南華大學科技學院資訊管理學系

碩士論文

Department of Information Management
College of Science and Technology
Nanhua University

Master Thesis

基於非對稱量子密碼不用指定驗證者的量子簽章方案

A Publicly Verifiable Quantum Signature Scheme based on Asymmetric Quantum Cryptography

周芳琪

Fang-Qi Zhou

指導教授：周志賢 博士

Advisor: Jue-Sam Chou, Ph.D

中華民國 108 年 5 月

May 2019

南 華 大 學

資訊管理學系

碩士學位論文

基於非對稱量子密碼不用指定驗證者的量子簽章方案

A publicly verifiable quantum signature scheme based on asymmetric quantum cryptography

研究生：周芳瑛

經考試合格特此證明

口試委員：周志賢

蔡家發

王佳文

指導教授：周志賢

系主任(所長)：

口試日期：中華民國 108 年 5 月 3 日

南華大學資訊管理學系碩士論文著作財產權同意書

立書人：周芳瑛 之碩士畢業論文

中文題目：

基於非對稱量子密碼不用指定驗證者的量子簽章方案

英文題目：

A publicly verifiable Quantum signature scheme based on asymmetric Quantum cryptography

指導教授：周志賢 博士

學生與指導老師就本篇論文內容及資料其著作財產權歸屬如下：

☑ 共同享有著作權

☐ 共同享有著作權，學生願「拋棄」著作財產權

☐ 學生獨自享有著作財產權

學　　生：周芳瑛 （請親自簽名）

指導老師：周志賢 （請親自簽名）

中華民國 108 年 5 月 3 月

南華大學碩士班研究生

論文指導教授推薦函

資訊管理 系碩士班 周芳琪 君所提之論文

係由本人指導撰述，同意提付審查。

指導教授 周志雯

108 年 5 月 3 日

致　　謝

承蒙指導教授周志賢博士，在學生就讀研究所期間的悉心教導與鼓勵，並且教導專業知識與論文的撰寫，不斷給予指導與啟發，並於學生論文撰寫期間，百忙中抽空逐字斧正，使論文得以順利完成，心中萬分感激。在這兩年的研究期間，也要特別感謝南華大學資管系，系上全體教師的。在學期間因有你們的陪伴而增添了不少色彩，也讓我有不斷前進的動力。由於您們的幫助，本論文才得以順利完成，在此一同致上由衷的感謝。

同時也要感謝家人給予的支持，由於您們給我的鼓勵與關懷，讓我能無後顧之憂的完成學業。最後，謹將此論文獻給愛我的家人及所有幫助過我的人，謝謝你們！

周芳琪　謹致於

南華大學資訊管理學系

2019 年　5 月

基於非對稱量子密碼不用指定驗證者的量子簽章方案

學生：周芳琪　　指導教授：周志賢

南　華　大　學資訊管理學系碩士班

摘 要

在 2018 年，Shi 等人表明，Kaushik 等人的量子簽章方案存在缺陷。它遭受了偽造攻擊。他們進一步提出了改進措施，試圖避免這種攻擊。但是，經過檢驗，我們發現他們改進的量子簽章法是可以被否認的，因為驗證者可以冒充簽章者簽署一條訊息。此後，當發生爭議時，他可以辯稱簽章是來自簽章者，而不是他所簽的。為了克服這種缺點，在本文中，我們提出了更進一步的改進，使其成為一個真實可用的量子簽章，可以被公開的非特定驗證者所驗證，因此可以更實際應用於現實生活中。在密碼分析之後，我們確認我們改進的簽章法不僅可以抵禦偽造攻擊，而且是不可否認的。

關鍵詞：不可否認的量子簽章方案、模擬攻擊、量子非對稱密碼、Trapdoor 單向函數、單量子位旋轉加密、可公開驗證簽章

A publicly verifiable quantum signature scheme

based on asymmetric quantum cryptography

Student：Fang-Qi Zhou Advisors：Dr. Jue-Sam Chou .

