Cryptanalysis of fair quantum blind signatures*

He Li-Bao(何立宝)[a)b)†], Huang Liu-Sheng(黄刘生)[a)b)], Yang Wei(杨 威)[b)], and Xu Rui(许 瑞)[b)]

[a)] *National High Performance Computing Center, Department of Computer Science and Technology, University of Science and Technology of China, Hefei* 230026, *China*

[b)] *Suzhou Institute for Advanced Study, University of Science and Technology of China, Suzhou* 215123, *China*

(Received 12 October 2010; revised manuscript received 31 August 2011)

We investigate the fair quantum blind signature scheme proposed by Wang and Wen [Wang T Y and Wen Q Y 2010 *Chin. Phys.* B **19** 060307], which uses the fundamental properties of quantum mechanics and the availability of a trusted arbitrator. However, in this paper, we find that the protocol cannot satisfy the property of non-forgeability even under the condition that the trusted arbitrator is totally credible. Moreover, a simple feasible suggestion for improving the protocol is proposed.

Keywords: fair blind signature, single photons, hash function

PACS: 03.67.Dd, 03.67.–a, 03.67.Ac, 03.67.Hk **DOI:** 10.1088/1674-1056/21/3/030306

1. Introduction

Digital signature, which plays an import role in modern cryptography, is a mathematical scheme employed to guarantee the authenticity, integrity and non-disavowal of digital messages or documents. Most classical digital signature schemes, whose security depends on some unproven difficult mathematical problems, such as the prime-factorization problem[1] and discrete logarithm problem,[2] would be broken by Shor's algorithm[3] once quantum computers are available in the future. However, in the quantum field, digital signature combining quantum theory with information theory, which is called quantum signature, uses the laws of physics to provide unconditionally secure authenticity of the data, in contrast to classical methods based on complexity theoretic assumptions.

Up to now, there exist lots of quantum signature schemes.[4−13] However, these common quantum signatures cannot satisfy the special needs in some specific applications, e.g., in E-voting and E-cash systems, the required signature scheme should protect the anonymity of message owners. Based on such a demand, some researchers tried to realize blind signatures[14] with quantum cryptography. Fortunately, they have successfully found several quantum blind signature schemes[15−18] in recent years. Wen *et al.*[15] proposed the first quantum weak blind signature scheme using the correlation of EPR pairs and a quantum one-time pad in 2008. Two years later, a new quantum blind signature based on a two-state vector formalism which has high efficiency and is easier to implement was designed by Su et al.[16] Afterwards, Xu *et al.*[17] proposed a quantum group blind signature scheme designed for a distributed E-voting system without using entanglements. In addition, In Ref. [18], Wang and Wen presented a fair quantum blind signature scheme whose signing key can be reused without restrictions. However, in fact, a long-term signing key cannot guarantee the security of a fair quantum blind signature scheme.

Fair blind signature schemes[19−21] consist of two protocols, a signing protocol involving the signer and a message owner, and a link-recovery protocol involving the signer and the trusted entity. By executing the signing protocol, the message owner could obtain a valid signature of a message in a way that the signer learns neither the message nor the resulting signature. By running the link-recovery protocol, the signer can trace the message owner with the help of the trusted entity. In Ref. [18], Wang and Wen presented a fair quantum blind signature scheme that requires the availability of a trusted entity in signature initialization and verification phases. However, we will show

*Project supported by the Major Research Plan of the National Natural Science Foundation of China (Grant No. 90818005), the National Natural Science Foundation of China (Grant Nos. 60903217 and 60773032), and the China Postdoctoral Science Foundation (Grant No. 20090450701).

†Corresponding author. E-mail: helibao@mail.ustc.edu.cn

© 2012 Chinese Physical Society and IOP Publishing Ltd

that the protocol cannot satisfy the property of non-forgeability even under the condition that the trusted entity is totally credible.

