A publicly verifiable quantum signature scheme based on asymmetric quantum cryptography

Yalin Chen[1] and Jue-Sam Chou[*2] and Fang-Qi Zhou[3]

[1]Institute of information systems and applications, National Tsing Hua University
Yalin78900@gmail.com

[2] Department of Information Management, Nanhua University, Taiwan *: corresponding author: jschou@nhu.edu.tw Tel: 886+ (0)5+272-1001 ext.56536

[3] Department of Information Management, Nanhua University, Taiwan
zz66016@gmail.com

Abstract

In 2018, Shi et al.′s showed that Kaushik et al.′s quantum signature scheme is defective. It suffers from the forgery attack. They further proposed an improvement, trying to avoid the attack. However, after examining we found their improved quantum signature is deniable, because the verifier can impersonate the signer to sign a message. After that, when a dispute occurs, he can argue that the signature was not signed by him. It was from the signer. To overcome the drawback, in this paper, we raise an improvement to make it publicly verifiable and hence more suitable to be applied in real life. After cryptanalysis, we confirm that our improvement not only resist the forgery attack but also is undeniable.

Keywords：Undeniable quantum signature scheme, Impersonation attack, Quantum asymmetric cryptography, Trapdoor one-way function, Single-qubit rotations encryption, Publicly verifiable signature

1. Introduction

There are many cryptographic scientists doing research in the field of secure digital signatures, ranging from general signature schemes [1-7], proxy signature schemes [8-35] to its variants such as, deniable authentication with a designated verifier [36-51] and k-out-of-n oblivious transfer protocol [52-80]. All of these methods are primarily intended to allow the signer to sign a message that can be verified by a public or designated verifier. In recent years, due to the development of science and technology (especially the advancement of physical materials and secure communication networks), combined with the application of quantum mechanics, the research of quantum cryptography has flourished [81-94].

In 2013, Kaushik et al. [80] proposed a simple quantum signature method based on asymmetric quantum cryptography. They claimed that their protocol can meet the security requirements of a signature scheme. However, in 2018, Shi et al. [81] discovered their scheme suffer form the forgery attack. Then, they further proposed an improvement on it and declared that their improved method is safe.

Yet, in this paper, we study their improved protocol and detect that it does not possess the non-repudiation property (the signer cannot deny he had signed the message before), because the signer and the verifier shared a common secret θ_{n1}. This leads to the denial problem for that the original signer Alice can deny her signed message and declare the signature is form Bob, due to the fact that Bob also can use her public key $|\varphi_{pk}\rangle_{Alice} = \otimes_{j=1}^{N} R^{(j)} (S_j\theta_n) |0_z\rangle$, together with their common secret θ_{n1} to perform a rotation operation $\otimes_{j=1}^{N} R^{(j)}(h_j\theta_{n1})$ on $|\varphi_{pk}\rangle_{Alice}$ to obtain the same signature as hers. That is, Alice can claim that Bob is able to use this method to generate the same signature, but indeed the signature is actually from herself. In other words, in the improvement of Kaushik et al.′s, the signer Alice can deny the facet that she had signed it before. This violates the security requirements of a signature scheme, because according to [35], any signature must satisfy four security attributes: (1)

unforgeability, (2) verifiability, (3) non-repudiation, and (4) identifiability. In this article, we will first show that Kaushik et al.'s improved method not only make the signer Alice be able to deny the signature he signed, but also let the verifier Bob has the ability to forge a signature while state that it is form Alice, if Bob is malicious. After that, we propose an undeniable quantum signature scheme, which can meet the above four security requirements and is publicly verifiable to be more consistent with human reasoning in concept.

The rest of this article will show up as follows. In Section 2, we introduce Kasumk et al.'s quantum signature scheme, and both Shi et al.'s attack and improvement. In Section 3 we propose a publicly verifiable quantum signature scheme based on asymmetric quantum cryptograph, Then, its security analyses are shown in Section 4. After that, we compare our scheme with the state of the art in Session 5. Section 6 gives the future work, and finally, a conclusion is given in Section 7.

2. Review Kasumk et al.'s Quantum Signature Scheme and Shi et al.'s Attack and Improvement

In this section, we first review Kaushik et al. 's quantum signature scheme in section 2.1, then describe Shi et al.'s attack and improvement in section 2.2.

2.1. Kaushik et al. quantum signature scheme

Their signature scheme is divided into three phases: (1) the key generation phase, (2) the signature phase, and (3) the verification phase. We describe them separately below:

(1) Key generation phase

At this stage, the cryptosystem generates a public/private key pair for each user in the system (now taking Alice as an example) by using the following steps.

(a) Produces A's private key d = (n, s) by selecting a random number n>>1 and a random string s = (s_1, s_2, ..., s_N) of length N, where s_j is selected from Z_{2n}.

(b) Prepares the N-qubits state $|0_z>^{\otimes N}$.

(c) Applies the rotation operation $R^{(j)}(S_j\theta_n)$ on the quantum state $|0_z>^{\otimes N}$, j=1 to N, to generate the public key of A, $|\varphi_{pk}>_A = \otimes_{j=1}^{N} R^{(j)}(S_j\theta_n)|0_z>$, where $\theta_n = \pi/2^{n-1}$.

(2) **Signature stage**

A signs on a n-bit traditional message M by using the following steps.

(a) Calculates *h=H (M),* where H represents a one-way hash function with an output length of N bits.

