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

Yalin Chen[1] and Jue-Sam Chou[*2] and Liang-Chun Wang[3] and Yu-Yuan Chou[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 [1], jschou@mail.nhu.edu.tw[2]
Tel: 886+ (0)5+272-1001 ext.56536
[3]Department of Electrical Engineering, National Sun Yat-sen University , Taiwan
b053011015@student.nsysu.edu.tw
[4] The Affiliated Zhongli Senior High School of National Central University
amy53750@yahoo.com.tw

Abstract

In recent years, several cryptographic scholars have proposed quantum blind signature schemes. However, their methods require the signatories and the inspectors to share common keys in advance, which makes them not only complicated in concept, but also suffering deniable problem. Moreover, due to the fact that not everyone can verify the blind signature, it needs to have a designated verifier. In view of Laurent, et al.'s argument that other than the assumption of the pre-image being collision-free, the one-way hash function is an attractive cryptographic component in the post-quantum era when designing a cryptosystem. Inspired by this, we propose a publicly verifiable quantum blind signature scheme based on the hash function. After security analyses, we confirm that our quantum blind signature not only is secure, but also have the needed properties. It includes anonymity, unforgeability, non-repudiation, blindness, public verifiability, and traceability. Hence, we conclude that this approach is better than the state-of-the-art, and is therefore more suitable for applications in real life, such as, mobile payments, quantum voting, or quantum government.

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

1. Introduction

Many cryptography scientists do research in the field of secure digital signatures, ranging from general signature schemes [1-7], proxy signature schemes [8-35] to their variants, for example, signature with designated verifiers, the identifiable identity authentication [36-51], and k-out-of-n oblivious transport protocol [52-80]. All of these methods are mainly for the signer to sign a message, and the signature can be verified by a public verifier or a specifically designated verifier.

In recent years, the vigorous developments of science and technology (especially in the advancement of physical materials and secure communication networks, and in the application of physics, quantum mechanics), have raised the development of quantum cryptography rapidly [81-94]. Between 2009 and 2018, several scholars [95-100] have proposed quantum blind signature schemes. All claims that their scheme can resist quantum attacks. However, each pair of the members must share a secret key in advance, and hence need to specify a designated verifier. The key shared actions make their scheme become complex in concept and somewhat inflexible, because they do not obey to the logic inferring habits of human beings. Therefore, in this study, based on the usage of public key system, we propose a quantum blind signature protocol that can be publicly verified (not limited to specific verifiers as in the state-of-the-art). Our method not only is conceptually clear, but also conform to human thinking logic.

The structure of this paper is as follows: In Section 2, we first describe the feature requirements of a quantum blind signature, then delineate the design components and the system model of our scheme. In Section 3, we present our quantum blind signature. Section 4 performs the security analyses. After that, we discuss our solutions and compare it with the other schemes nowadays in section 5. Finally, a conclusion is given in section 6.

2. Feature Requirements of a Quantum Blind Signature, and Our Design Component and System Model.

2. 1 The properties of a blind signature scheme

As described by Wang [100], a blind signature scheme must have the following characteristics:

(a) Unforgeability: No one else can generate a valid blind signature for a message, except for the legal one.

(b) Non-repudiation: The signer cannot deny the signature he signed.

(c) Verifiability: Anyone can verify the blind signature.

(d) Traceability: Once a dispute has occurred, the signatory can be traced with the help of a trusted third party to identify the original message owner.

(e) Blindness: The signer cannot know the content of the signed message.

2. 2 Our design components

Based on the arguments of Laurent, et al. [101], one-way hash function is a very fascinating cryptographic primitive in the post-quantum era, except for the assumption that the pre-image is collision-free. Therefore, we mainly design our scheme by using the one-way hash function.

2. 3 The system model

(1) The roles

There are four roles in this proposal: (a) The message M's owner A, (b) The blind signature signer B, (c) a non-designated verifier C, and (d) a trusted third party FC to identify the message owner once a dispute occurs.

(2) Overview

In the design, we first blind the intended signed message M by adding a random number, which becomes M_A. M_A is then transmitted to signer B to blindly sign on it, obtaining $|BSig\rangle_B$. $|BSig\rangle_B$ is passed back to A for her unblinding, obtaining $|uBS\rangle_B$. After that, anyone can verify $|uBS\rangle_B$ to see whether or not $|uBS\rangle_B$ is B's legal signature on message M. Once a dispute occurs, the fair third party FC can assist to trace the owner of the original message, ID_A. Prior to this, B should send A's blind message M_A, A's identity ID_A, and some of the intermediate process parameters to the FC storage, so that when a dispute happens, M's owner ID_A can be traced.