Department of Information

Management The Graduated Program

Nan-Hua University

Abstract

In 2018, Shi et al 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 signatureis 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 proposed an improvement to make it a practical signature to be publicly verified and can be applied in real life. After cryptanalysis, we confirm that our improvement not only can 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

Directory

論文著作財產權同意書 I
論文指導教授推薦函 II
致　謝 III
摘　要 IV
Abstract V
Directory VI
Chart catalog VII
Table directory VIII
1. Introduction 1
2. Review Kasumk et al.'s quantum signature scheme and Shi et al.'s attacks and improvements 2
2.1. Kaushik et al. quantum signature scheme 2
2.2. Shi et al.'s attacks and improvements 3
3. The problems found in Shi et al.'s scheme 5
4. The proposed quantum signature scheme 5
4.1 Signature phase 6
4.2 Verification phase 6
5. Security analysis 7
5.1. Unforgeability 8
5.2. Identifiability 9
5.3. Verifiability 10
5.4. Non-repudiation 10
6. Comparisons and discussions 10
6.1. Comparisons 10
6.2. Discussions 11
7. Conclusion 12
References 13

Chart catalog

Figure 1 The proposed quantum signature scheme 7
Figure 2 Schematic diagram of the rotation angles in the proposed quantum signature scheme 7

Table directory

Table 1 compares our work with the state-of-the-art 11

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 θ_{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, $|\varphi_{pk}\rangle_{Alice} = \bigotimes_{j=1}^{N} R^{(j)}(S_j\theta_n)\,|0_z\rangle$, together with their common secret θ_{n1} to perform a rotation operation $\bigotimes_{j=1}^{N} R^{(j)}(h_j\theta_{n1})$ 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 propose a publicly verifiable quantum signature scheme based on asymmetric quantum cryptography. 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 comparison results 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. quantum signature scheme

Their signature scheme [80] 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

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>>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 $|0_z\rangle^{\otimes N}$.

(c) Applies the rotation operation $R^{(j)}(S_j\theta_n)_A$ on the quantum state $|0_z\rangle^{\otimes N}$, j=1 to N, to generate the public key of A, $|\varphi_{pk}\rangle_A = \bigotimes_{j=1}^{N} R^{(j)}(S_j\theta_n)_A|0_z\rangle$, 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 $R^{(j)}(h_j\pi)$ on state $|0_z\rangle^{\otimes N}$, getting $|\varphi_{hj}\rangle_A = \bigotimes_{j=1}^{N} R^{(j)}(h_j\pi)|0_z\rangle$.

(c) Uses her private key $(S_j\theta_n)_A$ to perform a rotation operation $R^{(j)}(S_j\theta_n)_A$ on $|\varphi_{hj}\rangle_A$, obtaining the signature $|\varphi^{S}_{hj,sj}(\theta_n)\rangle_A = \bigotimes_{j=1}^{N} R^{(j)}(S_j\theta_n)_A\ |\varphi_{hj}\rangle$ of M, and then sends message M with the signature, $\{M, |\varphi^{S}_{hj,sj}(\theta_n)\rangle_A\}$, to Bob (B) .

(3) **Verification phase**

Upon receiving $\{M, |\varphi^{S}_{hj,sj}(\theta_n)\rangle_A\}$, B performs the verification operation by using the following steps.

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

(b) Performs reverse rotation operation $\bigotimes_{j=1}^{N} R^{(j)}(-h_j\pi)$ on $|\varphi^{S}_{hj,sj}(\theta_n)\rangle_A$, getting $|\varphi_{pk}\rangle'_A = \bigotimes_{j=1}^{N} R^{(j)}(-h_j\pi)\ |\varphi^{S}_{hj,sj}(\theta_n)\rangle_A$.

(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 $R^{(j)}(-h_j\pi)$ on $|\varphi^{s}_{hj,sj}(\theta_n)>_A$, obtaining $|\varphi_{pk}>'_A$.

(b) Chooses another message M' = {m_1', m_2',……,m_{N1}'} of length N, calculates $h'=H(M')$, and forges a signature $|\varphi^{s'}_{hj',sj}(\theta_n)>_A = \bigotimes_{j=1}^{N} R^{(j)}(h_j'\pi)\ |\varphi_{pk}>_A'$.

(c) Sends the message signature pair{M', $|\varphi^{s'}_{hj',sj}(\theta_n)>_A$ } 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 $n_1 >> 1$ 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 $|0_z>^{\otimes N}$, where $\theta_{n1}=\pi/2^{n1-1}$, giving the result $|\varphi_{hj}>_A=\bigotimes_{j=1}^{N} R^{(j)}(h_j\theta_{n1})|0_z>$. 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 $|\varphi^{s}_{hj,sj}(\theta_n)>_A$, instead of $R^{(j)}(-h_j\pi)$, measures and compares both the outcomes to see whether the two quantum states measurement results $|\varphi_{pk}'>_A$ ($=\bigotimes_{j=1}^{N} R^{(j)}(-h_j\theta_{n1})$ on $|\varphi^{s}_{hj,sj}(\theta_n)>_A$) and $|\varphi_{pk}>_A$ 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 θ_{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 n1>>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.(1), he can pretend signer A to sign on the message M'. That is, if the verifier B is malicious, after receiving $\{ M, |\varphi^{s}_{hj,sj}(\theta_n)>_A \}$ from A, B can pretend A to sign on another message M' as follows.