(b) Performs a rotation operation $R^{(j)}(h_j\pi)$ on state $|0_z>^{\otimes N}$, getting $|\varphi_{hj}>_{\mathrm{A}} = \otimes_{j=1}^{N} R^{(j)}(h_j\pi)|0_z>$

(c) Uses her private key $S_j\theta_n$ to perform a rotation operation $R^{(j)}(S_j\theta_n)$ on $|\varphi_{hj}>$, obtaining the signature $|\varphi_{hj,sj}^{s}(\theta_n)>_{\mathrm{A}} = \otimes_{j=1}^{N} R^{(j)}(S_j\theta_n)\ |\varphi_{hj}>$ of M, and then sends message M and the signature, $\{M,\ |\varphi_{hj,sj}^{s}(\theta_n)>_{\mathrm{A}}\}$, to Bob (B) .

(3) **Verification phase**

Upon receiving $\{\ M,\ |\varphi_{hj,sj}^{s}(\theta_n)>_{\mathrm{A}}\}$, B performs verification by using the following steps.

(a) Calculates *h* = *H (M).*

(b) Performs reverse rotation operation $\otimes_{j=1}^{N} R^{(j)}(-h_j\pi)$ on $|\varphi_{hj,sj}^{s}(\theta_n)>_{\mathrm{A}}$, getting $|\varphi_{pk}>' = \otimes_{j=1}^{N} R^{(j)}(-h_j\pi)\ |\varphi_{hj,sj}^{s}(\theta_n)>_{\mathrm{A}}$.

(c) Measure the quantum state $|\varphi_{pk}>'_{\mathrm{A}}$ to see if the outcome is equal to Alice′s public key $|\varphi_{pk}>_{\mathrm{A}}$, if the equation holds, B accepts it; otherwise, rejects.

2.2. Shi et al.'s attack and improvement

After analyzing Kaushik et al.'s [80] signature scheme, Shi et al.'s [81] discovered that if an attacker E launches a forgery attack, then the scheme fails. Thus, they proposed an improvement on it. In the following, we first describe the behavior of E in [81], then show the improvement on the scheme.

(1) E's forgery attack

(a) Calculates $h = H(M)$ and pretends to be the role of A to perform the inverse operation $R^{(j)}(-h_j\pi)$ on $|\varphi^{s}_{hj,sj}(\theta_n)>_{\mathrm{A}}$, obtaining $|\varphi_{pk}>'_{\mathrm{A}}$.

(b) Chooses another message M' = {m_1', m_2',……,$\mathrm{m}_{\mathrm{N}1}$'} of length N_N, calculates $h'=H(M')$, and forges a signature $|\varphi^{s'}_{hj',sj}(\theta_n)>_{\mathrm{A}} =\otimes^{N}_{j=1}R^{(j)}(h_j'\pi)\ |\varphi_{pk}>'$.

(c) Sends the message signature pair$\{M', |\varphi^{s'}_{hj',sj}(\theta_n)>_{\mathrm{A}}\}$ to B for verification, it is obvious that the signature pair can be successfully verified by B who thinks that the signature is from A.

(2) Shi et al.'s improvement

To avoid E's forgery attack, Shi et al.'s let the signer A and the verifier B share a random integer $\mathrm{n}_1 >> 1$ in advance. Then, A and B together perform the signature and verification process as follows.

(a) A's signing

A uses a rotation operation $R^{(j)}(h_j\theta_{n1})$, instead of $R^{(j)}(h_j\pi)$, to operate on the quantum state $|0_z>^{\otimes\mathrm{N}}$, where $\theta_{n1}=\pi/2^{n1-1}$, giving the result $|\varphi_{hj}>=\otimes^{N}_{j=1}R^{(j)}(h_j\theta_{n1})|0_z>$. The rest of the signature process is the same as in the original one (see section 2.1).

(b) B's verification

After receiving the message signature pair from A, B performs an inverse rotation operation $R^{(j)}(-h_j\theta_{n1})$ on $|\varphi^{s}_{hj,sj}(\theta_n)>_{\text{A}}$, instead of $R^{(j)}(-h_j\pi)$, measures and compares to see whether the two quantum states $|\varphi_{pk}'>_{\text{A}}$ $(=\otimes_{j=1}^{N}R^{(j)}(-h_j\theta_{n1})|\varphi^{s}_{hj,sj}(\theta_n)>_{\text{A}})$ and $|\varphi_{pk}>_A$ are equal. If the equation holds, B accepts; otherwise, rejects.

Undoubtedly, in B's verification, the equation will hold. Under this situation E cannot successfully launch a forgery attack, because he does not know the common secret θ_{n1} shared between A and B. Therefore, Shi et al.'s claimed that their improvement succeeds in satisfying the feature set of a signature scheme. Yet, we unearth that the improvement has several drawbacks still. Thus, we further improve it by proposing a new one. We will describe them in the following section 3.

3. The shortcomings in Shi et al.'s improvement and the proposed quantum signature scheme

In this section, we describe the shortcomings of Shi et al.'s improvement in section 3.1, then propose a new one in section 3.2.

3.1 The drawbacks of Shi et al.'s improvement

According to the improvement proposed by Shi et al.'s in section 2.2 (b), we notice that it is not a good idea for the signer and the verifier to share the secret key in advance during the signing process. It will lead the signer to deny her signed message. Moreover, for the reason that the quantum signature scheme in the current literature needs to specify a verifier, which may be too rigorous in concept and not be general enough to be applicable in real life. Based on the above two observations, in this study we attempt to design a new quantum signature scheme, without necessity to designate a specific verifier and thus is more consistent with human logic reasoning. Furthermore, it has the non-repudiation characteristic and thus more practical. We adopt the same key generation phase as Kaushik et al.'s quantum signature by assuming that each user has their own public/private key pair $(|\varphi_{pk}>/\ S_j\theta_n)$, and then present the signature phase and the verification phase as follows. The steps are also shown in Fig. 1. Fig. 2 is the schematic view of the corresponding rotation angles implied in Fig. 1.

