Improved on Identity-based quantum signature based on Bell states

Chang-Bin Wang[1],Shu-Mei Hsu[2],Hsiang Chang[3],Jue-Sam Chou[4*]
[1]Department of Information Management, Nanhua University, Taiwan
cbwang@mail.nhu.edu.tw
[2]Department of Mathematics and Physics Education, Chiayi University, Taiwan
10769553@nhu.edu.tw
[3]Department of Information Management, Nanhua University, Taiwan
10769511@nhu.edu.tw
[4]Department of Information Management, Nanhua University, Taiwan *: corresponding
author: jschou@nhu.edu.tw Tel: 886+ (05)+272-1001 ext.56536

Abstract

In 2020 Xin et al.proposed a new identity-based quantum signature based on Bell states scheme. By using a one-time padding (OTP) for both-side transfer operations like, "XOR", Hadamard H, and Y, they confirmed the security of the proposed scheme. However, after analyses, we found that the scheme cannot resist both the existing forgery attack and meaningful message attack. Therefore, we modified their scheme to include the required security, unforgeability, which is very important in quantum signature scheme.

Keywords:quantum signature, Identity-based signature, Hadamard gate, unforgeability, quantum state

1. Introduction

Signature scheme is a fundamental tool in the information security applied to the Internet in human daily life, such as, e-government, e-bank, e-commerce, etc. For coping with the upcoming quantum era, several quantum signature related articles have been proposed. There are two categories algorithms between them, i.e. the arbitrated algorithms [1, 2-18], where the verification is executed by a trusted third party, and the true signature schemes [3, 19], in which the verification can be executed by anybody. In 2020 Xin et al. proposed a new identity-based quantum signature based on Bell states scheme [1]. They claimed that their scheme is more secure, practical, and efficient than the similar public-key quantum signature schemes. However, upon closer examination, we discovered that it does not support the security requirement of preventing signature forgery attack. We will demonstrate this in the article. To enhance its security, we will modify their scheme to include this feature. In addition, we also describe the enhancement in this content.

The article is arranged as follows. In Section 2, we briefly introduce Xin et al.'s scheme. In Section 3, we analyze the weaknesses of the scheme. The modifications and the security issues are demonstrated and discussed in Section 4 and 5, respectively. Finally, a conclusion is given in Section 6.

2. Review of Xin et al.'s scheme

In 2020 Xin et al.proposed a new identity-based quantum signature based on Bell states scheme. It consists of three roles: the signer, the verifier, and a trusted PKG; and four phases: initializing phase, key generation phase, signing phase and verification phase. They claimed that their scheme is more secure, practical, and efficient than the similar public-key quantum signature schemes. In this article, we only review the key generation phase, the signing phase, and verification phase to illustrate its weaknesses. As for the definitions of the used notations, please refer to

the original article. We omit them here.

2.1 Key generation phase

In this phase, signer Alice sets her public key and obtains the private key from PKG, the phase is performed as follows:

(1) Alice chooses her identity $ID = (ID_1, ID_2, \dots, ID_n) \in \{0,1\}^n$ as her public key.

(2) PKG uses his master key G to calculate k= G (ID) to generate Alice's private key, where G: $\{0,1\}^* \rightarrow \{0,1\}^{2n}$ is an one-way function with uniform distribution.

(3) PKG transports Alice's private key by performing quantum key distribution protocol.

(a) Alice and PKG share a secret random 2n-bit string *x*.

(b) PKG calculates OTP ciphertext $x' = x \oplus k$, and publicly announces x'.

(c) Alice calculates her own private key $k = x \oplus x'$ according to the shared random x and OTP ciphertext x'.
(Alice's private key $k = (k_1, k_2, \dots, k_n, k_{n+1}, \dots, k_{2n}) \in \{0,1\}^{2n}$)

2.2 Signing phase

Signer Alice uses her private key k to generate signatures and encode messages, this phase is performed as follows:

(1)Alice encodes the message m as a Bell state sequence $|a\rangle = \bigotimes_{i=1}^{n} |a_i\rangle$ according to the following rules:

$$m_i = 00 \rightarrow |a_i\rangle = |\varphi^+\rangle, \qquad m_i = 01 \rightarrow |a_i\rangle = |\varphi^-\rangle,$$
$$m_i = 10 \rightarrow |a_i\rangle = |\psi^-\rangle, \qquad m_i = 11 \rightarrow |a_i\rangle = |\psi^+\rangle,$$

where $|a_i\rangle$ is the i-th Bell state of the sequence $|a\rangle$.

