Fair quantum blind signatures*

Wang Tian-Yin(王天银)[a)b)†] and Wen Qiao-Yan(温巧燕)[a)]

[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*

(Received 25 September 2009; revised manuscript received 17 November 2009)

We present a new fair blind signature scheme based on the fundamental properties of quantum mechanics. In addition, we analyse the security of this scheme, and show that it is not possible to forge valid blind signatures. Moreover, comparisons between this scheme and public key blind signature schemes are also discussed.

Keywords: fair blind signature, single photons, hash function

PACC: 0367, 0365, 4230

1. Introduction

The concept of a blind signature scheme was first introduced by Chaum. A blind signature scheme is a protocol that allows users to obtain the signature of a message in a way that the signer learns neither the message nor the resulting signature.[1] Blind signature schemes have been used to realize cryptographic protocols providing the anonymity of some participants, e.g., in electronic voting protocols, the votes need to be signed by the manager, but the content of the votes cannot be known by anyone including the manager,[2] and in secure electronic payment systems, the bank should sign the electronic-cash but protect the anonymity of the electronic-cash holders in each transaction.[1,3−8]

These protocols[1−8] provide perfect unlinkability, i.e., it is impossible except for the owner of a message to link the message-signature pair to the corresponding instance of the signing protocol. Unfortunately, this anonymity could be misused by criminals. In anonymous electronic payment systems, blind signatures prevent linking the withdrawal of money and the payment made by the same customer. The impossibility of relating withdrawals and payments allows perfect black-mailing or money-laundering. To solve this problem, Stadler *et al.*[9] proposed the concept of fair blind signatures, whereby the anonymity could be removed with the help of a trusted entity, when this is required for legal reasons. Over the years, much attention has been paid to fair blind signatures and their applications.[10−14]

The security of all such public key blind signature schemes[1−14] presently depends on the inability of a forger to solve certain difficult mathematical problems, such as factoring large numbers and solving discrete logarithms. Unfortunately, if a quantum computer is ever built, these difficult problems become tractable, thus allowing blind signatures to be forged.[15]

The physics of quantum systems opens a door to tremendously intriguing possibilities for cryptography, the art and science of communicating in the presence of adversaries. The security of quantum communication 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.[16−35] The idea of applying quantum mechanics to digital signatures was first introduced by Gottesman and Chuang,[36] whose scheme was absolutely secure even against quantum attack. Since then, a lot of quantum signature schemes have been presented.[37−43] Recently, Wen *et al.* proposed the first quantum weak blind signature scheme by using the correlation of Einstein–

*Project supported by the National Natural Science Foundation of China (Grant Nos. 60873191, 60903152 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), China Postdoctoral Science Foundation (Grant No. 20090450018), the Natural Science Foundation of the Education Bureau of Henan Province of China (Grant No. 2010B120008), and the Youth Foundation of Luoyang Normal University.

†Corresponding author. E-mail: wangtianyin@yahoo.cn

© 2010 Chinese Physical Society and IOP Publishing Ltd

Padolsky–Rosen (EPR) pairs and a one-time pad.[44] This scheme gives unconditional security, and once some disagreement happens, the signer can trace the message owner with the help of the trusted entity. Nevertheless, this scheme is not efficient as signing an n-bit message uses up n EPR pairs and a $4n$-bit key. In addition, the signing key can be used only once. Thus, when a signatory needs to sign the next electronic document, the signer has to obtain a new signing key. This will seriously impact availability and performance.

In this paper, we present a new fair blind signature scheme based on the fundamental properties of quantum mechanics. In this scheme, only single photons are used. In addition, the signing key can be reused. Moreover, this scheme is more efficient compared with the similar scheme in Ref. [44].

The rest of this paper is organized as follows. In the next section, we introduce some necessary preliminaries. In Section 3, we present this fair quantum blind signature scheme. Subsequently, a security analysis and discussion of this scheme are presented in Section 4. Finally, conclusions are drawn in Section 5.