3.2 The proposed quantum signature scheme

In this section, we present our scheme in the following.

(1) Signature phase

Alice (A) uses the following steps to sign on the traditional message M.

(a) Selects a random number r and calculates

$h=H(M, r\theta_n)$,

$R=H(rH(r), M)r\theta_n$,

$h=H(M, R)$,

$X_j=rS_j$,

$hrx=H(r, h, X, r\theta_n)$,

$Y_j=r^2S_j\theta_nh_j+S_jhr_j+S_j\theta_n=X_jr\theta_nh_j+S_jhrx_j+S_j\theta_n$,

$hr=H(M, hrx, h, Y)$,

$W_j=X_jr\theta_nh_j+S_jhrx_j+2S_j\theta_n$, where H represents a one-way hash function.

(b) Performs a rotation operation $R^{(j)}(W_j)$ on $|0_z>^{\otimes N}$, where j = 1 to N, obtaining $|Sig>_A=\otimes_{j=1}^{N}R^{(j)}(W_j)|0_z>$, and sends $\{M, r\theta_n, R, X, Y, hr, hrx, |Sig>_A\}$ to Bob (B).

(2) Verification phase

After receiving $\{M, r\theta_n, R, X, Y, hr, hrx, |Sig>_A\}$, B performs the following steps to verify it.

(a) Calculates $h'=H(M, R)$

(b) Calculates and compares to see if $hr_j'(=H(M, hrx_j, h, Y_j))=hr_j$, if the equation doesn't hold, abort.

(c) Applies $R^{(j)}(-Y_j)$ on $|Sig>_A$ to perform a reverse rotation operation to get quantum state $|Z>$,

(d) Measures and compares to see if the two quantum states $|Z>$ and $|\varphi_{pk}>_A$ are equal, if they are equal, Bob accepts; otherwise, rejects.

Alice	Bob
Signature Randomly choose an integer r Computes $R=H(rH(r), M)r\theta_n$ $h=H(M, R)$ $X_j=rS_j$ $hrx=H(r, h, X, r\theta_n)$ $Y_j=r^2S_j\theta_n h_j+S_j hrx_j+S_j\theta_n=X_j r\theta_n h_j+S_j hrx_j+S_j\theta_n$ $hr=H(M, hrx, h, Y)$ $W_j=r^2S_j\theta_n h_j+S_j hrx_j+2S_j\theta_n=X_j r\theta_n h_j+S_j hrx_j+2S_j\theta_n$ $\|Sig\rangle_A=/0_z\rangle^{\otimes N}$ Rotate to $\otimes_{j=1}^{N}R^{(j)}(W_j)\|0_z\rangle$ $\xrightarrow{\{M, r\theta_n, R, X, Y, hr, hrx, \|Sig\rangle_A\}}$	**Verification** Computes $h'=H(M, R)$ Computes and compare $hr_j'(=H(M, hrx_j, h, Y_j))$ $=?\ hr_j$ Performs inverse rotation $R^{(j)}\text{-}(Y_j)\|Sig\rangle_A$, obtaining $\|Z\rangle$ Compares $\|Z\rangle\ ?=\|\varphi_{pk}\rangle_A$

Figure 1 Quantum signature scheme

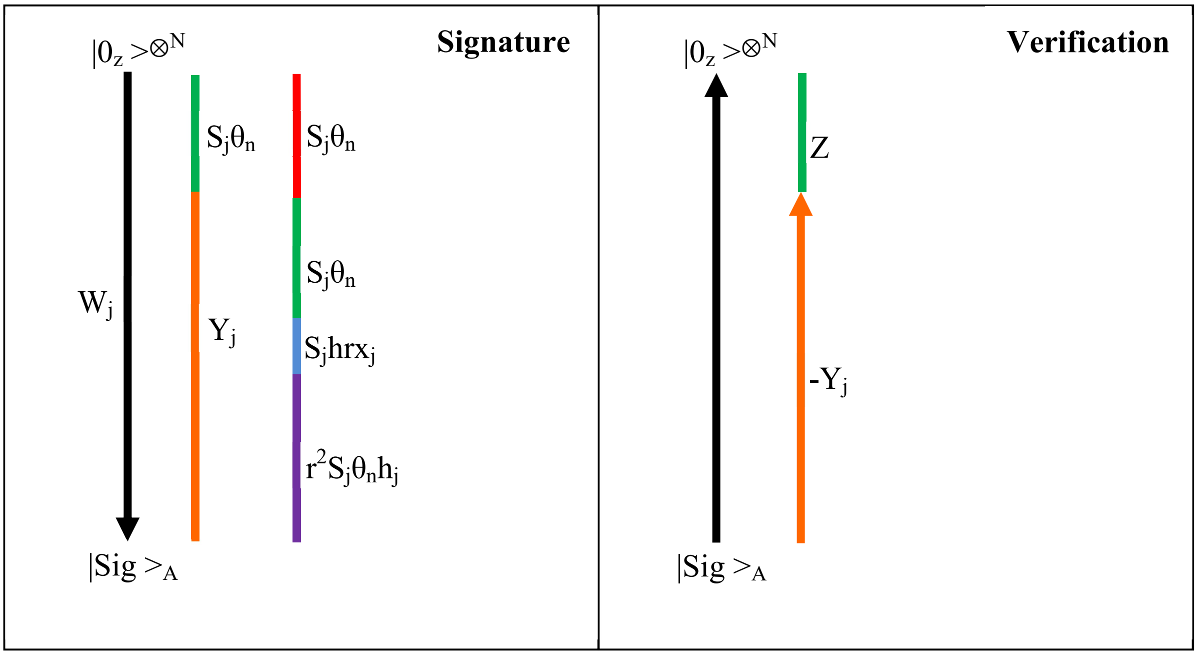

Figure 2 Schematic diagram of the rotation angle of the quantum signature scheme

4. Security analysis of the proposed quantum signature scheme

In this section, we analyze the security of our signature scheme by using the four security attributes argued in [35], as mentioned in Section 1.