(1) Computes $h=H(M)$ and applies an inverse rotation $R^{(j)}(-h_j\theta_{n1})$ on $|\varphi^{s}_{hj,sj}(\theta_n)>_A$to get $|\varphi_{pk}{}'>_A$,

(2) Chooses another message M' and computes $h'= H(M')$. By performing a rotation operation $\bigotimes_{j=1}^{N} R^{(j)}(h_j{}'\theta_{n1})on|\varphi_{pk}{}'>_A$, B gets $|\varphi^{s'}_{hj',sj}(\theta_n)>$.

(3) Sends $\{ M', |\varphi^{s'}_{hj',sj}(\theta_n) > \}$ 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 θ_{n1} and has her own public key $|\varphi_{pk}>_{\text{Alice}}$, 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 Figure1. Figure2 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) Calculates $H(m, r_1)= q^* (S_j\theta_n)_A+r = W_1$,

$X_1=(q-1)\ S_j$, $X_2=(\theta_n+\frac{r}{q-1}S_j^{-1})$,

$Q=H(H(m, (S_j\theta_n)_A, m, X_1, X_2)$,

$W= QW_1+Qr = Q\ ^*q^*\ S_j\theta_n+ Qr+ Qr= Q(q^*(S_j\theta_n)_A+2r)$,

$QX_1X_2=Q(q-1(S_j\theta_n)_A)+Qr$,

$Y=W-QX_1X_2-(S_j\theta_n)_A=Q(S_j\theta_n)_A+Qr-(S_j\theta_n)_A=(Q-1)(S_j\theta_n)_A+Qr$,

(3) $|Sig\rangle_A$ =Rotates state $|0_z\rangle^{\otimes N}$ to $\bigotimes_{j=1}^{N} R^{(j)}(W_j)|0_z\rangle$.

(4) Sends $\{H(m, S_j\theta_n), m, X_1, X_2, Y, |Sig\rangle_A\}$ to Bob (B) through the classical channel, and $|Sig\rangle_A$ through quantum channel.

4.2 Verification phase

After receiving $\{H(m, S_j\theta_n), m, X_1, X_2, Y, |Sig\rangle_A\}$, B performs the following steps to verify it.

(a) Computes $Q=H(H(m, (S_j\theta_n)_A, m, X_1, X_2)$,

(b) Performs inverse rotation operation $R^{(j)}(Q^*X_1^*X_2)$ on $|Sig\rangle_A$, , obtaining $|Z\rangle$,

(c) Performs rotation operation $R^{(j)}(Y_j)$ on $|\varphi_{pk}\rangle_A$, obtaining $|Z'\rangle$,

(d) 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.

Alice	Bob
Signature Randomly chooses an integer r_1 Computes $H(m, r_1)= q^* S_j\theta_n+r =W_1$, $X_1=(q-1)\ S_j$, $X_2=(\theta_n+\frac{r}{q-1}\ S_j^{-1})$, $Q=H(H(m, S_j\theta_n), m, X_1, X_2)$, $W= QW_1+Qr = Q\ ^*q^*\ S_j\theta_n+\ Qr+\ Qr= Q(q^*(S_j\theta_n)_A+2r)$, $QX_1X_2=Q(q-1(S_j\theta_n)_A)+Qr$, $Y=W-QX_1X_2-(S_j\theta_n)_A=Q(S_j\theta_n)_A+Qr-(S_j\theta_n)_A=(Q-1)(S_j\theta_n)_A+Qr$, $\|Sig\rangle_A=\|0_z\rangle^{\otimes N}$ Rotate to $\bigotimes_{j=1}^{N} R^{(j)}(W_j)\ /\ 0_z\rangle$ $\{H(m, S_j\theta_n), m, X_1, X_2, Y, \|Sig\rangle_A\}$ →	**Verification** Computes $Q=H(H(m, S_j\theta_n), m, X_1, X_2)$, Performs inverse rotation operation $R^{(j)}(Q^*X_1^*X_2)$ on $\|Sig\rangle_A$, obtaining $\|Z\rangle$ Performs rotation operation $R^{(j)}(Y_j)$ on $\|\varphi_{pk}\rangle_A$, obtaining $\|Z'\rangle$ 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.

