ATLANTIS PRESS

Advances in Engineering Research, volume 139

2nd International Conference on Electrical Engineering and Automation (ICEEA 2018)

Analysis of the Fair Quantum Blind Signature

Yifan Zhang

Mathematics and Applied Mathematics, Central South University, Changsha 410000, China

***Abstract*—The paper uses the uncertainty principle and no-cloning theorem; then combines the fundamental properties of quantum mechanics with the cryptographic hash function together; after that proposes a new security quantum blind signature. The analysis of security shows that the improved scheme has the feature of non-forgery, non-disavowal. Compares with other quantum signature, the new scheme needn't to update the signer's transmission private key and it can avoid the signer's private key being exposed by the sender. Moreover, the improved scheme has guiding significance value to further optimal design quantum blind signature and quantum signature, etc.**

Keywords—quantum blind signature; forge attack; quantum entangled state

I. INTRODUCTION

Digital signature is a technique for verifying the identity of the signer and ensuring the integrity of the information. Blind signature was first proposed by Chaum D in 1983[1]. In the blind signature protocol, the signer does not know the specific content of the signature message. Because the blind signature has a strong protective on the user's anonymity, it has a wide application in some electronic elections and electronic payments. For example, in the electronic payment, it is necessary for banks to sign e-cash to ensure the anonymity of consumers' personal messages and consumer contents, so blind signatures can well meet this demand. Many blind signatures are based on the difficulty of mathematical problems[2,3], but these problems are not unconditional security.

Because quantum cryptography is unconditionally secure, some scholars focus on the research of signature algorithm on quantum cryptography, and propose some quantum blind signature algorithms [4-10]. In this paper, a secure and reliable quantum blind signature scheme is proposed, which combines the basic principles of hash function and quantum mechanics to realize the security of the signature. This paper is organized as follows. In the second section, a new quantum blind signature scheme is proposed, the third section offers the proof of the new algorithm, the fourth section gives the conclusion.

II. THE NEW QUANTUM BLIND SIGNATURE

This paper proposes a new scheme with classical Vername algorithm to ensure that the signer cannot know the message. At the same time, the safety one-way hash function is combined with the basic principles of quantum mechanics, so as to ensure the safety of the system. Here H is a secure one-way hash function, which converts a binary string with indefinite length to a binary string with fixed length of n.

A. Initial Phase

The signer *Alice* and the trusted center Charlie share the key $K_{AC} \in \{0,1\}^n$ through the key distribution protocol, and the message sender U_j ,j$\in\{1,\ldots\ldots\}$ share the key K_j with the trusted center *Charlie*.

B. Blinding the Message Phase

The paper assumes the message sender U_j needs the signer Alice to sign the message M, which is a traditional binary message, and assumes its length is k.

Step B1: the message sender U_j randomly selects an integer $r \in \{0,1\}^n$ to generate an electronic fingerprint $R_B = H(K_j \| M \| r)$. Here || is the connection of two strings

Step B2: For(i=1 to k), the message sender U_j uses a Vernam-like encryption method to encrypt messages $M\{M^{(1)}, M^{(2)}, \cdots\cdots M^{(k)}\}$ with r to generate blind messages $m\{m^{(1)}, m^{(2)}, \cdots\cdots m^{(k)}\}$, with following method

$$m^{(i)} = M^{(i)} \oplus r^{(i \bmod n)} \tag{1}$$

Here $\oplus$ means that XOR operations, $m^{(i)}$ means the ith bit in the blind message, $M^{(i)}$ means the ith bit in the original message, so the formula (1) can be described as:

If the message length is less than the length of the hash function (k < n), the blind message is $m = (M^{(1)} \oplus r^{(1)}, M^{(2)} \oplus r^{(2)}, \cdots\cdots M^{(k)} \oplus r^{(k)})$

Otherwise if K≥n,

$$m = (M^{(1)} \oplus r^{(1)}, \cdots M^{(n)} \oplus r^{(n)}, M^{(n+1)} \oplus r^{(1)}, \cdots, M^{(k)} \oplus r^{(k \bmod n)})$$

Step B3: the message sender U_j sends the fingerprint $R_B = H(K_j \| M \| r)$ to the signer Alice.

C. Signing the Blind Message Phase

Step S1: the signer Alice receives the fingerprint R_B, and computes $R_A = H(K_{AC} \| R_B)$.