4.1. Unforgeability

Because there is no specific verifier designated in our scheme, anyone (but only one person can verify it because of the physical property of the quantum state) can verify the signature. Moreover, due to that the signer does not share his private key $S_j\theta_n$ with any other, so the signature cannot be forged. In other words, if we assume that attacker E had intercepted the signature of Alice $\{M, r\theta_n, R, X, Y, hr, hrx, |Sig>_A\}$, which is to be sent to Bob, attacker E cannot successfully launch Shi's attack type, since E doesn't have signer A′s private key or the common secret which A pre-shared with B. To sum up, our quantum signature scheme has the following advantages: (1) can resist the forgery attack, (2) is undeniable for the signer, and (3) without necessity to specify a oppoint verifier. In the following, we will delineate why our scheme has the above three merits.

(1) E only chooses another message M' to replace the original M, hoping that this can successfully forge A's signature.

Attacker E intercepts the parameters transmitted by A, $\{M, r\theta_n, R, X, Y, hr, hrx, |Sig>_A\}$, he only changes the message M to his own M' without changing the others, then transmits $\{M', r\theta_n, R, X, Y, hr, hrx, |Sig>_A\}$ to B for verification.

After receiving the changed message, B does the following computations.

(a) Calculates $hr'=H(M', R)$

(b) Calculates and compares to see if the equation $hr_j'(=H(M', hrx, h', Y))=hr_j$ holds

Apparently, B would find that the calculated hr' would not be equal to the transmitted hr. This is, because E had changed the message M. So, B detects that there is an abnormality happened. Therefore, E's intent fails.

(2) E whishes to achieve his goal actively, intercepts the message sent by the signer, and changes all the parameters as possible as he can.

Attacker E intercepts the parameters $\{M, r\theta_n, R, X, Y, hr, hrx, |Sig>_A\}$ transferred by A, computes $|Sig>_E$ using the steps as shown in Section 3.2.(1), and replaces the parameters with his own set $\{M', r\theta_n', R', X', Y_E', hr', hrx', |Sig>_E\}$, which is then passed to B for verification.

After receiving the message from E, whom B think as A, B does the following.

(a) Calculates $h'=(M', R')$

(b) Calculates and compares if the equation $hr_j''(=H(M', hrx_j', h', Y_j'))=?hr_j'$

(c) Inverts degree $(-Y_{Ej})$ on $|Sig>_E$, getting $|Z_E>$

(d) Compares the measure outcome of both the quantum state $|Z_E>$ and $|\varphi_{pk}>_A$ to see if the are equal $|\varphi_{pk}>_A$

Apparently, B cannot find any abnormality and will pass the checks from (a) to (c), because the parameters are prepared by E himself. But when B performs step (d), B finds $|Z_E>$ is not equal to A′s public key $|\varphi_{pk}>_A$, because the private secrets $S_j\theta_n$ selected by A and E are different. Therefore, E′s attack fails.

(3) E takes Alice's public key $|\varphi_{pk}>_{\text{Alice}}$ to rotate an angle Y_E, and also changes

the message M to M'.

E takes Alice's public key $|\varphi_{pk}>_A$ to rotate $\mathrm{Y_E}$ angle and also he changes M to M', but keeps the other parameters $\{r\theta_n, R, X, Y, hr, hrx\}$ unchanged. E first rotates an angle $\mathrm{Y_E}$ on $|\varphi_{pk}>_A$, calculates $|Sig>_E = \otimes_{j=1}^{N} R^{(j)}(Y_E)\ |\varphi_{pk}>_A = (r^2 S_j\theta_n + S_j hrx_j + S_j\theta_n)_E + (S_j\theta_n)_A = (X_j r\theta_n h_j + S_j hrx_j + S_j\theta_n)_E + (S_j\theta_n)_A$, then E transfers parameters $\{M', r\theta_n, R, X, Y, hr, hrx, |Sig>_E\}$ to B for his verification. After receiving message from E, B performs the following calculations.

(a) Calculates $h'=H(M', R)$

(b) Calculates and compares to see if $hr_j'\ (=H(M', hrx_j, h', Y_E)) = hr_j$ holds.

Since E had changed M', $\mathrm{Y_E}$, B's calculated h' also changed. B found that $\mathrm{hr_j}$' is not equal to $\mathrm{hr_j}$. Therefore, E's attack does not succeed.

(4) E takes Alice's public key $|\varphi_{pk}>_{\mathbf{Alice}}$ to rotate $\mathbf{Y_E}$ angle and tries his best to change as many parameters as possible, which he thinks is the most helpful for successful attack on the message sent by the signer.

E takes Alice's public key $|\varphi_{pk}>_A$ to rotate $\mathrm{Y_E}$ angle, computes $|Sig>_E$ using the steps as shown in Section 3.2.(1), and replaces all of A's parameters with his own $\{M', r\theta_n', R', X', Y', hr', hrx', |Sig>_E\}$. Then, E sent it to B for B's verification.

