the Chinese Ministry of Education (Grant No 109014), the Natural Science Foundation of Beijing (Grant No. 4072020), the National Laboratory for Modern Communications Science Foundation of China (Grant No 9140C1101010601), the Natural Science Foundation of Education Bureau of Henan Province (Grant No 2008B120005), and the Youth Foundation of Luoyang Normal University.
†Corresponding author. E-mail: wangtianyin@yahoo.cn

tum resources have been presented. Gottesman and Chuang[17] proposed a quantum version of classical digital signature schemes. It allows unconditionally secure authentication of classical messages, but their technique requires limited circulation of the public key. Zeng and Christoph[18] proposed an arbitrated quantum signature scheme by utilizing the correlation of the Greenberger–Horne–Zeilinger (GHZ) states and quantum one-time pad. Lee *et al.*[19] also presented two arbitrated quantum signature schemes based on GHZ states and quantum one-time pad. However, in these schemes,[18,19] the key shared by the signer and the arbitrator or shared by the receiver and the arbitrator could be used just once. Each time when a signer needs to sign an electronic document, he has to obtain a new key shared with the arbitrator through unconditionally secure QKD protocol. Curty *et al*[20] proposed a class of quantum authentication scheme that allows a secure authentication binary classical message with one qubit as the authentication key. Nevertheless, although key recycling is in principle possible in Curty *et al*'s scheme,[20] the security may be drastically reduced. Wang *et al*[21,22] and Li *et al*[23] proposed two arbitrated quantum signature schemes based on single photons, respectively. Yang *et al*[24] proposed an authentication scheme with Einstein–Podolsky–Rosen pairs and polarized single photons.

However, in all previously presented authentication schemes,[17−24] quantum data storage is necessary, and the signatures (or MACs), the encoding-key, and the decoding-key's lengths depend on the authentication message, except the arbitrated quantum signature scheme with appendix.[23] When the authentication message is very large, a lot of classical or quantum resources are required. Therefore, the efficiency of these schemes is not high. In this paper, we study how to improve the authentication of classical messages by using quantum and classical resources. Specifically, we present a scheme for secure authentication of classical messages with single photons and a hashed function, in which entanglement and quantum data storage are not required, and the MACs, the encoding-key, and the decoding-key's lengths are invariable and very short.

The rest of this paper is arranged as follows. In Section 2, we describe the preliminaries. In Section 3, we present the scheme for secure authentication of classical messages with single photons and hashed functions. In Section 4, the security analysis of this scheme is given. Finally, conclusions are drawn in Section 5.

2. Preliminaries

In this section, we will introduce some notations, which are necessary to the following authentication scheme, and are given as follows.

(i) ID_A: the identity of Alice.

(ii) ID_B: the identity of Bob.

(iii) M: the message to be authenticated.

(iv) T: the time of sending the message M.

(v) $H(\cdot)$: $\{0,1\}^* \longrightarrow \{0,1\}^{k_1}$, a hashed function such as MD5 and SHA-1, used to generate a digest.

(vi) $r_A \in_R \{0,1\}^{k_2}$: a k_2-bit string randomly chosen by Alice.

(vii) K: the secret key shared between Alice and Bob, and the length of the secret key string is k. Note that $k = k_1 + k_2$.

(viii) K^i: the i-th bit of the secret key K.

(ix) $||$: the concatenation of two strings.

3. Secure authentication of classical messages

Now let us study how to improve the authentication of classical messages by using quantum and classical resources. Suppose Alice needs to send a certified classical message M to Bob. The goal is to make Bob confident about the authenticity of the message M and the sender. The authentication scheme described in this section requires an error-free quantum channel and an ideal single photon source. This authentication scheme includes the following four steps.

1) Alice establishes a secret key K with Bob through an unconditionally secure QKD protocol.[7]

2) Alice chooses a random number $r_A \in_R \{0,1\}^{k_2}$ and computes $R_A = H(M||ID_A||ID_B||T||K||r_A)$.