(3) Theoretical basis

This design uses a simple mathematical equation $w=(S_j\theta_n)_B \cdot q+r$, where w is the angle at which the quantum state of the signature is rotated from the $|o\rangle_z$ state, and $(S_j\theta_n)_B$ is B's private key to which his public key quantum state $|\varphi_{pk}\rangle_B$ is mapped, q is the quotient, and r the remainder. In the equation, $(S_j\theta_n)_B$ is only known to B, q and r are thus unknown to the others. Then, r is embedded into Y and W, which both are the intended signed message M's relative parameters. After that, these two are returned to the message owner for unblinding. Once completed, they are passed to any non-specific verifier C for the signature verification. Below, we will analyze the probability of guessing r without the knowledge of $(S_j\theta_n)_B$, q, and w. That is, the equation $r=w-(S_j\theta_n)_B \cdot q$ has three unknown variables. Finding r is equivalent to solve the equation with these three unknown variables. Therefore, the maximal possibility of obtaining value r is by directly guessing. Assuming that all parameters are of a fixed length, n bits. Its probability is thus $\frac{1}{2^n}$. For the same reason, the maximum probability of guessing w is 2^{-n} as well. Hence, as long as n is large enough, the probability can be ignored.

3. The Quantum Blind Signature Scheme

Because our scheme needs not assign a specific verifier, anyone (but only one can verify it, because the quantum state cannot be copied due to the physical property of non-cloning theorem, except that each member prepares his public key quantum state many times [102, 103]) can verify the signature. Naturally, in this paper, we assume that each signer prepares one quantum public key for each signature generation.

In the previously proposed quantum blind signature schemes, the signer and the verifier should share a common secret key in advance, which we think is not a good idea. Because this will result in adding the complexity in maintaining the non-repudiation of the designed system. Moreover, they all need to specify a specific verifier. This may seem too rigid and not general enough in practical applications. Based on the above two observations, this study designs a quantum blind signature scheme that not only need not require the designation of a specific verifier, but also have the non-repudiation property. We roughly describe it as follows. The detail will be shown in section 3. 1 through 3. 4.
Alice (A) passes a message to Bob (B) for Bob's signing on it blindly, so A must first blind his message and then send it to B. Once B has completed blind signing, the blind signature will be returned to A for her unblinding. Finally, A passes the unblind message to C (anyone) for verification. In the proposed scheme, we use the same key generation phase as in Kaushik et al.s' quantum signature [81]. That is, we assume each user has its own public/private key pair ($|\varphi_{pk}\rangle$ / $S_j\theta_n$). We present our proposal using the following four stages. The steps are also shown in Fig. 1 and Fig. 2. Fig. 3 is a schematic view of the rotation angles in Fig. 1 and 2, respectively.

3. 1. Initial stage

A performs the following steps:
1. Randomly picks a random number r_1,
2. Calculates $M_A=r_1+H(m)$, $sh_A=H(M_A, (S_j)_A)$, $SM_A=M_A+sh_A$.

He passes SM_A and sh_A to B, for B to sign on the blind message M_A.

3. 2. The blind signature phase

After receiving the blind messages SM_A and sh_A transmitted by A, B performs the following steps to do the blind signature phase. For abreviation, we denote reverse rotation operation as rro, rotation operation as ro, $D_A=(S_j\theta_n)_A$, and $D_B=(S_j\theta_n)_B$. We also demonstrate it in Figure 1.

(1) Calculates $M_A=SM_A-sh_A$

(2) Randomly picks a random number r_2

Calculates $H(M_A, r_2)=q(S_j\theta_n)_B+r=W_1$

$$X_1=(q-2)(M_A)S_j,\ X_2=(\theta_n+r(q-2)^{-1}S_j^{-1})$$

$$Q=(H(H(M_A, (S_j\theta_n)_B), M_A, X_1, X_2)$$

$$X_1*X_2=(q-2)M_A(S_j\theta_n)_B+rM_A$$

$$QX_1X_2=QM_A((q-2)(S_j\theta_n)_B+r)=r_1Q((q-2)(S_j\theta_n)_B+r)+H(m)Q((q-2)(S_j\theta_n)_B+r)$$

$$W=(QW_1+2Qr)M_A+(S_j\theta_n)_B=Q(q(S_j\theta_n)_B+3r)M_A+(S_j\theta_n)_B=r_1(Qq(S_j\theta_n)_B+3Qr)+H(m)(Qq(S_j\theta_n)_B+3Qr)+(S_j\theta_n)_B$$

$$Y_B=W-QX_1X_2-(S_j\theta_n)_B=r_1Q(2(S_j\theta_n)_B+2r)+H(m)Q(2(S_j\theta_n)_B+2r)$$

$$K=Q*(2(S_j\theta_n)_B+2r)$$

where H represents a one-way hash function.

