A publicly verifiable quantum signature scheme based on asymmetric quantum cryptography without entanglement

Yalin Chen 1, Jue-Sam Chou 2*, Fang-Qi Zhou 3, Shu-Mei Hsu 4

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+(05)+272-1001 ext.56536
3 Department of Information Management, Nanhua University, Taiwan
zz66016@gmail.com
4 Department of Mathematics and Physics Education, Chiayi University, Taiwan
m8503015@gmail.com

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 solution 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, based on their key generation, we propose a novel scheme to make it publicly verifiable and hence more suitable to be applied in real life. After cryptanalysis, we confirm that our method not only resist the forgery attack, including the linear attack which is inevitably happening in a quantum state rotation-based scheme, but also is undeniable and publicly verifiable.

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 their 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 with the (especially the advancement of physical materials and secure communication networks) combination of quantum mechanics applications, 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 suffers from the forgery attack. They further proposed an improvement 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 the signature actually signed by him), because the signer and the verifier shared a common secret $\theta_{n1}$. This leads to the denial problem for that the original signer Alice can deny her signed message and declare the signature is from the verifier Bob, due to the fact that Bob also can use her public key, $|\varphi_{pk}\rangle_{Alice} = \bigotimes_{j=1}^{N} R(\theta_{n}) S_{j} |0\rangle_{j}$, together with their common secret $\theta_{n1}$ to perform a rotation operation $\bigotimes_{j=1}^{N} R(\theta_{n1})$ on $|\varphi_{pk}\rangle_{Alice}$ to obtain the same signature. 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 fact that she had signed the signature. 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.

For the reasons mentioned above, 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 can forge A’s signature on a message. After that, based on Laurent, et al.’s [95] argument that one-way function is an attractive cryptographic component in the post-quantum era, we propose a hash-based undeniable quantum signature protocol, which not only meet the above four security demands, but also is publicly verifiable and more consistent with human reasoning logic; hence, more applicable to real life than the state-of-the-art.

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 attacks and improvements. In Section 3, we describe the problems found in Shi et al.’s scheme. Then, we propose a publicly verifiable quantum signature scheme based on asymmetric quantum cryptography in Section 4. And its security analyses are shown in Section 5. After that in Section 6, we give the comparison results of our scheme with the state-of-the-art, and discussions about the applications and future work. Finally, a conclusion is given in Section 7.

2. Review Kasumk et al.’s quantum signature scheme and Shi et al.’s attacks and improvements

In this section, we first review Kaushik et al. ’s quantum signature scheme in Section 2.1, then describe Shi et al.’s attacks and improvements in Section 2.2.

2.1. Kaushik et al.’s quantum signature scheme

Their signature scheme [80] is divided into three phases: (1) the key generation phase, (2) the signature stage, and (3) the verification phase. We describe them separately below:

1) Key generation phase: In this stage, the cryptosystem generates a public private key pair for each user in the system by using the following steps.

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

(b) Prepares the N-qubits state $|\theta_z\rangle \otimes^N$.

(c) Applies the rotation operation $R^0(S_j\theta_n)_A$ on the quantum state $|\theta_z\rangle \otimes^N$, $j=1$ to N, to generate the public key of A, $|\varphi_{pk}\rangle_A = \otimes^N j=1 R^0(S_j\theta_n)_A |\theta_z\rangle$, 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 a fixed output length of N bits.

(b) Performs a rotation operation $R^0(h_j\pi)$ on state $|\theta_z\rangle \otimes^N$, getting $|\varphi_{h_j}\rangle_A = \otimes^N j=1 R^0(h_j\pi)|\theta_z\rangle$.

(c) Uses her private key $(S_j\theta_n)_A$ to perform a rotation operation $R^0(S_j\theta_n)_A$ at $|\varphi_{h_j}\rangle_A$, obtaining the signature $|\varphi_{h_j,s_j}(\theta_n)\rangle_A = \otimes^N j=1 R^0(S_j\theta_n)_A |\varphi_{h_j}\rangle_A$ of M, and then sends message M with the signature, $\{M, |\varphi_{h_j,s_j}(\theta_n)\rangle_A\}$, to Bob (B).

3) Verification phase: Upon receiving $\{M, |\varphi_{h_j,s_j}(\theta_n)\rangle_A\}$, B performs the verification operation by using the following steps.