(2)Alice selects a random $2n$ -bit string $r = (r_1, r_2, \dots, r_n, r_{n+1}, \dots, r_{2n})$ and computes

$$h = T_1(m \oplus k \oplus r), \qquad e = T_2(m \oplus k \oplus r),$$
$$l = T_3(m \oplus k \oplus r), \qquad u = T_4(m \oplus k \oplus r),$$

where the four Ts:$\{0,1\}^{2n} \rightarrow \{0,1\}^n$are four public one-way functions, each with uniform distribution.

Then, Alice uses *h, e, l, u* and $m_i = (m_{i1}, m_{i2})$ to calculate

$$w_i = m_{i1} \oplus r_i \oplus ID_i \oplus h_i, \qquad v_i = m_{i1} \oplus r_i \oplus ID_i \oplus e_i$$
$$g_i = m_{i2} \oplus r_{n+i} \oplus ID_i \oplus l_i, \qquad q_i = m_{i2} \oplus r_{n+i} \oplus ID_i \oplus u_i$$

(3)Alice performs the operation on the message state $|a_i\rangle$ and gets $|s_i\rangle$.
$|s_i\rangle = (H^{v_i} Y^{w_i}) \otimes (H^{g_i} Y^{q_i}) |a_i\rangle$.
The quantum signature for *me is* $|s\rangle := \bigotimes_{i=1}^{n} |s_i\rangle$

(4)Alice randomly inserts the decoy particles which are selected from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ into the sequence $|s\rangle$ and gets the corresponding photon sequence $|s'\rangle$ for checking eavesdropping. Finally, Alice sends the sequences $\{|s'\rangle, m, ID\}$ to Bob.

(5)Bob uses the corresponding basis to measure decoy particles according to the positions and bases announced by Alice, and compares the measurement outcome with Alice's announced states.

(6)After excluding eavesdropping, Bob recovers the quantum sequence $|s\rangle$ from $|s'\rangle$. and stores $\{|s\rangle, m, ID\}$ as Alice's quantum signature.

2.3 Verifying phase

After receiving Alice's quantum signature, Bob and PKG perform the following steps to verifying it:

(1)According to random pad t shared in advance, Alice calculates the OTP ciphertext $r' = r \oplus t$, and then publicly announces r'.

(2) According to shared random t and the OTP ciphertext r' announced by Alice, Bob calculates $r' = r \oplus t$. After that, according to m, ID, and r, Bob calculates $c_i = m_{i1} \oplus r_i \oplus ID_i$, $d_i = m_{i2} \oplus r_{n+i} \oplus ID_i$ $i = 1, 2, \dots, n$

Then, Bob performs the Hadamard operations on the message state $|s_i\rangle$, getting $|b_i\rangle$, where $|b_i\rangle = (H^{c_i}) \otimes (H^{d_i}) |s_i\rangle$ and $|b\rangle := \otimes_{i=1}^{n} |b_i\rangle$.

(3) Bob publicly announces m, r, ID, and sends the quantum sequence $|b\rangle$ to PKG.

(4) According to the m, r and ID publicly announced by Bob, PKG computes h, e, l and u. Then, he calculates w_i, q_i, and performs the operations $\left((Y^+)^{wi} H^{e_i} \otimes (Y^+)^{qi} H^{l_i}\right) on\ |b_i\rangle$, obtaining $|a_i\rangle$.

(5) PKG measures each $|a_i\rangle$ with the Bell base $\{|\varphi^+\rangle, |\varphi^-\rangle, |\psi^-\rangle, |\psi^+\rangle\}$, then decodes the quantum state $|a_i\rangle$ as the message m'_i by the following rules:

$$|a_i\rangle = |\varphi^+\rangle :\rightarrow m_i' = 00, \qquad |a_i\rangle = |\varphi^-\rangle :\rightarrow m_i' = 01,$$
$$|a_i\rangle = |\psi^-\rangle :\rightarrow m_i' = 10, \qquad |a_i\rangle = |\psi^+\rangle :\rightarrow m_i' = 11.$$

(6) According to *m,* which is publicly announced by Bob, PKG compares m' with m. If $m' = m$ holds, PKG publicly announces "Yes" and Bob accepts $\{|s\rangle, m, ID\}$ as Alice's valid quantum signature.