(3) Performs a rotation operation $R^{(j)}(W_j)$ on $|\varphi_{pk}\rangle_A$, where j = 1 to N, obtaining $|Z\rangle_B$.

(4) Compute $P_1=H(H(M_A, (S_j\theta_n)_B), M_A, Y_B, K, \theta)$

(5) If $H(Y_B)<Y_B$

Computes $\theta_1=Y_B-H(Y_B)$, $\theta=-\theta_1$, $Q\theta=-QX_1X_2+\theta$

Else Computes $\theta_2=H(Y_B)-Y_B$, $\theta=\theta_2$, $Q\theta=-QX_1X_2+\theta$

(6) Performs ro $R^{(j)}(P_1+Q\theta)$ on $|Z_B\rangle$, obtaining $|BSig\rangle_B$

(7) Transfers $\{M_A, SM_A, Y_B, H(M_A, (S_j\theta_n)_B), P_1, K, \theta\ |BSig\rangle_B\}$ to A for unblinding. Moreover, B also transmits $\{ID_A, M_A, Y_B\}$ to the FC storage for preserving the traceability.

3. 3 Unblinding phase

After receiving the message $\{M_A, SM_A, Y_B, H(M_A, (S_j\theta_n)_B), P_1, K, \theta, |BSig\rangle_B\}$ transmitted from B, A performs the following unblinding steps.

(1) Calculates $M'_A=SM_A-H(M_A, (S_j)_A)$ and compare to see if $M'_A=?M_A$.
If yes, continue with the following steps; otherwise, rejects.

(2) Computes $P'_1=H(H(M_A, (S_j\theta_n)_B), M_A, Y_B, K, \theta)$, if it equals to P_1, continues.

(3) Performs ro $R^{(j)}(H(Y_B)_j+P_{1j}+(S_j\theta_n)_{Aj})$ on $|\varphi_{pk}\rangle_B$, obtaining $|Z'\rangle$.

(4) Measures both states $|BSig\rangle_B$ and $|Z'\rangle$, compares the outcomes to see if they are equal. If they are, A accepts and continues.

(5) Randomly selects r_k Computes $Y_{A2}=(K-r_1)+2(S_j\theta_n)_A, Y_{A3}=H(m)(r_1)-2H(m)(S_j\theta_n)_A$

$+(S_j\theta_n)_A+r_k$.

(6) Computes $Y_{A4}=H(m)Y_{A2}+Y_{A3}=H(m)(K-r_1)+2(S_j\theta_n)_A)+H(m)r_1-2H(m)(S_j\theta_n)_A+(S_j\theta_n)_A+r_k=H(m)K+r_k+(S_j\theta_n)_A$,

(7) Computes $P_2=H(H(m),Y_{A2},Y_{A3},Y_{A4})$

(8) Perform rro,$R^{(j)}(P_1+\theta+r_1K)$ then r.o $R^{(j)}(P_2+r_k)$ on $|BSig\rangle_B$, obtaining $|uBS\rangle_B$ with degree $Y_{A1}=(S_j\theta_n)_A+(S_j\theta_n)_B+Y_B-r_1K+P_2+r_k=(S_j\theta_n)_A+(S_j\theta_n)_B+H(M)\cdot K+P_2+r_k$

(9) Transmits { $H(m)$, Y_{A2}, Y_{A3}, $|uBS\rangle_B$, P_2 } to C

(10) A transmits { Y_B, $H(m)$, $|uBS\rangle_B$ } to FC for preserving the traceability.

3. 4 Signature verification stage after unblinding

After receiving the unblinded signature message {$H(m)$,Y_{A2}, Y_{A3}, $|uBS\rangle_B$, P_2} from A, C performs the following steps to verify the unblind signature $|uBS\rangle_B$.