$|S>=\bigotimes_{i=1}^{n}|S^{(i)}>$

Step S2: Alice generates signatures with the private key K_{AC} and the electronic fingerprint R_A

$$\begin{cases}|S^{(i)}>=|0>, if\ \ K_{AC}{}^{(i)}=0\wedge R_A^{(i)}=0\\ |S^{(i)}>=|1>, if\ \ K_{AC}{}^{(i)}=0\wedge R_A^{(i)}=1\\ |S^{(i)}>=|+>, if\ \ K_{AC}{}^{(i)}=1\wedge R_A^{(i)}=0\\ |S^{(i)}>=|->, if\ \ K_{AC}{}^{(i)}=1\wedge R_A^{(i)}=1\end{cases} \quad (2)$$

Here, $R_A^{(i)}$, $K_{AC}{}^{(i)}$ represents the ith bit data in the electronic fingerprint R_A and the signer key K_{AC}, $|S^{(i)}>$ represents the ith qubit data in the quantum signature $|S>$. And $|+>=\frac{1}{\sqrt{2}}(|0>+|1>)$, $|->=\frac{1}{\sqrt{2}}(|0>-|1>)$.

Step S3: Alice sends the quantum signature $|S>$ to the message sender U_j through the quantum channel.

Step S4: the message sender U_j receives the quantum signature $|S>$, it generates the signature $|R>=\bigotimes_{i=1}^{n}|R^{(i)}>$ with the private key K_j and r ,the specific method is described as follows:

$$\begin{cases}|R^{(i)}>=|0>, if\ \ K_j{}^i=0\wedge r^i=0\\ |R^{(i)}>=|1>, if\ \ K_j{}^i=0\wedge r^i=1\\ |R^{(i)}>=|+>, if\ \ K_j{}^i=1\wedge r^i=0\\ |R^{(i)}>=|->, if\ \ K_j{}^i=1\wedge r^i=1\end{cases} \quad (3)$$

Step S5: Finally, U_j sends the final quantum blind signature ($|R>$, $|S>$) to the trusted center Charlie through the quantum channel. At the same time, the blind message M is also sent to Charlie for signature verification.

D. Verifying Phase

Step V1: Charlie first uses private key K_j to recover r' by measuring $|R>$. For(i=1 to n), if $K_j^{(i)}=0$, Charlie measured the signature $|R^{(i)}>$ by the measurement base$\{|0>,|1>\}$, if the result of the measurement is $|0>$, $r'^{(i)}=0$, else if the measurement is $|1>$, $r'^{(i)}=1$. If $K_j^{(i)}=1$, Charlie measured the signature $|R^{(i)}>$ by the measurement base$\{\{|+>,|->\}$, if the result of the measurement is $|+>$, $r'^{(i)}=0$, else if the measurement is $|->$, $r'^{(i)}=1$.

Step V2: Charlie measure $|S>$ to recover R_A' with the signer's key K_{AC} as Step V1 mentioned.

Step V3: Charlie uses the recovered parameter r' to decrypt the blind message, and recovers the original message M'. For(i=1 to k), Charlie computes

$$M^{(i)}{}'=m^{(i)}\oplus r^{(i\ \mathrm{mod}\ n)}{}' \quad (4)$$

Step V4: Charlie uses the message sender U_j's key K_j, the recovered message M' and the parameter r' to generates $R_B'=H(K_j\|M'\|r')$, then verifies the equation

$$R_A'\overset{?}{=}H(K_{AC}\|R_B') \quad (5)$$

If the equation is established, Charlie accepts the quantum blind signature ($|R>$, $|S>$) for the message M; otherwise Charlie rejects signature.

III. SECURITY ANALYSIS OF NEW ALGORITHM

A. Sender Is Unable to Perform Known Plaintext Attacks

The trusted center Charlie recovers (M',r', R_B') by measuring($|R'>$, $|S'>$). Then Charlie verifies the quantum blind signature $R_A'\overset{?}{=}H(K_{AC}\|R_B')$, and this attack method cannot be verified by this verification.

Because the signer uses K_{AC} and $H(K_{AC}\|R_B)$ to generate the signature, the key is contained in $H(K_{AC}\|R_B)$, and U_j does not have the key of the signer K_{AC}, so it cannot generate $H(K_{AC}\|R_B')$. Without $H(K_{AC}\|R_B')$, the message sender U_j cannot modify the signature $|S>$, and it cannot verified by equality $R_A\overset{?}{=}H(K_{AC}\|R_B')$.

Similarly hash function H is a security one-way function, if the message sender changed certain qubit in the signature $|S>$, to the equation $|S^i{}'>=\bigotimes_{i=1}^{n}\delta_2^{H(K_{AC}\|R_B')_j^i\oplus H(K_{AC}\|R_B)_j^i}|S^i>$, even if the message sender knows specific value of $H(K_{AC}\|R_B')_j^i\oplus H(K_{AC}\|R_B)_j^i$, he is unable to reverse the hash function according to the values R_B', which means that the receiver cannot forge the false message M'. Therefore, although the message sender U_j can change $H(K_{AC}\|R_B)\to H(K_{AC}\|R_B')$, with the hash function has the character one-way, U_j can't get the forged message M'.