3. Weakness of the scheme

Form step (3) of the verification phase, we can see that an attacker Eve can collect Bob's publicly announced messages m, r, ID, and perform the intercept and resend attack on the quantum sequence |b⟩, which B sends to PKG. Through the collected messages, Eve can launch both: (1) existential forgery, and (2) meaningful message attacks. We describe them below.

(1) Existential forgery attack

In this attack, Bob wants to forge a message m_e together with its corresponding $|b_i'\rangle$, such that when PKG performs the reverse Pauli operations on $|b_i'\rangle$, and then decodes the result to obtain its message, he cannot detect anything wrong. We describe this attack as follows.

When Bob sends out m, r, $|b_i\rangle = (H^{c_i} m_{i1}) \otimes (H^{d_i} m_{i2})$. Eve performs the Pauli matrix operation X on the wanted photon $(H^{c_i} m_{i1})$ or $(H^{d_i} m_{i2})$, according to which photon he wants to change to be in accordance with the modified bit in m. For example, if Eve operates on the left photon as follows:

Left: $|b_i'\rangle = X(H^{c_i}) \otimes (H^{d_i}) |s_i\rangle$, then Eve must flip the first bit of $m_i = 00$, getting m_e=10

Conversely, if he operates on the right as follows:

Right: $|b_i'\rangle = (H^{c_i}) \otimes X(H^{d_i}) |s_i\rangle$, then he must flip the second bit of m_i=00 $\rightarrow m_e$=01

Accordingly, Eve can change the message m to m_e by performing Pauli operation X on the corresponding photon of $|b_i\rangle$, obtaining $|b_i'\rangle$. Then, $\{m_e, |b_i'\rangle\}$ can be verified as valid by PKG. Thus, Eve succeeds in constructing such an existential forgery.

(2) Meaningful message attack

Eve first chooses a meaningful message m_m, then, according to $m \oplus r$, she finds the relevant r_m to launch such an attack, so that $m_m \oplus r_m = m \oplus r$. Secondly, according to the difference $Diff (= m \oplus m_m)$, Eve computes the relevant $r_m = Diff \oplus r$. Also, she performs X operations on the homologous photons according to the $Diff$. For example: if $m = 010111$ and $m_m = 110101$, she will do the operation X on the first and the fifth photons.

4. Modification

Due to the forgery attack their scheme suffers, in this section, we propose two types of improvements: (1) HMAC, and (2) decoy photons, on their scheme as follows.

(1) HMAC

Since A and PKG had pre-shared a session key K, this incurs that we can use the HMAC to make their scheme better. For example: When A sends out the sequences $\{|s'\rangle, m, ID\}$ to Bob, she also sends out the $HMAC = H(k, m)$. If concerning about its computational security in the upcoming quantum era, one can adopt an unconditional hash function [2]. Thus, if m is modified in the way from Bob to PKG, PKG can detect Eve's illegal behavior by computing and compare the $HMAC$.

(2) Decoy photons

Like the steps 4 through 6 done by Alice in the signing phase, when Bob sends out the quantum sequence $|b\rangle$ to PKG in step (3) of Section 2.3, Bob can add decoy photons into the quantum sequence $|b\rangle$, which is sent out to PKG, for checking Eve's illegal action to prevent such attack.

5. Security analysis

After the above modification, we can see that due to the one-way hash function property, from the $HMAC$ the attacker cannot obtain Alice's secret k. Thus, cannot calculate the value of $H(k, m)$, which means that the message m cannot be changed. Hence, the forged message attack fails. Meanwhile, we can also add decoy photons to the quantum sequence transmitted by Bob to PKG, like the one done by Alice to Bob. By this way, PKG can detect whether or not there exists an attacker. That means if Eve launches the forgery attack on the quantum sequence $|bi\rangle$ sent by Bob to PKG, he will be discovered. Therefore, both attacks on the original scheme have been thrawted away. Even if concerning about the computational security of the hash function in the upcoming quantum era, we can use the unconditional secure hash, as mentioned in the context of [2].