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

(b) Performs reverse rotation operation $\otimes^N j=1 R^0(-h_j\pi)$ on $|\varphi_{h_j,s_j}(\theta_n)\rangle_A$, getting $|\varphi_{pk}\rangle'_A = \otimes^N j=1 R^0(-h_j\pi)|\varphi_{h_j,s_j}(\theta_n)\rangle_A$.

(c) Measures both the quantum states of $|\varphi_{pk}\rangle_A$ and Alice’s public key $|\varphi_{pk}\rangle_A$ to see if the
outcomes are equal. If they are equal, B accepts; otherwise, he rejects.

2.2. Shi et al.’s attacks and improvements

After analyzing Kaushik et al.’s 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, then show the improvement.

(1) E’s forgery attacks:
(a) Calculates \( h = H(M) \) and pretends A to perform the inverse operation \( R^{(j)}(-h\pi) \) on \( |\varphi_{\theta_j\theta_n}^{s}(\theta_n)\rangle_A \), obtaining \( |\varphi_{pk}^{s}\rangle_A \).
(b) Chooses another message \( M' = \{m_1', m_2', \ldots, m_N'\} \) of length \( N \), calculates \( h' = H(M') \), and forges a signature \( |\varphi_{\theta_j\theta_n}^{s'}(\theta_n)\rangle_A = \bigotimes_{j=1}^{N} R^{(j)}(h'_j\pi) |\varphi_{pk}^{s'}\rangle_A \).
(c) Sends the message signature pair \{\( M' \), \( |\varphi_{\theta_j\theta_n}^{s'}(\theta_n)\rangle_A \} \) to B for verification.

It is obvious that the signature pair can be successfully verified by B as well, who thinks that the signature is from A. But indeed, it is signed by E.

(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 \( n_1 \rangle \rangle 1 \) in advance. Then, A and B together perform the signature and verification process as follows.

(a) A’s signing
A uses a rotation operation \( R^{(j)}(h_1\theta_{n1}) \), instead of \( R^{(j)}(h_\pi) \), to operate on the quantum state \( |\theta_2\rangle \bigotimes_{j=1}^{N} \), giving the result \( |\varphi_{h_1\theta_{n1}}^{s}(\theta_n)\rangle_A = \bigotimes_{j=1}^{N} R^{(j)}(h_j\theta_{n1}) |\theta_2\rangle \). 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 \( R^{(j)}(-h_1\theta_{n1}) \) on \( |\varphi_{h_1\theta_{n1}}^{s}(\theta_n)\rangle_A \), instead of \( R^{(j)}(-h_\pi) \), measures and compares both the outcomes to see whether the two quantum states measurement results \( |\varphi_{pk}^{s}\rangle_A = \bigotimes_{j=1}^{N} R^{(j)}(-h_j\theta_{n1}) |\varphi_{h_1\theta_{n1}}^{s}(\theta_n)\rangle_A \) and \( |\varphi_{pk}^{s'}\rangle_A \) are equal. If the equation holds, B accepts; otherwise, he rejects.

Undoubtedly, B’s verification equation will hold. Under this situation E cannot successfully launch a forgery attack, because he does not know the common secret \( \theta_{n1} \) shared between A and B. Therefore, Shi et al. 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 sections.

3. The problems found in Shi et al.’s scheme

In Shi et al.’s improvement, the signer A and the verifier B had to pre-share a random integer \( n_1 \rangle \rangle 1 \). This makes the signature can be verified only by the specific verifier B. In addition, if B initiates the same attack as described in Section 2.2.2.(1), he can pretend signer A to sign on the message \( M' \). That is, if the verifier B is malicious, after receiving \{\( M \), \( |\varphi_{h_1\theta_{n1}}^{s}(\theta_n)\rangle_A \}\) from A, B can pretend A to sign on another message \( M' \) as follows.