Now, let us start with a brief description of the fair quantum blind signature scheme.[18] For convenience, we use the same notations as in Ref. [18]. The protocol involves a signer Alice, a trusted entity Charlie, and several senders U_i, $i = 1, 2, \ldots, N$. The concrete steps are described as follows:

In the initializing phase, Alice, Charlie, and each U_i distribute two secret keys $K_{\rm AC}$ (Alice-Charlie) with length k and K_i (U_i-Charlie) with length k_i. The phase is performed only once, and should be completed in advance.

The signing phase can perform the task of signing blind messages. The sender U_i prepares a message M, blinds it to R_i based on the formula $R_i = H(M||r_i)$, where r_i is a random number chosen from $\{0,1\}^{k_i}$ and $H(\cdot)$ is a collision-free hash function, and then sends the fingerprint R_i to Alice. When the signer Alice receives R_i from the sender U_i, she generates the signature $|S\rangle = \otimes_{j=1}^{k}|S^j\rangle$ based on the following rules:

1) If $K_{\rm AC}^j = 0$, R_i^j is encoded in a rectilinear basis $\{|0\rangle, |1\rangle\}$, i.e., $|S^j\rangle$ is $|0\rangle$ ($|1\rangle$) when $R_i^j = 0$ (1), where $K_{\rm AC}^j$ denotes the j-th bit of the key $K_{\rm AC}$ and R_i^j denotes the j-th bit of the blind message R_i.

2) If $K_{\rm AC}^j = 1$, 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).

Then she sends the signature $|S\rangle$ to U_i and stores the fingerprint R_i in her database. When the sender U_i receives the signature $|S\rangle$, he generates the qubits $|R\rangle = \otimes_{j=1}^{k_i}|R^j\rangle$ by encoding the string r_i with the key K_i using the same method as Alice described above. The resulting blind signature of the message M is ($|S\rangle$, $|R\rangle$).

The verifying algorithm requires the trusted entity Charlie to verify the validity of the blind signature. After receiving the message–signature pair $(M, |S\rangle, |R\rangle)$ and the U_i's identity ID_i, Charlie performs single-particle measurements on the qubits $\otimes_{j=1}^{k}|S^j\rangle$ with respect to the key $K_{\rm AC}$ shared with Alice based on the following rules:

1) If $K_{\rm AC}^j = 0$, Charlie measures the qubit $|S^j\rangle$ with the rectilinear basis $\{|0\rangle, |1\rangle\}$.

2) If $K_{\rm AC}^j = 1$, Charlie measures the qubit $|S^j\rangle$ with the diagonal basis $\{|+\rangle, |-\rangle\}$.

Similarly, he measures the qubits $\otimes_{j=1}^{k_i}|R^j\rangle$ with respect to the key K_i shared with U_i. After gaining the measurement results R_i' and r_i', Charlie verifies whether R_i' is equal to $H(M||r_i')$. If it is not, the signature is not valid; otherwise, Charlie accepts the signature and stores R_i', M and ID_i.

The link-recovery phase allows the signer Alice to 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.

A major loophole of the quantum blind signature scheme[18] is that the scheme cannot satisfy the property of non-forgeability, an adversary Eve (for example, a malicious sender) who obtains enough blind message and partial signature pairs can successfully deduce the signing key $K_{\rm AC}$ with a probability exponentially close to one. We describe our attack scheme in detail in Table 1.

Table 1. Our attack scheme.