After receiving, B will do the following.

(a) Calculates $h'=H(M', R')$

(b) Calculates and compares if $hr_j''(=H(M', hrx_j', h', YE)) = hr_j'$

(c) Inverts by angle ($-\mathrm{Y_E}$) on $|\mathrm{Sig}>_E$, obtaining $|\mathrm{Z_E}>$

(d) Measures both the quantum states $|\mathrm{Z_E}>$ and $|\varphi_{pk}>_A$ and compares the outcomes to see if they are the same.

From the above mentioned, we know that although attacker E replaces all the parameters, however, when B does step (d), he will find that both the measure outcomes of the quantum states $|Z_E>$ and A's public key $|\varphi_{pk}>_A$ are not equal. Because the secrets $S_j\theta_n$ of A and E is thus different. Therefore, E cannot successfully disguise as A, thus E's attack fails.

4.2. Identifiability

Whenever, a verifier verifies the signature, he performs the reverse operation and obtains the quantum state $|Z>$. If the measurement outcome of quantum state $|Z>$ is equal to $|\varphi_{pk}>_A$, then the identity of the signer is A. From Section 4.1, we know that A is the real signer. Thus, our scheme has this identifiability feature.

4.3. Verifiability

From the analysis shown in Section 4.1, we see that our quantum signature is unforgeable. This guarantees that the signature is actually from the signer. Thus, our signature scheme can be verified when performing the steps shown in Section 3.2 (b).

4.4. Non-repudiation

For the reasons stated in Section 4.1 through 4.3 that our scheme cannot be forged, and has the identifiability and verifiability features, it naturally deduces this result that our scheme has the non-repudiation property.

5. Comparisons and discussions

In this section, we first compare our scheme with the state of the art by using the four security attributes mentioned in [35]. Then, we discuss the reason why our scheme is some what outstanding even the state of the art.

5.1. Comparisons

In this section, we compare our approach to the state of the art based on the four security requirements of a quantum signature scheme. We summarize it in Table 1.

Table 1 comparisons among state of the art

Schem Security requirements	Ours	Kaushik et al.'s scheme [80]	Shi et al.'s scheme [81]
Unforgeability	O	X	X
Non-repudiation	O	X	X
Verifiability	O	O	O
Identifiability	O	O	O

5.2. Discussions

From Table 1, we can see that our scheme is safer than the state of the art. Moreover, it does not need to assign a specific verifier, which is the first work in this aspect. And thus more coincide with the reasoning logic of human beings. We effect that our method will be greatly adopted in the real applications in human life to get rid of the appication obstacle when adapting the scheme in the state of the art to real life.

6. Future work

We know that voting is an important activity in every democratic country. The current method of voting in Taiwan demands that people must go to the prescribed place to vote within the prescribed time. This will cost a lot of manpower, material resources, time, and money. Once the voters are too much to be accommodated in the voting place, it is likely that the people who are late to vote will have to wait for a long time, which may cause the people unwilling to vote and thus quit his voting right. Therefore, if one can design an quantum voting system, the people only need to vote online at home, then the government can greatly simplify the process of vote counting.

In this paper, we have successfully proposed a quantum signature scheme. After this work, we consider that a voting system is basically a signature scheme for the ballot which has already embedded with a selected candidate to be blindly signed by the election committee. This stipulates our further work idea that we can further adapted the proposed to be to be applicable for a voting system. That is, our further work will be on the topics, which are : (1) a blind quantum signature scheme and (2) a quantum voting system using the proposed quantum signature combined with the one (1). Repeatedly, we want to combine our quantum signature scheme and the quantum blind signature scheme, which must satisfy five attributes: (1) unforgeability, (2) verifiability, (3) non-repudiation, and (4) identifiability (5) anonymity, to design a safe quantum voting system.

7. Conclusion

In this paper, we have successively presented a publicly verifiable quantum signature scheme. Through cryptanalysis, we confirm that our solution not only resists forgery attacks, but also possesses the undeniable function, which are more suitable for application in real life than the state of the art. In addition, in view of : (1) quantum computer is the development trend of the whole world in the future, (2) the inheritant nature of the voting system is basically the application of a signature combined with a blind signature scheme, and (3) the domestic election drawbacks shown at the end of the last year in Taiwan, the future work of this article tries to design a quantum blind signature, which will then be further applied in our secondary future design, a quantum voting system. Totally, how to design a truly secure quantum voting system is the ultimate goal that this series of research will achieve in its future work.

References

[1] KATZ, Jonathan, et al. Handbook of applied cryptography. CRC press, 1996.

[2] S. Saeednia, “An identity-based society oriented signaturescheme with anonymous signers,” Information processingLetters, vol. 83, no. 6, pp. 295–299, 2002.

[3] C. L. Hsu, T. S. Wu, and T. C. Wu, “Group-oriented signaturescheme with distinguished signingauthorities,” FutureGeneration Computer Systems, vol. 20, no. 5, pp. 865–873, 2004.

[4] C. Y. Lin, T. C. Wu, F. Zhang, and J. J. Hwang, “New identitybasedsociety oriented signature schemes from pairings onelliptic curves,” Applied Mathematics and Computation, vol.160, no. 1, pp. 245–260, 2005.

[5] Z. Shao, “Certificate-based verifiably encrypted signaturesfrom pairings,” Information Sciences, vol. 178, no. 10, pp.2360–2373, 2008.

[6] J. Zhang and J. Mao, “A novel ID-based designated verifiersignature scheme,” Information Sciences, vol. 178, no. 3, pp.766–773, 2008.