(1) Computes $Y_{A4}=H(m)\cdot Y_{A2}+Y_{A3}=H(m)K+r_k+(S_j\theta_n)_A$,

(2) Computes $P_2=H(H(m),Y_{A2},Y_{A3},Y_{A4})$

(3) Performs ro $R^{(j)}(Y_{A4}+P_2)$ on $|pk\rangle_B$, obtaining $|Z'\rangle_B$

(4) Compares $|uBS\rangle_B$ with $|Z'\rangle_B$, if they are equal, accepts.

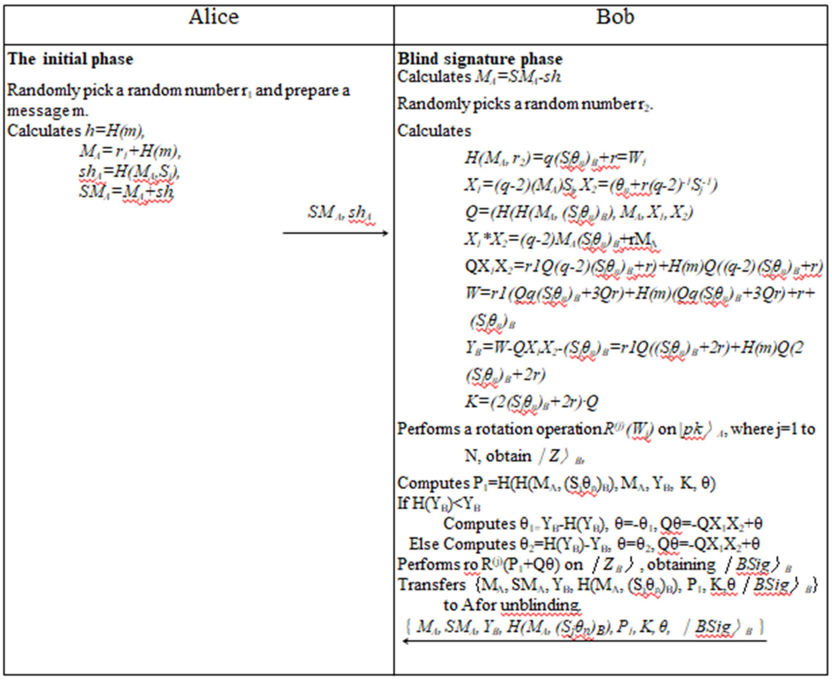

Figure 1. Quantum blind signature (blind signature phase)

Alice	Charile
Unblind phase Calculates $M_A'=SM_A- H(M_A, S_j)=?M_A$ Computes $P'_1 =H(H(M_A, (S_j\theta_n)_B), M_A, Y_B, K, \theta)$, if it equals to P_1, continues. Performs ro $R^{(j)}(H(Y_B)_j+P_{1j}+(S_j\theta_n)_{Aj})$ on $\|\varphi pk\rangle_B$, obtaining $\|Z'\rangle$. Measures both states $\|BSig\rangle_B$ and $\|Z'\rangle$, compares the outcomes to see if they are equal. If they are, A accepts and continues. Randomly selects r_k and calculates $Y_{A2}=(K-r_1)+2(S_j\theta_n)_A, Y_{A3}=H(m)(r_1)-2H(m)(S_j\theta_n)_A+(S_j\theta_n)_A+r_k$ /* $Y_{A2}+Y_{A3}=H(m)K+r_k$ */ Calculates $Y_{A4}=H(m)Y_{A2}+Y_{A3}=H(m) \cdot K+r_k+(S_j\theta_n)_A$ $P_2=H(H(m),Y_{A2},Y_{A3},Y_{A4})$ Performs rro $R^{(j)}(P_1+\theta+r_1K)$ then r.o $R^{(j)}(P_2+Y_k)$,on $\|BSig\rangle_B$, obtaining $\|uBS\rangle_B$ with degree $Y_{A1}=(S_j\theta_n)_A+(S_j\theta_n)_B+Y_B-r_1K+P_2+r_k=(S_j\theta_n)_A+(S_j\theta_n)_B+H(m)\cdot K+P_2+r_k$ Passes $\{H(m), R\}$ to FC, and transmit to C $\{H(m), Y_{A2}, Y_{A3} \|uBS\rangle_B, P_2\}$ →	**Verification phase** (1) Computes $Y_{A4}= H(m)\cdot Y_{A2}+Y_{A3}=K\ H(m)+ r_K+(S_j\theta_n)_A$, (2) Computes $P_2=H(H(m), Y_{A2}, Y_{A3}, Y_{A4})$ (3) Performs ro $R^{(j)}(Y_{A4}+P_2)$ on $\|pk\rangle_B$, obtaining $\|Z'\rangle_B$ (4) Compares $\|uBS\rangle_B$ with $\|Z'\rangle_B$, if they are equal, accept.