Input:	n pairs. Each pair, denoted by $(R_t', \|S_t\rangle)$ $(1 \le t \le n)$, represents the blind message and the corresponding partial signature.
Output:	$K_{\rm AC}'$.
For each j, $1 \le j \le k$, execute the following steps.	
Step 1:	For each t, $1 \le t \le n$, Eve initializes the variables $C_{tb}^{j\phi}$ to 0, where $\phi \in \{0,1,+,-\}$ and $b \in \{0,1\}$.
Step 2:	For each t, $1 \le t \le n$, Eve randomly chooses a measurement basis denoted as T_t^j between the rectilinear basis $\{\|0\rangle, \|1\rangle\}$ and the diagonal basis $\{\|+\rangle, \|-\rangle\}$.
Step 3:	For each t, $1 \le t \le n$, Eve uses the basis T_t^j to measure the qubit $\|S_t^j\rangle$ and obtain the measurement result $\|S_{tm}^j\rangle$, where $\|S_t^j\rangle$ denotes the j-th qubit of the signature $\|S_t\rangle$. If $\|S_{tm}^j\rangle = \|\psi\rangle$ and $R_t'^j = b_{\rm r}$, where $R_t'^j$ denotes the j-th bit of the blind message R_t', then Eve resets the value of $C_{tb_{\rm r}}^{j\psi}$ to 1.
Step 4:	For each $\phi \in \{0,1,+,-\}$ and each $b \in \{0,1\}$, Eve computes $C_b^{j\phi} = \sum_{t=1}^{n} C_{tb}^{j\phi}$.
Step 5:	Eve infers the signing key $K_{\rm AC}'$ from $C_b^{j\phi}$ based on the following rules:
	① If $C_0^{j1} > 0$ or $C_1^{j0} > 0$, she assigns $K_{\rm AC}'^j$ to 1, where $K_{\rm AC}'^j$ denotes the j-th bit of $K_{\rm AC}'$.
	② If $C_0^{j-} > 0$ or $C_1^{j+} > 0$, she assigns $K_{\rm AC}'^j$ to 0.
	③ If $C_0^{j1}, C_1^{j0}, C_0^{j-}, C_1^{j+} = 0$, she randomly assigns $K_{\rm AC}'^j$ to 0 or 1.

According to the description of our attack scheme mentioned in Table 1, it is not difficult to conclude the conditional probability $P(|S_{tm}^j\rangle = |\phi\rangle \mid K_{\rm AC}^j = b_{\rm AC}^j,\ R_t'^j = b_t^j)$, where $|\phi\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and $b_{\rm AC}^j, b_t^j \in \{0, 1\}$. The probability distributions of $|S_{tm}^j\rangle$ obtained under the condition that $k_{\rm AC}^j$ and $R_t'^j$ take all values in the set $\{0, 1\}$ are described in Table 2.

Table 2. Probability distribution of $|S_{tm}^j\rangle$.

$K_{\rm AC}^j$	$R_t'^j$	$\lvert S_t^j\rangle$	$P(\lvert S_{tm}^j\rangle = \lvert\phi\rangle)$ when $\lvert\phi\rangle$ is			
			$\lvert 0\rangle$	$\lvert 1\rangle$	$\lvert +\rangle$	$\lvert -\rangle$
0	0	$\lvert 0\rangle$	1/2	0	1/4	1/4
	1	$\lvert 1\rangle$	0	1/2	1/4	1/4
1	0	$\lvert +\rangle$	1/4	1/4	1/2	0
	1	$\lvert -\rangle$	1/4	1/4	0	1/2

Lemma 1 If $R_t'^j = 0$, then $P(K_{\rm AC}^j = 0 \mid |S_{tm}^j\rangle = |-\rangle) = 1$ and $P(K_{\rm AC}^j = 1 \mid |S_{tm}^j\rangle = |1\rangle) = 1$.

Proof From Table 2, we know that $P(|S_{tm}^j\rangle = |1\rangle \mid K_{\rm AC}^j = 0, R_t'^j = 0) = 0$ and $P(|S_{tm}^j\rangle = |-\rangle \mid K_{\rm AC}^j = 1, R_t'^j = 0) = 0$. In the case $R_t'^j = 0$, then

$$\begin{aligned}
&P(|S_{tm}^j\rangle = |-\rangle)\\
&= P(|S_{tm}^j\rangle = |-\rangle \mid K_{\rm AC}^j = 0)P(K_{\rm AC}^j = 0)\\
&\quad + P(|S_{tm}^j\rangle = |-\rangle \mid K_{\rm AC}^j = 1)P(K_{\rm AC}^j = 1)\\
&= P(|S_{tm}^j\rangle = |-\rangle \mid K_{\rm AC}^j = 0)P(K_{\rm AC}^j = 0)\\
&= P(K_{\rm AC}^j = 0, |S_{tm}^j\rangle = |-\rangle),
\end{aligned}$$