Therefore, the new scheme can effectively resist the known plaintext attacks as above mentioned.

B. The Message Receiver Cannot Obtain The Signer's Key

In the Wang-Wen signature scheme[4], the signer Alice generates the quantum blind signature with K_{AC} and $H(M \| r)$, but value of $H(M \| r)$ is determined by the message sender. Therefore, by measuring the signature of $|S>$, the key of the Alice is likely to be exposed.

TABLE I. THE PROBABILITY OF MEASUREMENT RESULT

$K_{AC}^{(i)}$	R_A	$\|S^{(i)}\>$	$Me^{(i)}$ (Measurement results for $\|S^{(i)}\>$)			
			$\|0\>$	$\|1\>$	$\|+\>$	$\|-\>$
0	0	$\|0\>$	1/2	0	1/4	1/4
	1	$\|1\>$	0	1/2	1/4	1/4
1	0	$\|+\>$	1/4	1/4	1/2	0
	1	$\|-\>$	1/4	1/4	0	1/2

If the message sender knows the specific value $R_A^{(i)}$ (Assuming the average distribution of $\{0,1\}$ in $K_{AC}^{(i)}$ and $R_A^{(i)}$), When the following special cases are met, the specific value of a certain key $K_{AC}^{(i)}$ can be obtained.

$$\begin{cases} P(K_{AC}^{(i)}=0 \mid (Me^{(i)}=|->, R_A^{(i)}=0))=1 \\ P(K_{AC}^{(i)}=0 \mid (Me^{(i)}=|+>, R_A^{(i)}=1))=1 \\ P(K_{AC}^{(i)}=1 \mid (Me^{(i)}=|1>, R_A^{(i)}=0))=1 \\ P(K_{AC}^{(i)}=1 \mid (Me^{(i)}=|0>, R_A^{(i)}=1))=1 \end{cases} \quad (6)$$

As an example

$P(K_{AC}^{(i)}=0 \mid (Me^{(i)}=|->, R_A^{(i)}=0))=1$, it is proved that the equation is established.

Proof: it can be obtained from Table I:

$$P(Me^{(i)}=|->, R_A^{(i)}=0 \mid K_{AC}^{(i)}=1)$$

$$=\frac{P(Me^{(i)}=|->, K_{AC}^{(i)}=1, R_A^{(i)}{}_i=0)}{P(K_{AC}^{(i)}=1)}=\frac{0}{P(K_{AC}^{(i)}=0)}=0,$$

So $P(Me^{(i)}=|->, R_A^{(i)}=0)$

$$\begin{aligned} &= P(Me^{(i)}=|->, R_A^{(i)}=0 \mid K_{AC}^{(i)}=0)P(K_{AC}^{(i)}=0) \\ &+P(Me^{(i)}=|->, R_A^{(i)}=0 \mid K_{AC}^{(i)}=1)P(K_{AC}^{(i)}=1) \\ &= P(Me^{(i)}=|->, R_A^{(i)}=0 \mid K_{AC}^{(i)}=0)P(K_{AC}^{(i)}=0) \\ &= P(K_{AC}^{(i)}=0, Me^{(i)}=|->, R_A^{(i)}=0) \end{aligned}$$

Therefore $P(K_{AC}^{(i)}=0 \mid (Me^{(i)}=|->, R_A^{(i)}=0))$

$$=\frac{P(K_{AC}^{(i)}=0, Me^{(i)}=|->, R_A^{(i)}=0)}{P(Me^{(i)}=|->, R_A^{(i)}=0)}$$

$$=\frac{P(K_{AC}^{(i)}=0, Me^{(i)}=|->, R_A^{(i)}=0)}{P(K_{AC}^{(i)}=0, Me^{(i)}=|->, R_A^{(i)}=0)}=1$$

The other equations in equation (6) can be proven as above mentioned. It is obtained by equation (6), if the result of the ith particle $|S^{(i)}>$ measurement is $|->$ and $R_A^{(i)}=0$, then the $K_{AC}^{(i)}$ must be 0(In fact, this is also very easy to understand. Because $R_A^{(i)}=0$, according to the signature rule, $|S^{(i)}>$ must be $|0>$ or $|+>$, and the measurement result is $|->$, thus it can be obtained $|S^{(i)}>\neq|+>$, so $|S^{(i)}>$ must be $|0>$, thus obtaining $K_{AC}^{(i)}$ =0.)