2. Preliminaries

In this section, let us introduce the fair blind signature, hash function and some other relevant preliminaries that are useful in presenting this scheme.

A fair blind signature scheme consists of several senders, a signer, and a trusted entity (e.g., a judge), and of two protocols:

(i) A signing protocol involving the signer and a sender.

(ii) A link-recovery protocol involving the signer and the trusted entity.

By executing the signing protocol, the sender obtains a valid signature of a message of his/her choice such that the signer cannot link his/her view of the protocol to the resulting message-signature pair. By running the link-recovery protocol, the signer obtains information from the trusted entity that enables him/her to recognize the corresponding protocol view and message-signature pair.[9]

In general, a fair blind signature should have the following properties:

(a) Non-forgeability Nobody can generate a valid blind signature except for the legal signer.

(b) Non-deniability Once the signer issues a blind signature, he/she cannot deny it.

(c) Verifiability Anyone can verify the validity of blind signatures.

(d) Blindness The signer cannot know the content of the message that he/she has signed.

(e) Traceability Once some disagreement happens, the signer can trace the message owner with the help of a trusted entity.

A hash function is any well-defined procedure or mathematical function which converts a large, possibly variable-sized amount of data into a small datum, usually a single integer that may serve as an index into an array. The values returned by a hash function are called hash values, hash codes, hash sums, or simply hashes.[45] We denote a collision-free hash function by

$$H(\cdot) : \{0,1\}^* \longrightarrow \{0,1\}^k, \tag{1}$$

which is used to generate a fingerprint in this paper. The notation $||$ denotes the concatenation of strings, and ID_i represents the identity of the sender U_i.

Applying the preliminaries introduced above, we will detail this fair quantum blind signature scheme in the next section.

3. Fair quantum blind signature scheme

The presented fair quantum blind signature scheme includes four phases: initializing phase, signing phase, verifying phase and link-recovery phase. A signer Alice, a trusted entity Charlie, and several senders U_i, $i = 1, 2, \ldots, N$, are also involved.

3.1. Initializing phase

The signer Alice establishes a k-bit key $K_{\rm AC}$ with the trusted entity Charlie in a secure manner, e.g., by directly contacting or using an unconditionally secure quantum key distribution protocol.[16−18] Every sender U_i, $i = 1, 2, \ldots, N$, also establishes a k_i-bit key K_i with Charlie in a similar manner. As an aside, this phase is performed only once, i.e., the shared keys $K_{\rm AC}$ and K_i, $i = 1, 2, \ldots, N$, could be reused, and this phase should be completed in advance.

3.2. Signing phase

When the sender U_i wants to obtain the blind signature of a message M from Alice, he sends a request to Alice, then he can obtain the blind signature by executing the following signing protocol with Alice.

(I) The sender U_i randomly chooses a number $r_i \in \{0,1\}^{k_i}$, and computes the fingerprint of the string $M||r_i$ as follows:

$$R_i = H(M||r_i). \tag{2}$$

Then he sends the fingerprint R_i to Alice.

(II) When Alice receives the fingerprint R_i, she generates the signature $|S\rangle = \otimes_{j=1}^{k}|S^j\rangle$ by encoding the string R_i with her signing key $K_{\rm AC}$; the value of $K_{\rm AC}^j$ determines the encoding basis, where $K_{\rm AC}^j$ denotes the j-th bit of the key $K_{\rm AC}$. If $K_{\rm AC}^j$ is 0, R_i^j is encoded in the rectilinear basis $\{|0\rangle, |1\rangle\}$, i.e., $|S^j\rangle$ is $|0\rangle$ ($|1\rangle$) when $R_i^j = 0$ (1); otherwise, if $K_{\rm AC}^j$ is 1, R_i^j is encoded in the diagonal basis $\{|+\rangle, |-\rangle\}$, i.e., $|S^j\rangle$ is $|+\rangle$ ($|-\rangle$) when $R_i^j = 0$ (1), where $|+\rangle = \frac{\sqrt{2}}{2}(|0\rangle + |1\rangle), |-\rangle = \frac{\sqrt{2}}{2}(|0\rangle - |1\rangle)$, and R_i^j denotes the j-th bit of the string R_i. Then she sends the signature $|S\rangle$ to U_i via an error-free quantum channel and stores the fingerprint R_i in her database.