and

$$\begin{aligned}
&P(|S_{tm}^j\rangle = |1\rangle)\\
&= P(|S_{tm}^j\rangle = |1\rangle \mid K_{\rm AC}^j = 0)P(K_{\rm AC}^j = 0)\\
&\quad + P(|S_{tm}^j\rangle = |1\rangle \mid K_{\rm AC}^j = 1)P(K_{\rm AC}^j = 1)\\
&= P(|S_{tm}^j\rangle = |1\rangle \mid K_{\rm AC}^j = 1)P(K_{\rm AC}^j = 1)\\
&= P(K_{\rm AC}^j = 1, |S_{tm}^j\rangle = |1\rangle).
\end{aligned}$$

Therefore, we have

$$\begin{aligned}
&P(K_{\rm AC}^j = 0 \mid |S_{tm}^j\rangle = |-\rangle)\\
&= \frac{P(K_{\rm AC}^j = 0, |S_{tm}^j\rangle = |-\rangle)}{P(|S_{tm}^j\rangle = |-\rangle)} = 1,
\end{aligned}$$

and

$$\begin{aligned}
&P(K_{\rm AC}^j = 1 \mid |S_{tm}^j\rangle = |1\rangle)\\
&= \frac{P(K_{\rm AC}^j = 1, |S_{tm}^j\rangle = |1\rangle)}{P(|S_{tm}^j\rangle = |1\rangle)} = 1.
\end{aligned}$$

□

Lemma 2 If $R_t'^j = 1$, then $P(K_{\rm AC}^j = 0 \mid |S_{tm}^j\rangle = |+\rangle) = 1$ and $P(K_{\rm AC}^j = 1 \mid |S_{tm}^j\rangle = |0\rangle) = 1$.

Proof Just the same as the Proof of Lemma 1. □

Lemma 3 For any j and t, $1 \le j \le k, 1 \le t \le n$, $P(C_{t0}^{j1} = 1 \text{ or } C_{t0}^{j-} = 1 \text{ or } C_{t1}^{j+} = 1 \text{ or } C_{t1}^{j0} = 1) = 1/4$.

Proof Known from the definition of $C_{tb}^{j\phi}$, $C_{tb}^{j\phi} = 1$ if and only if $R_t'^j = b$ and $|S_{tm}^j\rangle = |\phi\rangle$. After some manipulations, we find

$$\begin{aligned}
&P(C_{t0}^{j1} = 1 \text{ or } C_{t0}^{j-} = 1 \text{ or } C_{t1}^{j+} = 1 \text{ or } C_{t1}^{j0} = 1)\\
&= P(|S_{tm}^j\rangle = |1\rangle \mid R_t'^j = 0)P(R_t'^j = 0) + P(|S_{tm}^j\rangle = |-\rangle \mid R_t'^j = 0)P(R_t'^j = 0)\\
&\quad + P(|S_{tm}^j\rangle = |+\rangle \mid R_t'^j = 1)P(R_t'^j = 1) + P(|S_{tm}^j\rangle = |0\rangle \mid R_t'^j = 1)P(R_t'^j = 1)\\
&= P(|S_{tm}^j\rangle = |-\rangle \text{ or } |1\rangle \mid R_t'^j = 0)P(R_t^j = 0) + P(|S_{tm}^j\rangle = |+\rangle \text{ or } |0\rangle \mid R_t'^j = 1)P(R_t'^j = 1)\\
&= P(|S_{tm}^j\rangle = |-\rangle \text{ or } |1\rangle \mid R_t'^j = 0, K_{\rm AC}^j = 0)P(K_{\rm AC}^j = 0)P(R_t'^j = 0)\\
&\quad + P(|S_{tm}^j\rangle = |-\rangle \text{ or } |1\rangle \mid R_t'^j = 0, K_{\rm AC}^j = 1)P(K_{\rm AC}^j = 1)P(R_t'^j = 0)\\
&\quad + P(|S_{tm}^j\rangle = |+\rangle \text{ or } |0\rangle \mid R_t'^j = 1, K_{\rm AC}^j = 0)P(K_{\rm AC}^j = 0)P(R_t'^j = 1)\\
&\quad + P(|S_{tm}^j\rangle = |+\rangle \text{ or } |0\rangle \mid R_t'^j = 1, K_{\rm AC}^j = 1)P(K_{\rm AC}^j = 1)P(R_t'^j = 1)\\
&= 1/4.
\end{aligned}$$