6. Conclusion

In this paper, we showed that Xin et al.'s identity-based quantum signature based on Bell states scheme has weaknesses. It suffers from Pauli matrix X operation attack. We, therefore, modified it to avoid this hole. From the analyses shown in section 5, we confirm that we have promoted its security.

7. **References**

[1]Xin, Xiangjun, Zhuo Wang, and Qinglan Yang. "Identity-based quantum signature based on Bell states." Optik 200 (2020): 163388.

[2]Zeng, Guihua. Quantum private communication. Springer Publishing Company, Incorporated, 2010.

[3]Zeng, Guihua, et al. "Continuous variable quantum signature algorithm." International Journal of Quantum Information 5.04 (2007): 553-573.

[4]A. Kaushik, A.K. Das, D. Jena, “A novel approach for simple quantum digital signature based on asymmetric quantum cryptography.”Int. J. Appl. Innov.Eng. Manage.（IJAIEM）6（June（6））（2013）

[5]Shi, W. M., Wang, Y. M., Zhou, Y. H., & Yang, Y. G.（2018）. Cryptanalysis on quantum digital signature based on asymmetric quantum cryptography. Optik-International Journal for Light and Electron Optics, 154, 258-260.

[6]Shi, Wei-Min, et al. "A non-interactive quantum deniable authentication protocol based on asymmetric quantum cryptography." Optik-International Journal for Light and Electron Optics 127.20（2016）: 8693-8697.

[7]Shi, Wei-Min, et al. "A restricted quantum deniable authentication protocol applied in electronic voting system." Optik-International Journal for Light and Electron Optics 142（2017）: 9-12.

[8]Shi, Wei-Min, et al. "A scheme on converting quantum signature with public verifiability into quantum designated verifier signature." Optik 164（2018）: 753-759.

[9]Wen, Xiaojun, et al. "A weak blind signature scheme based on quantum cryptography."Optics Communications282.4（2009）: 666-669.

[10]Yang, Yu-Guang, and Qiao-Yan Wen. "Arbitrated quantum signature of classical messages against collective amplitude damping noise."Optics Communications 283.16（2010）: 3198-3201.

[11]Lee, Hwayean, et al. "Arbitrated quantum signature scheme with message recovery."Physics Letters A 321.5-6（2004）: 295-300.

[12]Wang, Jian, et al. "Comment on: “Arbitrated quantum signature scheme with message recovery”[Phys. Lett. A 321（2004） 295]." Physics Letters A 347.4-6（2005）: 262-263.

[13]Luo, Yi-Ping, and Tzonelih Hwang. "Erratum “New arbitrated quantum signature of classical messages against collective amplitude damping noise”[Optics Communications 284（2011） 3144]." Optics Communications 303（2013）: 73.

[14]Yang, Yu-Guang, and Qiao-Yan Wen. "Erratum: Arbitrated quantum signature of classical messages against collective amplitude damping noise（Opt. Commun. 283（2010） 3198–3201）." Optics Communications 283.19（2010）: 3830.

[15]Hwang, Tzonelih, et al. "New arbitrated quantum signature of classical messages against collective amplitude damping noise." Optics communications 284.12（2011）: 3144-3148.

[16]Chong, Song-Kong, Yi-Ping Luo, and Tzonelih Hwang. "On “arbitrated quantum signature of classical messages against collective amplitude damping noise”." Optics Communications284.3（2011）: 893-895.

[17]Qi, Su, et al. "Quantum blind signature based on two-state vector formalism." Optics Communications 283.21（2010）: 4408-4410.

[18]Qiu, Lirong, Feng Cai, and Guixian Xu. "Quantum digital signature for the access

control of sensitive data in the big data era." Future Generation Computer Systems（2018）
[19]Chen, Yalin, et al. "A publicly verifiable quantum signature scheme based on asymmetric quantum cryptography." IACR Cryptology ePrint Archive 2019 (2019): 24.