In the same way, in all events, we can know that the occurrence probability of equation (6) is $1/4$. Therefore, after the K round signing the message, the message sender can obtain the signer's key K_{AC} with the probability of $(1-(3/4)^k)^n$, where n is the length of the key K_{AC} [6].

The new scheme can also prevent the signature key exposure problem [5]. Because the signer Alice generates the quantum blind signature with K_{AC} and $R_A=H(K_{AC} \| R_B)$. And without the K_{AC}, the message sender cannot generates $H(K_{AC} \| R_B)$. Without $H(K_{AC} \| R_B)$, the message sender cannot know the value of $R_A^{(i)}$, even it measures the signature $|S>$. Therefore, the message sender cannot know the signature key K_{AC}. Assuming that $\{0,1\}$ is evenly distributed in $K_{AC}^{(i)}$ and $R_A^{(i)}$, it can be obtained

C. Unforgeability

From the 3.1 section, it can know that the new scheme can prevent message sender from making known plaintext attacks. From the 3.2 section, we know that the sender cannot get the key of the signer, without the signature key K_{AC}, the message sender cannot generate the signature $|S>$ directly. Assuming

that it generates a forged blind signature $(|R'>,|S'>)$, the trusted center Charlie can find this kind of attack. Charlie obtains r' by measuring $|R'>$, and then obtains R_A' by measuring $|S'>$, but it is not feasible to make the equation $R_A' = H(K_{AC} \| H(K_j \| m \oplus r' \| r'))$ to be established. Charlie will reject the signature, so the message sender cannot make a forgery attack.

Similarly, without the signer's key K_{AC} and the message sender's key K_j, even if other attackers Eve have intercepted blind signatures ($|R>$, $|S>$), it can't forge attacks. Because if it modifies ($|R'>$, $|S'>$) and blind message m', it cannot be verified by equation $R_A' \stackrel{?}{=} H(K_{AC} \| R_B')$. Therefore, other attackers cannot make a forgery attack.

D. Non-Repudiation

If the signature is set up, Charlie can be sure that the signer Alice has signed the blind message m. Because at the signing phase, the signature key of the Alice K_{AC} is contained in the R_A ($R_A = H(K_{AC} \| R_B)$ .If Alice signs the message correctly, the trusted center Charlie is able to verify the validity of the signature by verifying the equation $R_A' \stackrel{?}{=} H(K_{AC} \| R_B')$. At the same time, in the new scheme, the message sender cannot make a forgery attack, so if Charlie verifies that the signature is correct, the signer Alice cannot deny that the blind message M has been signed.

In the same way, Charlie can also be sure that the message sender is blind to the message and produces electronic fingerprints $R_B = H(K_j \| M \| r)$ .Since the effective blind signature for message M is $(|R>,|S>)$, the message sender generates $|R>$, the key K_j is included in the $|R>$, and the K_j is also included in the R_B .If U_j generates $|R>$ correctly, the trusted center restores the original message M, the signature parameter r' .Then the trusted center compares the equation $R_A' = H(K_{AC} \| H(K_j \| M \| r'))$, it can determine that U_j had blinded the message and produced the electronic fingerprint $R_B = H(K_j \| M \| r)$. So if the signature is set up, the message sender U_j is also undeniable.

E. Message Blindness

The Wang-Wen scheme is a weak blind signature. In this scheme, the signer first signs the blind message, after that transmits the signature to the message sender. Then the message sender sends the signature and the original message to the trusted center Charlie to verify the signature. Although the signer signs the blind signature firstly, b But the sender did not encrypt the original message M to the trusted center. So there is still a loophole for the signer to know the original message M:

(1) After receiving the message sender's electronic fingerprint R_j, the signer generates an illegal signature $|S'>$ and transmits the illegal signature $|S'>$ to the sender.

(2) When the sender sends the quantum blind signature($|R>$, $|S'>$) and the original message M to the trusted center, the signer Alice intercepts the M , so that the content of the original message M can be obtained.

Because $|S'>$ is an illegal signature, the trusted center judges the signature is illegal. As long as the trusted center let the sender resign the message, so the signer can know the content of the original message M

In the new scheme, even if the signer interceptes the blind message M, the signer Alice could not get the original message M. Suppose the message length is k, and the length of the message sender's parameter r is n.

If k<=n, the blinded message is $m = (M^{(1)} \oplus r^{(1)}, M^{(2)} \oplus r^{(2)}, \cdots\cdots M^{(k)} \oplus r^{(k)})$ .The encryption method is the traditional Vernam method, and the Vernam encryption methods can be proved to be unconditionally secure. Without parameter r, even if the signer intercepted the encrypted message m, it cannot recover the original M.