[7] Y. F. Chung, Z. Y.Wu, and T. S. Chen, “Ring signature schemefor ECC-based anonymous signcryption,” Computer Standardsand Interfaces, vol. 31, no. 4, pp. 669–674, 2009.

[8] M. Mambo, K. Usuda, and E.Okamoto, “Proxy signature: delegationof the power to sign messages,” IEICE—Transactionson Fundamentals of Electronics, vol. E79-A, no. 9, pp. 1338–1354, 1996.

[9] R. Lu, Z. Cao, and Y. Zhou, “Proxy blind multi-signaturescheme without a secure channel,” Applied Mathematics andComputation, vol. 164, no. 1, pp. 179–187, 2005.

[10] H. F.Huang and C. C. Chang, “A novel efficient （t, n）thresholdproxy signature scheme,” Information Sciences, vol. 176, no. 10,pp. 1338–1349, 2006.

[11] B. Kang, C. Boyd, and E. Dawson, “Identity-based strongdesignated verifier signature schemes: attacks and new construction,”Computers and Electrical Engineering, vol. 35, no. 1,pp. 49–53, 2009.

[12] K. L. Wu, J. Zou, X. H. Wei, and F. Y. Liu, “Proxy groupsignature: a new anonymous proxy signature scheme,” inProceedings of the 7th International Conference on MachineLearning and Cybernetics（ICMLC’08）, pp. 1369–1373, Kunming,China, July 2008.

[13] Z. Shao, “Improvement of identity-based proxy multisignaturescheme,” The Journal of Systems and Software, vol. 82,no. 5, pp. 794–800, 2009.

[14] Z. H. Liu, Y. P. Hu, X. S. Zhang, and H. Ma, “Secure proxysignature scheme with fast revocation in the standard model,”Journal of China Universities of Posts and Telecommunications,vol. 16, no. 4, pp. 116–124, 2009.

[15] Y. Yu, C. Xu, X. Huang, and Y. Mu, “An efficient anonymousproxy signature scheme with provable security,” ComputerStandards and Interfaces, vol. 31, no. 2, pp. 348–353, 2009.

[16] F. Cao and Z. Cao, “A secure identity-based proxy multisignaturescheme,” Information Sciences, vol. 179, no. 3, pp.292–302, 2009.

[17] A. Yang andW. P. Peng, “A modified anonymous proxy signaturewith a trusted party,” in Proceedings of the 1st InternationalWorkshop on Education Technology and Computer Science（ETCS’09）, pp. 233–236,Wuhan, China, March 2009.

[18] J. H. Hu and J. Zhang, “Cryptanalysis and improvement of athreshold proxy signature scheme,” Computer Standards andInterfaces, vol. 31, no. 1, pp. 169–173, 2009.

[19] Y. Yu, C. X. Xu, X. S. Zhang, and Y. J. Liao, “Designated verifierproxy signature scheme without random oracles,” Computersand Mathematics with Applications, vol. 57, no. 8, pp. 1352–1364, 2009.

[20] J. H. Zhang, C. L. Liu, and Y. I. Yang, “An efficient secure proxyverifiably encrypted signature scheme,” Journal of Network andComputer Applications, vol. 33, no. 1, pp. 29–34, 2010.

[21] B. D. Wei, F. G. Zhang, and X. F. Chen, “ID-based ring proxysignatures,” in Proceedings of the IEEE International Symposiumon Information Theory（ISIT’07）, pp. 1031–1035, Nice,France, June 2007.

[22] T. S. Wu and H. Y. Lin, “Efficient self-certified proxy CAEscheme and its variants,” The Journal of Systems and Software,vol. 82, no. 6, pp. 974–980, 2009.

[23] S. Lal and V. Verma, “Identity based Bi-designated verifierproxy signature schemes,” Cryptography EprintArchiveReport 394, 2008.

[24] S. Lal and V. Verma, “Identity based strong designated verifierproxy signature schemes,” Cryptography EprintArchiveReport 394, 2006.

[25] C. Y. Yang, S. F. Tzeng, and M. S. Hwang, “On the efficiency ofnonrepudiable threshold proxy signature scheme with knownsigners,” The Journal of Systems and Software, vol. 73, no. 3, pp.507–514, 2004.

[26] H. Xiong, J. Hu, Z. Chen, and F. Li, “On the security of anidentity based multi-proxy signature scheme,” Computers andElectrical Engineering, vol. 37, no. 2, pp. 129–135, 2011.

[27] Y. Sun, C. Xu, Y. Yu, and Y. Mu, “Strongly unforgeable proxysignature scheme secure in the standard model,” The Journalof Systems and Software, vol. 84, no. 9, pp. 1471–1479, 2011.

[28] Y. Sun, C. Xu, Y. Yu, and B. Yang, “Improvement of a proxymulti-signature scheme without random oracles,” ComputerCommunications, vol. 34, no. 3, pp. 257–263, 2011.

[29] Z. Liu, Y. Hu, X. Zhang, and H. Ma, “Provably securemulti-proxy signature

scheme with revocation in the standardmodel," Computer Communications, vol. 34, no. 3, pp. 494–501, 2011.

[30] H. Bao, Z. Cao, and S. Wang, "Improvement on Tzenget al.'s nonrepudiable threshold multi-proxy multi-signaturescheme with shared verification," Applied Mathematics andComputation, vol. 169, no. 2, pp. 1419–1430, 2005.

[31] J. G. Li and Z. F. Cao, "Improvement of a threshold proxy signaturescheme," Computer Research and Development, vol. 39,no. 11, pp. 1513–1518, 2002.