(III) When the sender U_i receives the signature $|S\rangle$, he generates the qubits $|R\rangle = \otimes_{i=1}^{k_i}|R^i\rangle$ by encoding the string r_i with the key K_i by the same method as Alice does in step (II). The resulting blind signature of the message M is $(|S\rangle, |R\rangle)$.

3.3. Verifying phase

When the blind signature $(|S\rangle, |R\rangle)$ needs to be verified, the sender U_i sends it to the trusted entity Charlie via an error-free quantum channel. At the same time, he sends the message M and his identity ID_i to Charlie via a classical channel, or a quantum channel after transforming them to qubits according to the rectilinear basis $\{|0\rangle, |1\rangle\}$.

After receiving the message-signature pair $(M, |S\rangle, |R\rangle)$ and the identity ID_i, Charlie performs single-particle measurements on the qubits $\otimes_{j=1}^{k}|S^j\rangle$ depending on the key $K_{\rm AC}$ shared with Alice. If $K_{\rm AC}^j$=0, Charlie measures the qubit $|S^j\rangle$ with the rectilinear basis $\{|0\rangle, |1\rangle\}$; otherwise, he measures it with the diagonal basis $\{|+\rangle, |-\rangle\}$. In the same way, he measures the qubits $\otimes_{i=1}^{k_i}|R^i\rangle$ depending on the key K_i shared with U_i. After gaining the measurement outcomes R_i' and r_i', Charlie verifies whether R_i' is equal to

$$H(M||r_i'). \tag{3}$$

If it is not, the signature is not valid; otherwise, Charlie accepts the signature and stores R_i', M and ID_i. Then he tells the sender U_i the verification outcome.

If no disagreement happens, the blind signature protocol is now completed. Otherwise, we continue to run the following link-recovery protocol.

3.4. Link-recovery phase

The signer Alice sends the fingerprint R_i to the trusted entity Charlie, Charlie performs a search in his database until he finds out $R_i' = R_i$. Then he can trace the message-signature pair $(M, |S\rangle, |R\rangle)$ and the sender's identity ID_i according to the fingerprint R_i' stored in the verifying phase.

4. Security analysis and discussion

This fair quantum blind signature scheme is based on private key cryptosystems. The trusted entity Charlie knows the signing key $K_{\rm AC}$ and each sender's encryption key K_i, $i = 1, 2, \ldots, N$. Moreover, he acts as the judge in the verifying phase. These enable him to generate valid blind signatures. Therefore, the trusted entity Charlie must be totally credible in this scheme, i.e., he does not forge signatures, or help one party to cheat the other party. In the following, we will show that this scheme can satisfy the properties of non-forgeability, non-deniability, blindness and traceability under the condition that Charlie is totally credible.

4.1. Non-forgeability

Firstly, we show that it is impossible to obtain the signing key $K_{\rm AC}$ except for Alice and Charlie. Because the signing key $K_{\rm AC}$ is established in a secure manner, nobody can learn it through this process except Alice and Charlie. Therefore, if an opponent wants to acquire the key $K_{\rm AC}$, he has only two ways, one is to obtain l, $l \geq 0$, legitimate messages and the corresponding blind signatures, and then deduce the signing key $K_{\rm AC}$ by measuring the obtained qubits. The other is to entangle an ancillary state on every qubit $|S^j\rangle$, $j = 1, 2, \ldots, k$, when it is sent to Charlie, and then gain some useful information by measuring the ancillary state. However, the signer Alice encodes each string R_i with two different bases according to the key $K_{\rm AC}$ and the two bases cannot be perfectly distinguished according to the measurement postulate of the quantum theory. If the opponent can acquire the signing key $K_{\rm AC}$, he can perfectly distinguish the

bases $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$. Obviously, this is contradictory to quantum mechanics. Therefore, it is not possible for anybody to obtain the signing key $K_{\rm AC}$ except Alice and Charlie.