1. Computes \( h = H(M) \) and applies an inverse rotation \( R^{(j)}(-h_1\theta_{n1}) \) on \( |\varphi_{h_1\theta_{n1}}^{s}(\theta_n)\rangle_A \) to get \( \langle\varphi_{pk}^{s'}| \rangle_A \).
2. Chooses another message \( M' \) and computes \( h' = H(M') \). By performing a rotation operation \( \bigotimes_{j=1}^{N} R^{(j)}(h'_j\theta_{n1}) \) on \( |\varphi_{pk}^{s'}\rangle_A \), B gets \( |\varphi_{h_1\theta_{n1}}^{s'}(\theta_n)\rangle_A \).
3. Sends \{\( M' \), \( |\varphi_{h_1\theta_{n1}}^{s'}(\theta_n)\rangle_A \} \) to the dispute resolution authority.
 Obviously, it can be successfully verified by the authority. Therefore, although B counterfeits the signature of A, it is not a signature that Alice can deny. Because B can say that A is the original signer due to the fact that A also knows the common secret \( \theta_n \) and has her own public key \( \varphi_{pk} \), whereas the message is actually signed by B. This means that in Shi et al's, improved scheme the signer is deniable. To avoid the drawback, we propose a publicly verifiable quantum non-deniable signature scheme in Section 4.

4. The proposed quantum signature scheme

Because there is no specific verifier designated in our scheme, anyone can verify the signature. But only one person can verify it due to the physical property no-cloning theorem of a quantum state, except that each member prepares his public key quantum state many times [96-98]. Naturally in this paper, we assume that each signer prepares one quantum public key for each of his signature generation.

In this section, we present our scheme in the followings. We also depict it in Figure 1. Figure 2 shows the semantic diagram of the rotation angles in the proposed protocol.

4.1. Signature phase

A uses the following steps to sign on a message M.

1. Selects a random number \( r_1 \).
2. \( H(m_1, r_1) = q \ast (S \theta_n) + r = W_1, \) \( hq=H(q, r, (S \theta_n)) \)
   \( X_1 = (q-1)S, X_2 = (\theta_n + \frac{3r}{q-1}S) \)
   \( Q = H(m, r_1, (S \theta_n), X_1, X_2) \)
   \( W = QW_1 + Qr = Q(q \ast (S \theta_n)) + Qr = Q(q \ast (S \theta_n) + 2r) \)
   \( QX_1X_2 = Q((q-1)S) + 3Qr \)
   \( Y = W - QX_1X_2 = (S \theta_n) + Qr = (Q-1)(S \theta_n) - Qr \)
   \( hw = H(m, r_1, hq, \theta, X_1, X_2, Y, hw) \)
3. \( |\text{Sig}_A\rangle = R_j(W + hw) |0_z\rangle \)
4. Sends \( m, r_1, hq, Q, X_1, X_2, Y, hw \) to Bob (B) through the classical channel, and \( |\text{Sig}_A\rangle \) through quantum channel.

4.2. Verification phase

After receiving \( \{ m, r_1, hq, Q, X_1, X_2, Y, hw, |\text{Sig}_A\rangle \} \), B performs the following steps to verify it.

1. Computes \( hw = H(m, r_1, hq, Q, X_1, X_2, Y, hw) \)
2. Computes \( H(Y) \), and \( QX_1X_2 \)
3. If \( H(Y) < Y \), computes \( \theta_1 = Y - H(Y), Q\theta = hm + QX_1X_2 + \theta_1 \), else computes \( \theta_2 = H(Y) - Y, Q\theta = hm + QX_1X_2 - \theta_2 \)
4. Performs inverse rotation operation \( R_j(Q\theta) \) on \( |\text{Sig}_A\rangle \), obtaining \( |Z\rangle \)
5. Performs rotation operation \( R_j(H(Y)) \) on \( |\varphi_{pk}\rangle \), obtaining \( |Z'\rangle \)
6. Measures both states \( |Z\rangle \) and \( |Z'\rangle \), compares the outcomes to see if they are equal. If the equation holds, B accepts; otherwise, he rejects.
5. Security analysis

In this section, we first analyze the unforgeability attribute of our signature scheme, then analyze the other properties argued in [35] (as mentioned in Section 1).