[32] Y. Yu, Y. Mu, W. Susilo, Y. Sun, and Y. Ji, "Provably secureproxy signature scheme from factorization,"MathematicalandComputer Modelling, vol. 55, no. 3-4, pp. 1160–1168, 2012.

[33] K. Shum and V. K. Wei, "A strong proxy signature schemewith proxy signer privacy protection," in Proceedings of the11th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises（WETICE'02）, pp.55–56, Pittsburgh, Pa, USA, 2002.

[34] N. Y. Lee and M. F. Lee, "The security of a strong proxy signaturescheme with proxy signer privacy protection," AppliedMathematics and Computation, vol. 161, no. 3, pp. 807–812,2005.

[35] Chou, Jue-Sam."A novel anonymous proxy signature scheme." Advances in Multimedia 2012 （2012）： 13.

[36] C.Dwork,M.Naor,A.Sahai,"Concurrentzero-knowledge."Proceedings of 30th ACMSTOC'98, 1998, pp. 409–418.

[37] Y.Aumann,M.Rabin,"Efficientdeniableauthenticationoflongmessages."Int. Conf. on Theoretical Computer ScienceinHonorofProfessorManuelBlum's 60th birthday, http: //www.cs.cityu.edu.hk/dept/video.html. April 20–24, 1998.

[38] MarioDiRaimondo,RosarioGennaroandHugoKrawczyk,"Deniable 17 AuthenticationandKeyExchange,"ACM CCS'06, October, 2006, Alexandria,

Virginia, USA.

[39] C. Boyd, W. Mao, K. Paterson, “Deniableauthenticatedkeyestablishmentfor Internetprotocols.”11th International Workshop on Security Protocols, Cambridge （UK）, April 2003.

[40] C. Boyd&W. Mao,“Keyagreementusingstaticallykeyedauthentication.” AppliedCryptologyandNetworkSecurity（ACNS’04）, LNCS 3089, pp.248-262.

[41] Z.Shao,“Efficientdeniableauthenticationprotocolbasedongeneralized ElGamalsignaturescheme.”Computer Standards & Interfaces 26 （5）, 2004, pp.449–454.

[42] R. Lu,Z.Cao,“Anewdeniableauthenticationprotocolfrombilinearpairings.” Applied Mathematics and Computation 168 （2）, 2005, pp.954–961.

[43] R.Lu,Z.Cao,“Non-interactive deniable authentication protocol based on factoring.”Computer Standards & Interfaces 27 （4）, 2005, pp.401–405.

[44] TianjieCao,DongdaiLinaandRuiXue,“AnefficientID-baseddeniableauthentication protocolfrompairings,”Proceedings of the 19th International ConferenceonAdvancedInformationNetworkingandApplications（AINA’05）, IEEE, 2005.

[45] Wei-Bin Lee, Chia-Chun Wu and Woei-JiunnTsaur,“AnoveldeniableauthenticationprotocolusinggeneralizedElGamalsignaturescheme,” Information Science, 2006.

[46] Rongxing Lu, Zhenfu Cao, “Erratumto“Non-interactive deniable authentication protocol based on factoring”[ComputerStandards&Interfaces27（2005） 401–405].”Computer Standards & Interfaces 29, pp.275, February 2007

[47] Chun-Ta Li, Min-Shiang Hwang and Chi-Yu Liu, “Anelectronic voting protocol with deniable authentication for mobile ad hoc networks.”Computer Communication 31（10）, pp.2534-2540, June 2008.

[48] Bin Wang and ZhaoXia Song, “Anon-interactive deniable authentication scheme based on designated verifier proofs.”Information Sciences 179（6）, pp.858-865, March 2009.

[49] Taek-Young Youn, Changhoon Lee and Young-Ho Park, “Anefficient non-interactive deniable authentication scheme based on trapdoor commitment schemes.”Computer Communications, In Press, Corrected Proof, March 2010.

[50] LeinHarn and Jian Ren, “Design of Fully Deniable Authentication Service for E-mail Applications.”IEEE Communications Letters 12（3）, pp.219-221, March 2008.

[51] Chen, Yalin, Jue-Sam Chou, and Chi-Fong Lin. "A Novel Non-interactive Deniable Authentication Protocol with Designated Verifier on elliptic curve cryptosystem." IACR Cryptology ePrint Archive 2010 （2010）: 549.

[52] F. Kerschbaum, N. Oertel, and L. W. F. Chaves, “Privacypreservingcomputation of benchmarks on item-level datausing RFID.” in Proceedings of the 3rd ACM Conference onWireless Network Security （WiSec ‘10）, pp. 105–110, March2010.

[53] M. O. Rabin, “How to exchange secrets with obliviousransfer.”Tech. Rep. TR-81, Aiken Computation Lab, HarvardUniversity, Cambridge, Mass, USA, 1981.

[54] S.Even, O. Goldreich, and A. Lempel, “A randomized protocolfor signing contracts.”Communications of the ACM, vol. 28,no. 6, pp. 637–647, 1985.

[55] G. Brassard, C. Crepeau, and J.-M.Robert, “All-or-nothingdisclosure of secrets.” in Proceedings of the InternationalConference on Advances in Cryptology （CRYPTO ‘86）, vol. 263of Lecture Notes in Computer Science, pp. 234–238, 1986.