Secondly, we show that it is impossible to forge a valid blind signature if the opponent does not know the signing key $K_{\rm AC}$. Because the opponent does not know the signing key $K_{\rm AC}$, he will choose the wrong encoding bases with the probability 50% when he prepares the signature $|S\rangle$, thus he will introduce no less than 25% error rate and cannot pass the trusted entity Charlie's verification. A feasible attack is to tamper with the content of the message M when the opponent obtains the legitimate message-signature pair $(M, |S\rangle, |R\rangle)$. Nevertheless, since $H(\cdot)$ is a collision-free hash function, it is impossible to find M', and r_i' such that $H(M||r_i) = H(M'||r_i')$. Therefore, nobody can generate valid blind signatures or tamper with the content of the legitimate message except Alice and Charlie.

4.2. Non-deniability

Since only Alice and Charlie can generate valid blind signatures, Charlie is totally trusted, and the signing key $K_{\rm AC}$ is included in the verifying phase, once the signer Alice issues a blind signature, she cannot deny it.

4.3. Blindness

In the signing phase, the sender U_i only sends the fingerprint R_i of the message M to the signer Alice. In addition, it is impossible to learn M due to the property of $H(\cdot)$. Therefore, Alice does not know the content of the message M that she has signed, i.e., the message M is "blind" to her.

4.4. Traceability

Once some disagreement happens, the signer Alice can trace the message-signature pair and the sender with the help of the trusted entity Charlie by running the link-recovery protocol.

Unlike public blind signature schemes,[1−14] only the trusted entity Charlie can verify the validity of blind signatures in this scheme. This is primarily because this scheme is based on private key cryptosystems. Compared with public key blind signature schemes,[1−14] the security of this scheme is based on fundamental properties of quantum mechanics, instead of an unproven assumption, and the signature $|S\rangle$ are unknown qubits to the sender U_i. Therefore he cannot generate an identical signature according to the no-cloning theorem, which means the blind signature $(|S\rangle, |R\rangle)$ can be used only once, but this special property can be used to prevent electronic-cash from being double-spent. Compared with the scheme in Ref. [44], this scheme is more efficient, as signing an n-bit message only uses up k qubits no matter how large n is. In addition, the key $K_{\rm AC}$ and K_i, $i = 1, 2, \ldots, N$, are shorter and could be reused. Moreover, entanglement is not necessary in this scheme.

It is noted that this scheme requires quantum storage and an error-free quantum channel, which are difficult to achieve with present technology. Nevertheless, these problems may be resolved in the future with the development of quantum technology.

5. Conclusion

In summary, using single photons and hash functions, we have presented a new fair quantum blind signature scheme. We have also analysed the security of this scheme and shown that it is impossible to forge valid blind signatures in theory. This scheme is more efficient compared with the previous scheme under quantum cryptography and may have a wide application in secure electronic-payment systems, and electronic-government, etc.