5.1. Unforgeability

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 message of Alice $\{m, r_1, hq, Q, X_1, X_2, Y, hw, |\text{Sig}^A\}$, which is signed by A and sent to Bob for verification, attacker E cannot successfully launch Shi’s type attack, since E doesn’t have signer A’s private key, or the common secret which A pre-shared with B. In the following, we will use five cases to show the reasons why our scheme has the unforgeability merit. The fourth is the case which we define as rotating-to-PKA-and-forge (RPAf) attack. In this attack, E tries to use the transmitted parameters to reversely rotate $|\text{Sig}^A\rangle$ to the same degree as $|\varphi_{pk}^A\rangle$, named state $|Z\rangle$. Then, based on both states, $|\varphi_{pk}^A\rangle$ and $|Z\rangle$, E intends to forge relative parameters to be successfully verified by B. The fifth is the case which we define as a linear attack, where the attacker E rotates $|\text{Sig}^A\rangle$ by rotating degree $k$, $k \in \mathbb{Z}$, producing state $|Z\rangle$ and also rotates $Q^{\theta}+H(Y)+k$ on $|\varphi_{pk}^A\rangle$ to produce state $|Z'\rangle$. He launches such an attack to make the measurement outcomes of both equally.

Case (1): Attacker E intercepts the signature parameters $\{m, r_1, hq, Q, X_1, X_2, Y, hw, |\text{Sig}^A\}$ transmitted by A, E tries to keep all the transmitted message unchanged to the maximum extent, because he doesn’t know the signer’s private key $(S_j\theta_n)^A$, but forge the other parameters.

Under this situation, because E doesn’t know the signer’s private key $(S_j\theta_n)^A$, the signer’s private key related parameters $hq, Q, X_1, X_2, Y, hw, |\text{Sig}^A\rangle$ cannot be changed. The left parameters which are $(S_j\theta_n)^A$ unrelated are $m$ and $r_1$. Without loss of generality, we assume $m$ is unchanged. Since $hm (= H(m, r_1, hq, Q, X_1, X_2, Y, hw))$ is signer’s private key $(S_j\theta_n)^A$ related. It must be kept the same. From this, we know that $r_1$ cannot be changed, neither. Totally, without the knowledge of signer’s private key, any parameter cannot be altered.

Case (2): E tries to achieve the attack, regardless of any parameter changed in the sent message from the signer. E replaces all of A’s parameters with his own, $\{hr', m', r_1', X_1', X_2', Y', |\text{Sig}'^A\}$, except that he does not attempt to change A’s private $(S_j\theta_n)^A$.

In this regard, we assume that E chooses another message m’s and a random number $r_1'$ to compute the relative parameters as shown in the signature phase. Since E doesn’t have the signer’s quantum private
key, from the equations in the signature phase, we can easily see that other than \( m, r_1 \), each parameter is \((S_{\theta_n})_E\) related. Under this scenario, After receiving the sent message from A, B computes \( hm'=H(m', r_1', hq, Q, X_1, X_2, Y, hw) \). But now \( hm' \) does not equal to \( hm \), which is embedded in \(|\text{Sig}\rangle_A\). Hence, in step(6), B will reject the signature.

**Case (3): E tries to achieve the attack, regardless of any parameter changed in the sent message from the signer. E replaces all of A’s parameters by using his own private key \((S_{\theta_n})_E\), \{hq, r, m', \( r_1', X_1, X_2', Y, |\text{Sig}\rangle \}_A\}.

In this regard, we assume that E chooses another message \( m' \)’s and a random number \( r_1' \) to compute the relative parameters as shown in the signature phase. This will result in the altering of related parameters. We show them as follows.

\[
W_j=H(m', r_1)=q'*((S_{\theta_n})_E+r'), \quad hw'=H(q', r', (S_{\theta_n})_E), \quad h^r=H(m', r_1', (S_{\theta_n})_E), \quad X_1'=q'-1 (S_{\theta_n})_E, \quad X_2'=\theta_n+3r (S_{\theta_n})_E, \quad Q'=H(m', r_1', (S_{\theta_n})_E, X_1, X_2), \quad W'=Q'W'+Q'r' (Q'=(q'*((S_{\theta_n})_E+r')) \quad hw'=H(w', Q', X_1', X_2', Y, (S_{\theta_n})_E)
\]

\[
Q'X_1X_2=Q'(q'-1) (S_{\theta_n})_E+3Q'r'
\]

\[
Y'=w'Q'X_1X_2 (Q'=(q'-1) (S_{\theta_n})_E) \quad hw'=H(m', r_1', hq, Q', X_1', X_2', Y, hw')
\]

\[
|\text{Sig}\rangle_A = \text{Rotates state } |\theta_z\rangle \otimes^N \bigotimes_{j=1}^N R^{(0)}(W''+hm')_j |\theta_z\rangle.
\]

Under this scenario, After receiving \{ \( m', r_1', hq', Q', X_1', X_2', Y', hw'\}, \(|\text{Sig}\rangle \}_A\}, B performs the following steps to verify it.