Figure 1 The proposed quantum signature scheme

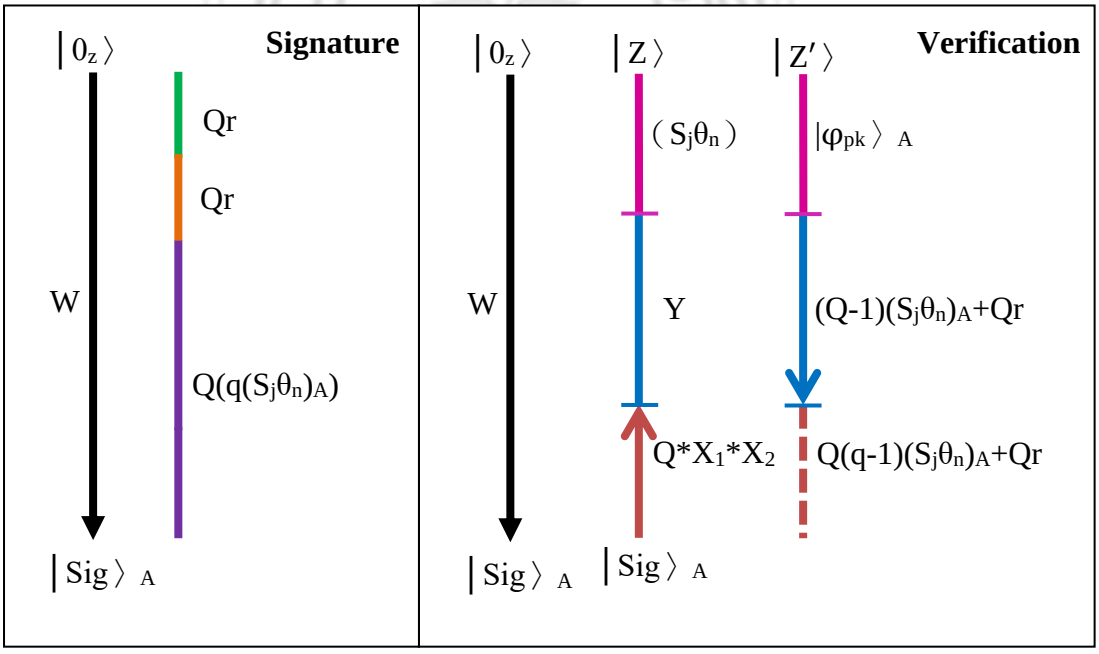

Figure 2 Schematic diagram of the rotation angles in the proposed quantum signature scheme

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{$H(m, S_j\theta_n)$, m, X_1, X_2, Y, $|Sig\rangle_A$ }, 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 two cases to show the reasons why our scheme has the unforgeability merit.

(1) **Attacker E intercepts the signature parameters transmitted by A{$H(m, S_j\theta_n)$, m, X_1, X_2, Y, $|Sig\rangle_A$ }, E only keeps the message $H(m, S_j\theta_n)$ unchanged, because he doesn't know the signer's private key $(S_j\theta_n)_A$, and wants to change the other parameters**.

There are two situations in this case: (a) m is unchanged, and (b) m is changed . But the effects of these two are the same for the attacker, since doesn't have the value of r_1, which yields to all the parameters X_1, X_2, Y, $|Sig\rangle_A$ changed. We take situation (a) as an example. That is, E wants to send{$H(m, S_j\theta_n)$, m, X_1', X_2', Y', $|Sig\rangle_E$} to B for verification. Under this situation, we found that once m is kept unchanged, without the knowledge of r_1 and $(S_j\theta_n)_A$, E cannot have the values q, r, X_1, X_2. That means X_1 and X_2 should also be kept unchanged. Under the case that X_1, X_2 are not modified, this implies that q, r unchanged and value Q also reamins, since $Q=H(H(m,(S_j\theta_n)_A), m, X_1, X_2)$. Then $Y=(Q-1)(S_j\theta_n)_A+Qr$ can't be altered, neither. Totally, all parameters must be kept the same, even for $|Sig\rangle_A$, because the angle W in $|Sig\rangle_A$ equals to $Q(q(S_j\theta_n)_A+2r)$. Equivalently, E cannot change any parameters signed by A. Hence, E's attack fails.