References

[1] Chaum D 1983 *Advances in Cryptology-Crypto 1982* (Berlin: Springer-Verlag) p. 199

[2] Benaloh J and Yung D 1986 *Proceedings of the 5th ACM Symposium on Principles of Distributed Computing* (New York: ACM Press) p. 52

[3] ElGamal T 1985 *IEEE Transaction on Information Theory* **IT-31** 469

[4] Chaum D, Fait A and Naor M 1988 *Advances in Cryptology-Crypto 1988* (Berlin: Springer-Verlag) p. 319

[5] Brands S 1994 *Advances in Cryptology-Crypto 1993* (Berlin: Springer-Verlag) p. 302

[6] Camenisch J L, Pivetau J M and Stadler M A 1995 *Advances in Cryptology-Eurocrypto 1994* (Berlin: Springer-Verlag) p. 428

[7] Abe M and Okamoto T 2000 *Advances in Cryptology-Crypto 2000* (Berlin: Springer-Verlag) p. 271

[8] Wang T Y, Cai X Q and Zhang J Z 2007 *Application Research of Computers* **24** 130 (in Chinese)

[9] Stadler M, Piveteau J M and Camenisch J 1995 *Advances in Cryptology-Eurocrypto 1995* (Berlin: Springer-Verlag) p. 209

[10] Camenisch J, Piveteau J M and Stadler M 1996 *Proceedings of the 3rd ACM Conference on Computer and Communications Security* (New York: ACM Press) p. 88

[11] Maitland G and Boyd C 2001 *Proceedings of ICICS 2001* (Berlin: Springer-Verlag) p. 461

[12] Traore J and Canard S 2003 *Proceedings of ACISP'03* (Berlin: Springer-Verlag) p. 237

[13] Wang T Y, Cai X Q and Zhang J Z 2007 *Computer Engineering and Applications* **33** 155 (in Chinese)

[14] Wang C J, Tang Y and Li Q 2007 *J. Computer and Technology* **22** 487

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

[16] Bennett C H and Brassard G 1984 *IEEE Int. Conf. on Computers, Systems and Signal Processing* (New York: IEEE) p. 175

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

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

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

[20] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A **68** 042317

[21] Guo G P and Guo G C 2003 *Phys. Lett.* A **310** 247

[22] Deng F G, Li X H, Zhou H Y and Zhang Z J 2005 *Phys. Rev.* A **72** 044302

[23] Yan F L and Gao T 2005 *Phys. Rev.* A **72** 012304

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

[25] Sun Y, Du J Z, Qin S J, Wen Q Y and Zhu F C 2008 *Acta Phys. Sin.* **57** 4689 (in Chinese)

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

[27] Wang T Y, Wen Q Y, Chen X B, Guo F Z and Zhu F C 2008 *Opt. Commun.* **281** 6130

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

[29] Wang T Y, Wen Q Y, Gao F, Lin S and Zhu F C 2008 *Phys. Lett.* A **373** 65

[30] Wang X B 2005 *Phys. Rev.* A **72** 050304

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

[32] Lin S, Wen Q Y, Gao F and Zhu F C 2008 *Phys. Rev.* A **78** 064304

[33] Song T T, Zhang J, Gao F, Wen Q Y and Zhu F C 2009 *Chin. Phys.* B **18** 1333

[34] Wang T Y, Wen Q Y and Zhu F C 2009 *Chin. Phys.* B **18** 3189

[35] Wang T Y, Wen Q Y and Zhu F C 2009 *Opt. Commun.* **282** 3382

[36] Gottesman D and Chuang I 2001 arXiv:0105032 [quant-ph]

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

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

[39] Wang J, Zhang Q, Liang L M and Tang C J 2005 *Phys. Lett.* A **347** 262

[40] Yang Y G, Wen Q Y and Zhu F C 2008 *Chin. Phys.* B **17** 415

[41] Wen X J, Liu Y and Sun Y 2007 *Z. Naturforschung* A **62** 147

[42] Curty M and Lütkenhaus N 2008 *Phys. Rev.* A **77** 046301

[43] Li Q, Chan W H and Long D Y 2009 *Phys. Rev.* A **79** 054307

[44] Wen X J, Niu X M, Jia L P and Tian Y 2009 *Opt. Commun.* **282** 666

[45] Damgård I 1990 *Advances in Cryptology-Crypto 1989* (Berlin: Springer-Verlag) p. 416