1. Computes \( hm'=H(m', r_1', hq', Q', X_1', X_2', Y', hw') \)
2. Computes \( H(Y') \), and \( Q'X_1'X_2' \)
3. If \( H(Y') < Y' \), computes \( \theta_1' = Y'-H(Y') \), \( Q\theta' = hm'+Q'X_1X_2+\theta_1' \), else computes \( \theta_2' = H(Y')-Y' \), \( Q\theta' = hm'+Q'X_1X_2-\theta_2' \)
4. Performs inverse rotation operation \( R^{(0)}(Q\theta') \) on \(|\text{Sig}\rangle_A\), obtaining \(|Z\rangle\),
5. Performs rotation operation \( R^{(0)} H(Y_j) \) on \(|\varphi_p\rangle \}_A\), obtaining \(|Z'\rangle\)

In step (4), we can see that \(|Z\rangle\) is not equal to \(|Z'\rangle\), because the rotating angle in \(|Z'\rangle\) is \( H(Y)+(S_{\theta_n})_A \), which is not equal to the angle in \(|Z\rangle\) with angle \((W''+hm') \cdot Q\theta')\), which contains only \((S_{\theta_n})_E\) no \((S_{\theta_n})_A\).

**Case (4): E tries to launch a rotating-to-PKA-and-forge (RPAf) attack**

In this aspect, E does steps (1) through (3) in the verification phase by reversely rotating degree \( Q\theta + H(Y) \) on \(|\text{Sig}\rangle \}_A\). This results in \(|\text{Sig}\rangle \}_A\) now have the same degree with \(|\varphi_p\rangle \}_A\). Then, E forges \( m', r_1 \), and replaces all the A’s private related parameters \( hq, Q, X_1, X_2, Y, hw \), with his own secret \((S_{\theta_n})_E\). He then computes \( H(Y) \), produces \( Q\theta' \) and \(|\text{Sig}_A\rangle \)’ according to the following:

\[
E \text{ computes } \quad Q' = H(m', r_1, (S_{\theta_n})_E, X_1', X_2'), \quad X_1'X_2'=(q'-1) (S_{\theta_n})_E+3r', \quad W' = Y'+H(m', r_1, (S_{\theta_n})_E, X_1, X_2), \quad X_1'X_2'=(S_{\theta_n})_A \quad \text{......Eq(1)}
\]

\[
hw' = H(W', Q', X_1', X_2', Y, (S_{\theta_n})_E), \quad \text{...... Eq(2)}
\]

\[
hm' = H(m', r_1', hq', Q', X_1', X_2', Y, hw'), \quad \text{...... Eq(3)}
\]

if \( H(Y') < Y' \), E computes

\[
\theta_1' = Y'-H(Y')
\]

\[
Q\theta' = hm'+Q'X_1'X_2'+\theta_1'
\]

else computes
\[ \theta'_2 = H(Y) - Y' \]
\[ Q0' = hm' + Q' X_1' X_2' - \theta'_2 \]

such that in B’s verification, by rotating the degree of H (Y’) on state \( |\varphi_{pk}\rangle_A \) (which will become \( |Z'\rangle \)) will equal to the state \( |Z\rangle \), which is obtained by reversely rotating \( Q0' \) on \( |\text{Sig}_A\rangle \).

That is, E must find a value \( W' \) in Eq.(1) to fake \( hw' (= H(W', Q', X_1', X_2', Y', (S_\theta_n)_E)) \) used in computing \( hm' \) and subsequently in the \( Q0' \) calculation, as shown in Eq(1), Eq(2), and Eq(3), respectively. However, without the knowledge of \( (S_\theta_n)_E \), E cannot find such \( W' \). Hence, E’ RPAd attack fails.