(2) **E tries his best to achieve the goal, regardless of any parameter change in the sent message from the signer.**

E chooses another message m's and a random number r_1' to compute the relative parameters:

(a) Computes $H(m', r_1')=q'(s)=q'(S_j'\theta_n')_E+r'=W_1'$, $X_1'=(q'-1)S_j'$, $X_2'=(\theta_n'+\frac{r'}{(q-1)'}(S_j')^{-1})$,

(b) $Q'=H(H(m', (S_j'\theta_n')_E), m', X_1', X_2')$,

(c) $W'=Q'W'_1+Q'q'(S_j'\theta_n')_E+Q'r'+Q'r'=Q(q'(S_j'\theta_n')_E+2r')$,

(d) $Y'=Q'(S_j'\theta_n')_E+Q'r'-(S_j'\theta_n')_E$.

E replaces all of A's parameters with his own, $\{H(m', (S_j'\theta_n')_E), m', X_1', X_2', Y', |Sig\rangle_E\}$, where $|Sig\rangle_E$ is the resultant state that E rotates an angle W_E on state $|0_z\rangle^{\otimes N}$. E then sends the modified message to B. B will do the followings.

(a) Compute $Q'=H(H(m', (S_j'\theta_n')_E, m', X_1', X_2')$,

(b) Compute $Q'X_1'X_2'=Q'((q'-1)(S_j'\theta_n')_E+r')$,

(c) Performs inverse rotation $R^{(j)}(Q'*X_1'*X_2')$ on $|Sig\rangle_E$, obtaining state $|Z\rangle$ with degree $((q'(S_j'\theta_n')_E+2r')-Q'(q'-1)(S_j'\theta_n')_E+r')=Q'(S_j'\theta_n')_E+Q'r'$,

(d) Performs rotation $R^{(j)}(Y_j')$ on $|\varphi_{pk}\rangle_A$, obtaining $|Z'\rangle$ with degree $(S_j\theta_n)_A+Q'(S_j'\theta_n')_E+Q'r'-(S_j'\theta_n')_E$,

(e) Measures and compares the outcomes to see if $|Z\rangle = ?\ \ |Z'\rangle$.

Although E replaces all the parameters of A with his own, when B checks step (e), he will find that the measured outcomes of both states $|Z\rangle$ and $|Z'\rangle$ are not equal. Because E doesn't know the secrets of A, $(S_j\theta_n)_A$, to prepare $Y'=Q'(S_j'\theta_n')_E+Q'r'-(S_j\theta_n)_A$, rather than the value $Y=Q'(S_j'\theta_n')_E+Q'r'-(S_j'\theta_n')_E$. Therefore, the attack of E fails.

5.2. Identifiability

Whenever a verifier checks the signature, he performs the related rotation operation and obtains the quantum state $|Z>$. If the measurement outcomes of both quantum states $|Z>$ and $|Z'\rangle$ 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 1 compares our work with the state-of-the-art

Security requirements \ Scheme	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

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 cryptanalyses, 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 secondary 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 work.

References

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

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

[3] C. L. Hsu, T. S. Wu, and T. C. Wu, “Group-oriented signature scheme with distinguished signing authorities,” Future Generation Computer Systems, vol. 20, no. 5, pp. 865–873, 2004.

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

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

[6] J. Zhang and J. Mao, “A novel ID-based designated verifier signature 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: delegation of 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 strong designated 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 group signature: a new anonymous proxy signature scheme,” in Proceedings of the 7th International Conference on Machine Learning and Cybernetics (ICMLC’08), pp. 1369–1373, Kunming,China, July 2008.

[13] Z. Shao, “Improvement of identity-based proxy multisignature scheme,” 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 proxy signature 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 multisignature scheme,” Information Sciences, vol. 179, no. 3, pp.292–302, 2009.

[17] A. Yang andW. P. Peng, “A modified anonymous proxy signature with a trusted party,” in Proceedings of the 1st International Workshop 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 a threshold proxy signature scheme,” Computer Standards and Interfaces, 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 proxy verifiably encrypted signature scheme,” Journal of Network and Computer Applications, vol. 33, no. 1, pp. 29–34, 2010.