[56] Chou, Jue-Sam, and Yi-ShiungYeh."Mental poker game based on a bit commitment scheme through network." Computer Networks 38.2 （2002）:

247-255.[57] M. Bellare and S. Micali, “Non-interactive oblivious transferand application,” in Proceedings of the International Conferenceon Advances in Cryptology （CRYPTO ‘89）, vol. 435 ofLectureNotes in Computer Science, pp. 547–557, 1989.

[57] M. Naor and B. Pinkas, “Oblivious transfer with adaptivequeries,” in Proceedings of the International Conference on Advancesin Cryptology （CRYPTO ‘99）, Lecture Notes in ComputerScience, pp. 573–590, 1999.

[58] M. Naor, B. Pinkas, and R. Sumner, “Privacy preserving auctionsand mechanism design,” in Proceedings of the 1st ACMConference on Electronic Commerce, 1999.

[59] M. Naor and B. Pinkas, “Distributed oblivious transfer,” inProceedings of the International Conference on Advances inCryptology（CRYPTO ‘00）, vol. 1976 of Lecture Notes in Computer Science, 2000.

[60] M. Naor and B. Pinkast, “Oblivious transfer and polynomialevaluation.” in Proceedings of the 31st Annual ACM Symposiumon Theory of Computing （FCRC ‘99）, pp. 245–254, May 1999.

[61] M.NaorandB.Pinkas, “Efficient oblivious transfer protocols.”inProceedings of the 12th annual ACM-SIAM symposium onDiscret Mathematics（SODA ‘01）, pp. 448–457, 2001.

[62] H. Ghodosi, “On insecurity of Naor-Pinkas’ distributedoblivious transfer,” Information Processing Letters, vol. 104, no.5, pp. 179–182, 2007.

[63] Y. Mu, J. Zhang, and V. Varadharajan, “m out of n oblivioustransfer,” in Proceedings of the 7th Australasian Conference onInformation Security and Privacy（ACISP ‘02), vol. 2384 ofLecture Notes in Computer Science, pp. 395–405, 2002.

[64] H. Ghodosi and R. Zaare-Nahandi, “Comments on the ‘m outof n oblivious transfer.”Information Processing Letters, vol. 97,no. 4, pp. 153–155, 2006.

[65] W. Ogata and K. Kurosawa, “Oblivious keyword search.”Journal of Complexity, vol. 20, no. 2-3, pp. 356–371, 2004.

[66] C. K. Chu and W. G. Tzeng, “Efficient k-out-of-n oblivioustransfer schemes with adaptive and non-adaptive queries.” inProceedings of the 8th International Workshop on Theory andPractice in Public Key Cryptography （PKC ‘05）, pp. 172–183,January 2005.

[67] J. Zhang and Y.Wang, “Two provably secure k-out-of-n oblivioustransfer schemes,” AppliedMathematics and Computation,vol. 169, no. 2, pp. 1211–1220, 2005.

[68] H. F. Huang and C. C. Chang, “A new design for efficient tout-n oblivious transfer scheme.” in Proceedings of the 19thInternational Conference on Advanced Information Networkingand Applications （AINA ‘05）, pp. 28–30, March 2005.

[69] A. Parakh, “Oblivious transfer using elliptic curves.” in Proceedingsof the 15th International Conference on Computing（CIC ‘06）, pp. 323–328, November 2006.

[70] S. Kimand G. Lee, “Secure verifiable non-interactive oblivioustransfer protocol using RSA and Bit commitment on distributedenvironment.”Future Generation Computer Systems, vol.25, no. 3, pp. 352–357, 2009.

[71] Y. F. Chang and W. C. Shiao, “The essential design principlesof verifiable non-interactive OT protocols.” in Proceedings ofthe 8th International Conference on Intelligent Systems Designand Applications （ISDA ‘08）, pp. 241–245, November 2008.

[72] L. M. Kohnfelder, “On the signature reblocking problem inpublic-key cryptography.”Communications of the ACM, vol.21, no. 2, p. 179, 1978.

[73] S. Halevi and Y. T. Kalai, “Smooth projective hashing andtwo-message oblivious transfer.”Cryptology ePrint Archive2007/118, 2007.

[74] J. Camenisch, G. Neven, and A. Shelat, “Simulatableadaptiveoblivious transfer.” in Proceedings of the Annual InternationalConference on the Theory and Applications of CryptographicTechniques, vol. 4515 of Lecture Notes in Computer Science, pp.573–590, 2007.

[75] M. Green and S. Hohenberger, “Blind identity-based encryptionandsimulatable oblivious transfer.”Cryptology ePrintArchive 2007/235, 2007.

[76] J. Qin, H. W. Zhao, and M. Q. Wang, “Non-interactive obliviousransfer protocols.” in Proceedings of the InternationalForum on Information Technology and Applications （IFITA ‘09）,pp. 120–124, May 2009.

[77] C. C. Chang and J. S. Lee, “Robust t-out-of-n oblivioustransfer mechanism based on CRT.”Journal of Network andComputer Applications, vol. 32, no. 1, pp. 226–235, 2009.

[78] X. Ma, L. Xu, and F. Zhang, “Oblivious transfer with timedreleasereceiver’s privacy.”Journal of Systems and Software, vol.84, no. 3, pp. 460–464, 2011.

[79] Chou, Jue-Sam."A novel k-out-of-n oblivious transfer protocol from bilinear pairing." Advances in Multimedia 2012 （2012）： 3.

[80] 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）

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

[82] 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.

[83] 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.

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

[85] Wen, Xiaojun, et al. "A weak blind signature scheme based on quantum cryptography." Optics Communications 282.4 （2009）： 666-669.

[86] 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.

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

[88] 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.

[89] 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.

[90] 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.

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

[92] 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.

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

[94] 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）.