Figure 2. Quantum blind signature (unblining and verification phase)

Figure 3 through 5 show the semantic diagrams of the rotation angles in the proposed protocol.

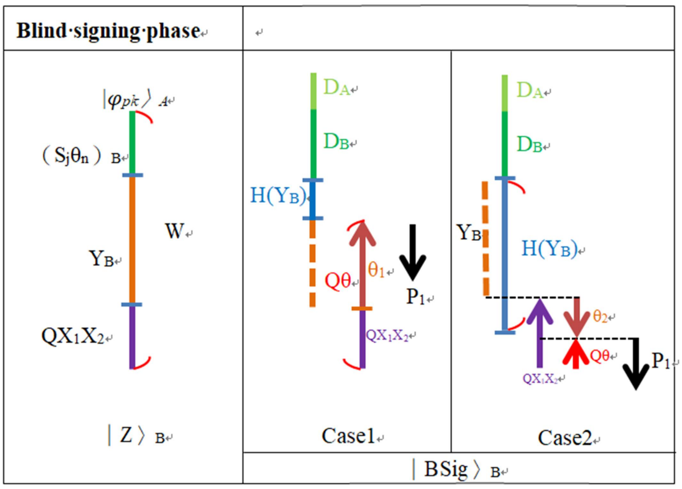

Figure3. Semantic diagram of rotation angles in Blind signing phase

4. Security Analysis

In this section, based on the needed characteristics of a blind signature mentioned in Section 2, we analyze them to see the reason why our proposed can satisfy these properties as follows.

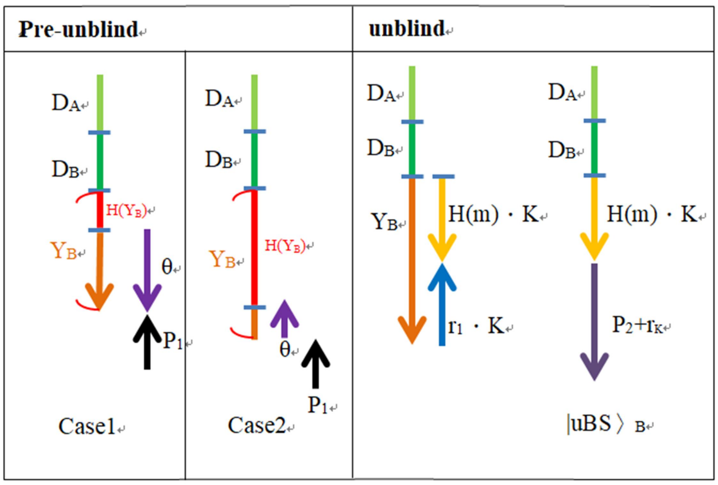

Figure 4. Semantic diagram of rotation angles in unblind phase.

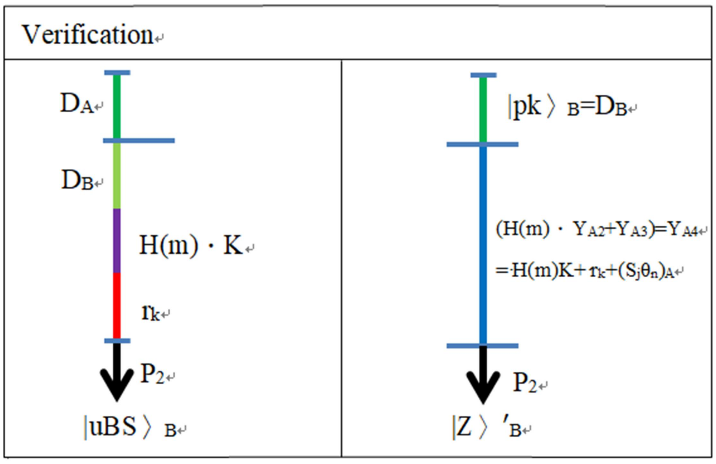

Figure 5. Semantic diagram of rotation angles in verification phase

4. 1 Unforgeability

Our scheme is unforgeable. We explore this property by considering the following three cases.