□

Lemma 4 For any j and t, $1 \le j \le k, 1 \le t \le n$, if $C_{t0}^{j1} = 1, C_{t0}^{j-} = 1, C_{t1}^{j+} = 1$ or $C_{t1}^{j0} = 1$, then $K_{\rm AC}'^j$ must be equal to $K_{\rm AC}^j$; otherwise, $K_{\rm AC}'^j$ equals to $K_{\rm AC}^j$ with probability 1/2.

Proof We use Lemmas 1 and 2 to prove Lemma 4. Without loss of generality, let $C_{t0}^{j1} = 1$, then $C_0^{j1} > 0$. From Step 5 of our attack algorithm, we know that $K_{\rm AC}'^j$ equals 1. In addition, $C_{t0}^{j1} = 1$ means that $R_t'^j = 0$ and $|S_{tm}^j\rangle = |1\rangle$. According to Lemma 1, we can deduce that $K_{\rm AC}^j = 1$ from the equation $P(K_{\rm AC}^j = 1 \mid |S_{tm}^j\rangle = |1\rangle, R_t'^j = 0) = 1$. Therefore, if $C_{t0}^{j1} = 1$, then $K_{\rm AC}'^j$ must be equal to $K_{\rm AC}^j$. Similarly, we can conclude that $K_{\rm AC}'^j = K_{\rm AC}^j$ when $C_{t0}^{j-} = 1, C_{t1}^{j+} = 1$ or $C_{t1}^{j0} = 1$. Known from Step 5 of the proposed attack scheme, Eve randomly assigns $K_{\rm AC}'^j$ to 0 or 1 when $C_{t0}^{j1}, C_{t0}^{j-}, C_{t1}^{j+}$ and C_{t1}^{j0} are all

equal to 0, hence $K'^{j}_{\rm AC}$ equals $K^{j}_{\rm AC}$ with probability 1/2 under the scenario. □

Theorem 5 Suppose Eve obtains n legitimate blind message R'_t $(1 \le t \le n)$ and the corresponding partial signature $|S_t\rangle$, then she could use the proposed attack acheme to recover the signing key $K_{\rm AC}$ with a success probability at least equal to $(1-(3/4)^n)^k$, where k is the length of the signing key $K_{\rm AC}$.

Proof We use Lemmas 3 and 4 to prove the theorem. For any j, $1 \le j \le k$, it is not difficult to conclude that

$$\begin{aligned}
&P(K'^{j}_{\rm AC} = K^{j}_{\rm AC}) \\
&\ge P(C_0^{j1} > 0 \text{ or } C_0^{j-} > 0 \text{ or } C_1^{j+} > 0 \text{ or } C_1^{j0} > 0) \\
&= 1 - \prod_{t=1}^{n} P(C_{t0}^{j1} = 0 \text{ and } \\
&\quad C_{t0}^{j-} = 0 \text{ and } C_{t1}^{j+} = 0 \text{ and } C_{t1}^{j0} = 0) \\
&= 1 - \prod_{t=1}^{n} (1 - P(C_{t0}^{j1} = 1 \text{ or } \\
&\quad C_{t0}^{j-} = 1 \text{ or } C_{t1}^{j+} = 1 \text{ or } C_{t1}^{j0} = 1)) \\
&= 1 - (3/4)^n.
\end{aligned}$$