3) Alice encodes the string $r_A||R_A$ with her secret key K. The value of K^i determines the encoding basis. If K^i is 0, then $(r_A||R_A)^i$ is encoded in the Z-basis $\{|0\rangle, |1\rangle\}$, where $|0\rangle$ and $|1\rangle$ denote the horizontal and vertical polarization states respectively, and if $(r_A||R_A)^i$=0 (1), $|P^i\rangle = |0\rangle$ ($|1\rangle$); if K^i is 1, then $(r_A||R_A)^i$ is encoded in the X-basis $\{|+\rangle, |-\rangle\}$, where $|+\rangle = \frac{\sqrt{2}}{2}(|0\rangle + |1\rangle)$ and $|-\rangle = \frac{\sqrt{2}}{2}(|0\rangle - |1\rangle)$, and if $(r_A||R_A)^i$=0 (1), $|P^i\rangle = |+\rangle$ ($|-\rangle$). After her encoding, Alice takes the qubits $\otimes_{i=1}^{k}|P^i\rangle$ as the MACs of

the message M, and sends $\otimes_{i=1}^{k}|P^i\rangle$ to Bob through an error-free quantum channel. At the same time, she sends the strings M, ID_A, ID_B, T to Bob with a classical channel. Finally, she updates the encoding-key K to $K\oplus(r_A||R_A)$, where $\oplus$ denotes the bitwise XOR operation.

4) When Bob receives the strings M, ID_A, ID_B, T and the MACs $\otimes_{i=1}^{k}|P^i\rangle$, he measures the received qubits $\otimes_{i=1}^{k}|P^i\rangle$ depending on the secret key K shared with Alice. If K^i=0, the qubit $|P^i\rangle$ is measured with the Z-basis; otherwise, the X-basis. After Bob gains the measurement outcomes $r'_A||R'_A$, he verifies whether the following equation

$$R'_A = H(M||ID_A||ID_B||T||K||r'_A) \tag{1}$$

is true, if it is not true, Bob must discard it and tell Alice the outcome, then they restart the authentication process from the step 1); otherwise, he accepts that the message M is coming from Alice and cannot be tampered, then he also updates the decoding-key K to $K\oplus(r'_A||R'_A)$.

So far we have proposed an authentication scheme of classical messages with single photons and a hashed function. As are shown, only single photons are used, and quantum data storage and entanglement are not required in this scheme.

4. Security analysis

Now let us discuss the security of this authentication scheme.

Firstly, we will show that anyone cannot learn the secret key K except for Alice and Bob. For the key K is established through an unconditionally secure QKD protocol,[7] anyone cannot learn it through this QKD protocol. Thus, if an attacker Eve wants to acquire the key K, she has the only two ways, one is to intercept the message M and its MACs $\otimes_{i=1}^{k}|P^i\rangle$, then deduce the encoding-key K according to that. The other is to entangle an ancillary state on each qubit $|P^i\rangle$ $(i = 1, 2, \ldots, k)$. However, the two options are not valid to this authentication scheme. Let us consider the first option. Suppose Eve intercepts the message M and its MACs $\otimes_{i=1}^{k}|P^i\rangle$, nevertheless, Alice encodes the string $r_A||R_A$ with two different basis according to the key K, and the two basis cannot be perfectly distinguished by measurement according to the law of quantum mechanics. Thus, Eve cannot acquire the key K by measurement, and the optimal attack strategy for her is to perform a SWAP test[25] between the qubit $|P^i\rangle$ and a designated qubit ($|0\rangle$, $|1\rangle$, $|+\rangle$, or $|-\rangle$). Such a test succeeds with average probability $p_{\text{suc}} = \frac{3}{4}$. In addition, at the end of the test the two qubits are entangled, and Eve cannot distinguish between them, so she can perform the SWAP test only once. Therefore, Eve acquires the key K^i with probability $\frac{1}{4}p_{\text{suc}} = \frac{3}{16}$. Let us consider the second option, suppose Eve entangles an ancillary state on each qubit $|P^i\rangle$ $(i = 1, 2, \ldots, k)$, but if she entangles an ancillary state $|E^i\rangle$ on the qubit $|P^i\rangle$, they will inevitably introduce errors and be detected by Bob. Without loss of generality, suppose Eve employs a general operation U on the qubit $|P^i\rangle$ and the ancillary state $|E^i\rangle$, which can be denoted as follows:

$$U|0\rangle|E^i\rangle = a|0\rangle|\delta_{00}\rangle + b|1\rangle|\delta_{01}\rangle, \tag{2}$$

$$U|1\rangle|E^i\rangle = c|0\rangle|\delta_{10}\rangle + d|1\rangle|\delta_{11}\rangle, \tag{3}$$

where $||a||^2 + ||b||^2 = 1$ and $||c||^2 + ||d||^2 = 1$. Since the qubit $|P^i\rangle$ is one of the four states $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|-\rangle$, if Eve wants to introduce no error. The general operation U must satisfy the following conditions:

$$U|0\rangle|E^i\rangle = a|0\rangle|\delta_{00}\rangle + b|1\rangle|\delta_{01}\rangle = a|0\rangle|\delta_{00}\rangle, \tag{4}$$

$$U|1\rangle|E^i\rangle = c|0\rangle|\delta_{10}\rangle + d|1\rangle|\delta_{11}\rangle = d|1\rangle|\delta_{11}\rangle, \tag{5}$$

$$\begin{aligned} U|+\rangle|E^i\rangle &= (a|0\rangle|\delta_{00}\rangle + b|1\rangle|\delta_{01}\rangle \\ &\quad + c|0\rangle|\delta_{10}\rangle + d|1\rangle|\delta_{11}\rangle)/\sqrt{2} \\ &= |+\rangle(a|\delta_{00}\rangle + b|\delta_{01}\rangle + c|\delta_{10}\rangle + d|\delta_{11}\rangle)/2 \\ &\quad + |-\rangle(a|\delta_{00}\rangle - b|\delta_{01}\rangle + c|\delta_{10}\rangle - d|\delta_{11}\rangle)/2 \\ &= |+\rangle(a|\delta_{00}\rangle + b|\delta_{01}\rangle + c|\delta_{10}\rangle + d|\delta_{11}\rangle)/2, \end{aligned} \tag{6}$$

$$\begin{aligned} U|-\rangle|E^i\rangle &= (a|0\rangle|\delta_{00}\rangle + b|1\rangle|\delta_{01}\rangle \\ &\quad - c|0\rangle|\delta_{10}\rangle - d|1\rangle|\delta_{11}\rangle)/\sqrt{2} \\ &= |+\rangle(a|\delta_{00}\rangle + b|\delta_{01}\rangle - c|\delta_{10}\rangle - d|\delta_{11}\rangle)/2 \\ &\quad + |-\rangle(a|\delta_{00}\rangle - b|\delta_{01}\rangle - c|\delta_{10}\rangle + d|\delta_{11}\rangle)/2 \\ &= |-\rangle(a|\delta_{00}\rangle - b|\delta_{01}\rangle - c|\delta_{10}\rangle + d|\delta_{11}\rangle)/2. \end{aligned} \tag{7}$$

From the above equations (4), (5), (6) and (7), we can get

$$b = c = 0, \tag{8}$$

$$a|\delta_{00}\rangle - b|\delta_{01}\rangle + c|\delta_{10}\rangle - d|\delta_{11}\rangle = \mathbf{0}, \tag{9}$$

$$a|\delta_{00}\rangle + b|\delta_{01}\rangle - c|\delta_{10}\rangle - d|\delta_{11}\rangle = \mathbf{0}. \tag{10}$$

Here $\mathbf{0}$ denotes a column vector. Further, we can get $a|\delta_{00}\rangle = d|\delta_{11}\rangle$, and conclude that Eve introduces no error only when the ancillary state $|E^i\rangle$ and the qubit

$|P^i\rangle$ are product states, so this attack is also invalid to this authentication scheme. Therefore, anyone cannot learn the key K.