If k>n, the encryption method is similar to the Vernam encryption method, when the signer intercepts the encrypted message m, it can be obtained

$$\begin{cases} m^{(i)} = M^{(i)} \oplus r^{(i)} \\ m^{(i+n)} = M^{(i+n)} \oplus r^{(i)} \end{cases} \Rightarrow m^{(i)} \oplus m^{(i+n)} = M^{(i)} \oplus M^{(i+n)} \quad (7)$$

From the equation (8) , we can only know whether the ith original message $M^{(i)}$ is equal to the (i+n)th original message $M^{(i+n)}$. If $m^{(i)} \oplus m^{(i+n)} = 0$, because the signer cannot know the distribution situation of $\{0,1\}$ in the original message M, and the signer only knows $M^{(i)} = M^{(i+n)}$, but the signer doesn't know $M^{(i)} = 1$ or $M^{(i)} = 0$; otherwise, if $m^{(i)} \oplus m^{(i+n)} = 1$, it means $M^{(i)} \neq M^{(i+n)}$, and the signer cannot know $M^{(i)} = 1$ or $M^{(i)} = 0$. So to the signer Alice, even if it interceptes the encrypted message m, it cannot know the original message M.

F. Traceability

When the signature is established, once there are some disputes between the signers and the message sender, the signer can be able to track the identity of the sender with the help of the trusted center. The signer sends the message sender $U_j's$ electronic fingerprint R_B to the trusted center Charlie.

According to the parameter $(K_{AC}, K_j, |R>, |S>, R_B)$, trusted center Charlie can restore the signature parameter r'and the original message M' by measuring $|R>$, and then identify the message sender's identity by comparing $R_B = H(K_j \| M' \| r')$.

IV. CONCLUSIONS

In this paper, a new quantum blind signature algorithm based on the hash function of cryptography is proposed. Compared with the other algorithm, the new algorithm does not use quantum entangled state, and its signature length is fixed, so it can be applied to long messages, and more effective to implement. At the same time, after each signature, the key of the new scheme can be reused, thus reducing the shortcomings of the key redistribution. Compared with [5], the new scheme can also ensure that the signer's key will not be found by the message sender, and the message sender cannot carry out the known plaintext attack. Through the security analysis, the new scheme has the characteristics of unforgeability, non repudiation, traceability and so on.

REFERENCES

[1] Chaum D.Blind signatures for untraceable payments[C]. Advances in Cryptology-Crypto, 1982:199-205.

[2] Verma, GK , Singh, BB. Efficient message recovery proxy blind signature scheme from pairings [J]. Efficient message recovery proxy blind signature scheme from pairings.2017,28(11).

[3] Zhu, HF ,Tan, YA, Zhang, XS, Zhu, LH . A round-optimal lattice-based blind signature scheme for cloud services [J]. FUTURE GENERATION COMPUTER SYSTEMS-THE INTERNATIONAL JOURNAL OF ESCIENCE.2017,73: 106-114.

[4] Wen Xiaojun, Niu Xiamu, Ji Liping. A weak blind signature scheme based on quantum cryptography [J], Optics Communications, 2009, 282(4): 666-669.

[5] Wang Tian-Yin, Wen Qiao-Yan. Fair quantum blind signatures [J]. Chinese Physics B, 2010, 19(6): 66-70.

[6] He Li-Bao,Huang Liu-Sheng,Yang Wei, Xu Ru. Cryptanalysis of fair quantum blind signature[J]. Chinese Physics B, 2012, 21(3): 63-66.

[7] Xu Rui, Huang Liusheng, Yang Wei. Quantum group blind signature scheme without entanglement [J]. Optics Communications, 2011, 284(14): 3654-3658.

[8] Li W, Shi JJ , , Guo Y. Blind Quantum Signature with Controlled Four-Particle Cluster States [J]. INTERNATIONAL JOURNAL OF THEORETICAL PHYSICS.2017,56(8): 2579-2587.

[9] Yang YY, Xie SC, Zhang JZ . An Improved Quantum Proxy Blind Signature Scheme Based on Genuine Seven-Qubit Entangled State[J]. INTERNATIONAL JOURNAL OF THEORETICAL PHYSICS. 2017,56(7): 2293-2302.

[10] Zhang Ming-Hui,Li Hui-Fang. Fault-tolerant quantum blind signature protocols against collective noise [J]. QUANTUM INFORMATION PROCESSING.2016,15(10): 4283-4301.