Therefore, we have

$$\begin{aligned}
P(K'_{\rm AC} = K_{\rm AC}) &= \prod_{j=1}^{k} P(K'^{j}_{\rm AC} = K^{j}_{\rm AC}) \\
&\ge (1-(3/4)^n)^k,
\end{aligned}$$

where $K'_{\rm AC}$ is the recovered signing key by utilizing our attack scheme. □

Remark $P(K'_{\rm AC} = K_{\rm AC}) \ge (1-(3/4)^n)^k \ge 1 - k(3/4)^n$, which demonstrates that any sender can successfully recover the signing key $K_{\rm AC}$ with a probability exponentially close to one once k is fixed.

Definition (h-security) The singing key $K_{\rm AC}$ has h-security if it can be recovered by using our attack scheme with a probability at most $1-h$, where $0 \le h \le 1$.

Remark Suppose δ is a real number satisfying $0 < \delta < 1$, let $(1-(3/4)^n)^k \ge 1-\delta$, then $n \ge \log_{\frac{3}{4}}(1-\sqrt[k]{1-\delta})$. Thence, an adversary sender who obtains $\lceil \log_{\frac{3}{4}}(1-\sqrt[k]{1-\delta}) \rceil$ blind message and partial signature pairs from the signer Alice could recover the signing key $K_{\rm AC}$ with successful probability $1-\delta$ by using the proposed attack scheme. In other words, in order to guarantee the h-security of the signing key $K_{\rm AC}$, we should not reuse the same key more than $\lceil \log_{\frac{3}{4}}(1-(1-h)^{1/k}) \rceil$ times.

In conclusion, we have shown that the quantum blind signature scheme[18] does not satisfy the property of non-forgeability even under the condition that Charlie is totally creadible. In order to ensure the security of the quantum blind signature scheme,[18] it is a feasible suggestion to update the signing key $K_{\rm AC}$ regularly or simply replace $K_{\rm AC}$ with a quantum one-time pad.[22]

References

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

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

[3] Shor P W 1997 *SIAM Journal on Computing* **26** 1484

[4] Zeng G H and Keitel C H 2002 *Phys. Rev.* A **65** 042312

[5] Curty M and ütkenhaus N L 2008 *Phys. Rev.* A **77** 046301

[6] Zeng G H 2008 *Phys. Rev.* A **78** 016301

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

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

[9] Yang Y G and Wen Q Y 2008 *Sci. China Ser.* G **51** 1505

[10] Zou X F and Qiu D W 2010 *Phys. Rev.* A **82** 042325

[11] Gao F, Qin S J, Guo F Z and Wen Q Y 2011 *Phys. Rev.* A **84** 022344

[12] Yang Y G and Wen Q Y 2010 *Opt. Commun.* **283** 3198

[13] Yang Y G, Wang Y, Teng Y W, Chai H P and Wen Q Y 2010 *Commun. Theor. Phys.* **54** 84

[14] Chaum D 1983 *Advances in Cryptology-Crypto'82* (Berlin: Springer-Verlag) p. 199

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

[16] Su Q, Huang Z, Wen Q Y and Li W M 2010 *Opt. Commun.* **283** 4408

[17] Xu R, Huang L S, Yang W and He L B 2011 *Opt. Commun.* **284** 3654

[18] Wang T Y and Wen Q Y 2010 *Chin. Phys.* B **19** 060307

[19] Stadler M, Piveteau J M and Camenisch J 1995 *Advances in Cryptology-EUROCRYPT '95: International Conference on the Theory and Application of Cryptographic Techniques* Saint-Malo, May 21–25, 1995 p. 209

[20] Fan C I and Lei C L 2002 *Journal of Information Science and Engineering* **18** 47

[21] Camenisch J, Piveteau J M and Stadler M 1996 *CCS '96 Proceedings of the 3rd ACM Conference on Computer and Communications Security* New Delhi, March 14–16, 1996 p. 88

[22] Boykin P O and Roychowdhury V 2003 *Phys. Rev.* A **67** 042317