Secondly, we will show that anyone cannot forge valid MACs if he/her cannot learn the secret key K. Suppose Eve tempers the message M sent by Alice and sends a forgery message M' to Bob, Eve must prepare corresponding MACs of the message M' if she wants to pass Bob's verification. However, Eve will choose the wrong basis with the probability 50% when she prepares the MACs because she does not know the key K. Therefore, Bob will detect the forgery message M'.

In the end, we emphasize that in this presented authentication scheme, the preshared secret key is used together with a random number, Eve will not obtain the same polarization qubits even if the same message is transmitted again; moreover, the key is updated after successfully authenticating a message. Therefore, different MACs are generated with different encoding-keys, and Eve cannot forge valid MACs by impersonating Alice even if she has a lot of messages and their MACs.

5. Conclusions

We propose a scheme for secure authentication of classical messages with single photons and a hashed function. We also analyze the security of this scheme, and show that anyone cannot alter the message sent by Alice even if she has a lot of messages and their MACs. In addition, in this scheme, no entanglement and quantum data storage are required, and the MACs, the encoding-key, and the decoding-key's length do not depend on the authentication message. Moreover, the QKD protocol in step 1) is performed only when the authentication message is attacked. Therefore, this scheme is more efficient and economical, in comparison with those presented schemes.

References

[1] Diffie W and Hellman M 1976 *IEEE Transactions on Information Theory* **22** 644

[2] Wegman M N and Carter J L 1981 *J. Computer and System Sciences* **22** 265

[3] Yang B, Karri R and McGrew D 2006 *IEEE J. Selected Areas in Communication* **24** 1831

[4] Rivest R, Shamir A, and Adleman L 1978 *Communications of the ACM* **21** 120

[5] ElGamal T 1985 *IEEE Transactions on Information Theory* **31** 469

[6] Shor P 1997 *SIAM J. Computing* **26** 1484

[7] Bennett C H and Brassard G 1984 Proc. *IEEE Int. Conf. on Computers, Systems and Signal Processing*, Bangalore, India (IEEE, New York) 173

[8] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[9] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121

[10] Yang L, Wu L A and Liu S H 2002 *Acta Phys. Sin.* **51** 2446 (in Chinese)

[11] Guo F Z, Gao F, Wen Q Y and Zhu F C 2006 *Chin. Phys.* **15** 1690

[12] Man Z X and Xia Y J 2007 *Chin. Phys.* **16** 1197

[13] Song J, Zhu A D and Zhang S 2007 *Chin. Phys.* **16** 621

[14] Mi J L, Wang F Q, Lin Q Q and Liang R S 2008 *Chin. Phys.* B **17** 1178

[15] Gao F, Wen Q Y and Zhu F C 2008 *Chin. Phys.* B **17** 3189

[16] Wang T Y, Qin S J, Wen Q Y and Zhu F C 2008 *Acta Phys. Sin.* **57** 7452 (in Chinese)

[17] Gottesman D and Chuang I 2001 http://arxiv.org/abs/quant-ph/0105032

[18] Zeng G H and Christoph H K 2002 *Phys. Rev.* A **65** 042312

[19] Lee H, Hong C, Kim H, Lim J and Yang H J 2004 *Phys. Lett.* A **321** 295

[20] Curty M and Santos D J 2001 *Phys. Rev.* A **64** 062309

[21] Wang J, Zhang Q and Tang C J 2006 *Int. Conf. on Advanced Communication Technology* (IEEE, New York) 1375

[22] Wang J, Zhang Q and Tang C J 2007 *J. on Communications* **28** 64 (in Chinese)

[23] Li Q, Long D Y and Wang C J 2008 http://arxiv.org/abs/0806.0557

[24] Yang Y G, Wen Q Y and Zhu F C 2007 *Chin. Phys.* **16** 1838

[25] Buhrman H, Cleve R, Watrous J and Wolf R 2001 *Phys. Rev. Lett.* **87** 167902