**Case (5): E tries to launch a linear attack.**

In this aspect, we assume that E wants to forge A’s signature by rotating degree \( k \). Without loss of generality, assume \( k > 0 \). He intends to find a value \( Y' \) to satisfy \( hm' + H(Y') = hm + H(Y) + k \), where \( hm' = H(m', r'_1, hq', Q', X_1', X_2', Y', hw') \), for B’s verification. However, according to the property of cryptographic one-way hash function that it is computationally infeasible to find a pre-image hashing to a specific value \( H(Y) + k \). Even to date, a quantum era, hash function is still an attractive primitive in security protocol design [95]. Thus, we conclude that E’s linear attack fails.

5.2. **Identifiability**

Whenever a verifier checks the signature, he performs the related rotation operation and obtains the quantum state \( |Z\rangle \). If the measurement outcomes of both quantum states \( |Z\rangle \) and \( |\text{Sig}\rangle_A \) are equal, from Section 4.2, we know that A is the real signer. Thus, our scheme has this identifiability feature.

5.3. **Verifiability**

From the analysis in Section 5.1, we know that our quantum signature is unforgeable. This guarantees that the signature is actually from the signer and can be verified by anyone performing the steps as shown in Section 4.2.

5.4. **Non-repudiation**

For the same reasons as stated in section 5.1 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. To sum up, our quantum signature scheme has the following advantages: (1) can resist the forgery attack, (2) is undeniable for the signer, (3) without necessity to specify a specific verifier, and (4) identifiability.

6. **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 Section 5. Then, we discuss the reason why our scheme is outstanding compared with the state-of-the-art and then plan our future research work in section 6.2.

6.1. **Comparisons**

We compare our approach with the other schemes based on the four security attributes of a quantum signature scheme. We summarize them in Table 1.

<table>
<thead>
<tr>
<th>Security requirements</th>
<th>Ours</th>
<th>Kaushik et al.’s scheme [80]</th>
<th>Shi et al.’s scheme [81]</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Ours</td>
<td>Kaushik et al.’s scheme [80]</td>
<td>Shi et al.’s scheme [81]</td>
</tr>
</tbody>
</table>
### 6.2. Discussions

From Table 1, we can see that our scheme is safer than the state-of-the-art. Moreover, it doesn't not need to pre-share any common secret between any parties and thus needn't assign a specific verifier, which is the first attempt in this aspect. And hence more coincide with the reasoning logic of human beings. We anticipate that our method will be globally adopted in the applications in human life to get rid of the possible obstacles which might occur when adopting the other schemes. As for our future work, we know that voting is an important activity in a democratic country.

The current voting system in Taiwan demands that people must go to the prescribed place to vote within the prescribed time. This will cost a lot of resources such as manpower, material resources, time, and money. Moreover, once the voters are too much to be accommodated in the voting place, it is likely that the other people will have to wait for a long time, which might cause them to abandon their voting rights. Therefore, if one can design a quantum voting system, where the people only need to vote online home, then the government can greatly simplify the whole voting process.

After the proposal of our quantum signature scheme, we consider that a voting system is basically a signature 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 adapt the proposed to be applied in 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 blind one, as (1) stated. 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, (4) identifiability, and (5) anonymity, to realize a safe quantum voting system.

### 7. Conclusion

In this paper, we successively presented a publicly verifiable quantum signature scheme. Through cryptanalysis, we confirm that our solution not only resists forgery attacks, but also possess the undeniable and public verifiable functions, which are more suitable for applications in real life than the state-of-the-art. In addition, in view of: (1) quantum computer is the development trend worldwide, (2) the inherent nature of the voting system is basically a signature combined with a blind signature scheme, and (3) the election drawbacks found at the end of 2018 in Taiwan, the future work of this article tries to design a quantum blind signature, which will then be applied to our third future design, a quantum voting system. Totally, how to design a truly secure quantum voting system is the ultimate goal that our series of research will achieve in the future.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>O</th>
<th>X</th>
<th>X</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unforgeability</td>
<td>O</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Non-repudiation</td>
<td>O</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Verifiability</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>Identifiability</td>
<td>O</td>
<td>O</td>
<td>O</td>
</tr>
</tbody>
</table>
References


Shi, Wei-Min, et al. "A scheme on converting quantum signature with public verifiability into