[21] B. D. Wei, F. G. Zhang, and X. F. Chen, “ID-based ring proxy signatures,” in Proceedings of the IEEE International Symposium on 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 verifier proxy signature schemes,” Cryptography EprintArchiveReport 394, 2008.

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

[25] C. Y. Yang, S. F. Tzeng, and M. S. Hwang, “On the efficiency of non repudiable threshold proxy signature scheme with known signers,” 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 an identity based multi-proxy signature scheme,” Computers and Electrical Engineering, vol. 37, no. 2, pp. 129–135, 2011.

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

[28] Y. Sun, C. Xu, Y. Yu, and B. Yang, “Improvement of a proxy multi-signature scheme without random oracles,” Computer Communications, 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 standard model,” Computer Communications, vol.

34, no. 3, pp. 494–501, 2011.

[30] H. Bao, Z. Cao, and S. Wang, “Improvement on Tzenget al.’s non repudiable threshold multi-proxy multi-signature scheme with shared verification,” Applied Mathematics and Computation, vol. 169, no. 2, pp. 1419–1430, 2005.

[31] J. G. Li and Z. F. Cao, “Improvement of a threshold proxy signature scheme,” 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 secure proxy 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 scheme with 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 signature scheme with proxy signer privacy protection,” Applied Mathematics 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-baseddeniableauthenticationprotocol from pairings,”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, “Erratum to“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, “An electronic 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, “A non-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, “An efficient non-interactive deniable authentication scheme based on trapdoor commitment schemes.”Computer Communications, In Press, Corrected Proof, March 2010.

[50] Lein Harn 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 data using RFID.” in Proceedings of the 3rd ACM Conference on Wireless Network Security (WiSec ‘10), pp. 105–110, March2010.

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

[54] S.Even, O. Goldreich, and A. Lempel, “A randomized protocol for 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-nothing disclosure of secrets.” in Proceedings of the International Conference 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. Naor and B. Pinkas, “Oblivious transfer with adaptive queries,” in Proceedings

of the International Conference on Advances in Cryptology (CRYPTO ‘99), Lecture Notes in Computer Science, pp. 573–590, 1999.

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

[59] M. Naor and B. Pinkas, “Distributed oblivious transfer,” in Proceedings of the International Conference on Advances in Cryptology(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 Symposium on Theory of Computing (FCRC ‘99), pp. 245–254, May 1999.

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

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

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

[64] H. Ghodosi and R. Zaare-Nahandi, “Comments on the ‘m out of 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 oblivious transfer schemes with adaptive and non-adaptive queries.” In Proceedings of the 8th International

Workshop on Theory and Practice in Public Key Cryptography (PKC ‘05), pp. 172–183,January 2005.

[67] J. Zhang and Y.Wang, “Two provably secure k-out-of-n oblivious transfer schemes,” Applied Mathematics 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 Networking and Applications (AINA ‘05), pp. 28–30, March 2005.

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

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

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

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

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

[74] J. Camenisch, G. Neven, and A. Shelat, “Simulatable adaptive oblivious transfer.” in Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, vol. 4515 of Lecture Notes in Computer Science, pp.573–590, 2007.

[75] M. Green and S. Hohenberger, “Blind identity-based encryption and simulatable

oblivious transfer.”Cryptology ePrint Archive 2007/235, 2007.

[76] J. Qin, H. W. Zhao, and M. Q. Wang, “Non-interactive oblivious transfer protocols.” in Proceedings of the International Forum 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 oblivious transfer mechanism based on CRT.”Journal of Network and Computer Applications, vol. 32, no. 1, pp. 226–235, 2009.

[78] X. Ma, L. Xu, and F. Zhang, “Oblivious transfer with timed release receiver’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 quantum digital 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).

[95] Castelnovi, Laurent, Ange Martinelli, and Thomas Prest. "Grafting Trees: a Fault Attack against the SPHINCS framework." International Conference on Post-Quantum Cryptography. Springer, Cham, 2018.

[96] IMRE, Sandor; GYONGYOSI, Laszlo, "*Advanced quantum communications: an engineering approach*", John Wiley & Sons, 2012.

[97] Hassanien, Aboul Ella, Mohamed Elhoseny, and Janusz Kacprzyk, eds. "*Quantum computing: an environment for intelligent large scale real application*, "Springer International Publishing, 2018.

[98] Nielsen, Michael A., and Isaac Chuang. "*Quantum computation and quantum information*." (2002): 558-559.