(1) **When E wants to pretend A to send B M_A'**

For this purpose, E will send B $SM_A'$and sh_A', where $SM_A'= M_A'+sh_A'$. But when B returns SM_A', M_A' to A, according to the description in Section 3.3, A will find his M_A does not equal to $(SM_A'-H(M_A', (S_j)_A)$. This is because E does not know A's secret $(S_j)_A$. According to the characteristics of the hash function, E cannot find M_A' and S_j' in feasible time, so that $SM_A'- M_A'=sh_A'=sh_A=H(M_A', S_j')$. Therefore, E's attack cannot succeed.

(2) **After signature phase, if E intercepts the message from B to A, {$|BSig\rangle_B$}, M_A, SM_A, $H((M_A), (S_j\theta_n)_B)$, Y_B, P_1, θ, K} , E cannot succeed in altering any parameters. We explain this as follows.**

From the above mentioned in (1), we know that E cannot alter SM_A, Sh_A since he doesn't know $(S_j)_A$. In addition, E cannot modify any one of the parameters,$H(M_A, (S_j\theta_n)_B)$, Y_B, P_1, θ, K neither, because $P_1 = H(H(M_A), (S_j\theta_n)_B), M_A, Y_B, K, \theta)$ is embedded in $|BSig\rangle_B$. Without loss of generality, we take modifying Y_B to Y_B' as an example. E computes $P_1'=H(H(H(M_A), (S_j\theta_n)_B, M_A, Y_B', K, \theta)$. Although, E can change Y_B to Y_B' and send{ $|BSig\rangle_B'$, M_A, SM_A, $H(M_A)$, $(S_j\theta_n)_B)$, Y_B', P_1', θ, K}to A. However, without the knowledge of A's secret D_A, E cannot correctly generate $|BSig\rangle_B'$ such that when performing ro $R^{(j)}(H(Y_B')_j+P_{1j}'+D_A)$ on $|\varphi_{pk}\rangle_B$, the state measurement outcome will equal to $|BSig\rangle_B'$, as performed by A in Section 3.3, due to E doesn't have the knowledge of W to construct $|Z\rangle_B$, and QX_1X_2 to yield correct Qθ in generating $|BSig\rangle_B'$ in steps (3) through (6) of Section 3.2 to be equally compared in step (4) of Section 3.3. Even when E lauches a linear attack, which we define as E modifies Y_B to Y_B' to satisfy $H(Y_B')=H(Y_B)+k$. And makes a ro $R^{(j)}(k)$ on $|BSig\rangle_B$. However, when E does this, he will be detected, because E cannot find Y'_Bs such that $H(Y_B')=H(Y_B)+k$ due to the property of cryptographic one way hash function.

(3) **After the unblinding phase, it is assumed that attacker E intercepts the message {*H(m)*, $|uBS\rangle_B$, Y_{A2}, Y_{A3}, P_2} which Alice sends to Charlie for verifying the unblind signature $|uBS\rangle_B$, and changes some of the parameters of its own.**

Still, attacker E cannot succeed, neither. We use the following two cases to explain the unforgeable reasons.

(a) E only conservatively chooses another message H(m') to replace the original H(m), hoping that this can successfully forge the signature of B on H(m').

In this case, E only changes H(m) to H(m'), keeps the other parameters unchanged. This will lead P_2 to change as well, because $Y_{A4}'=H(m')Y_{A2}+Y_{A3}$ and $P_2'=H(H(m'), Y_{A2}, Y_{A3}, Y_{A4}')$. E transmits{$H(m')$, $|uBS\rangle_B$, Y_{A2}, Y_{A3}, P_2'}to verifier Charlie. Assume that E computes $Y_{A4}'=H(m')Y_{A2}+Y_{A3}$ accordingly. However, the state $|Z'\rangle_B$ he obtains will not equal to $|uBS\rangle_B$ after C has done step (4) in Section 3.4. From this, we can easily see that E cannot pass Charlie's verification. Therefore, E's attack fails.

(b) E tries his best to achieve his goal, regardless of whether or not the parameters change scale is large.

E tries his best to replace all the parameters in the intercepted message with his own, $\{H(m'), |uBS\rangle_B', Y_{A2}', Y_{A3}', P_2'\}$ and computes $Y_{A4}'=H(m')Y_{A2}'+Y_{A3}'(\neq H(m')\cdot K+r_k+D_A)$, $P_2'=(H(M'),Y_{A2}',Y_{A3}',Y_{A4}')\}$, and passes them, to C for verification. However, we can easily see that after C has done step (4) in section 3.4, C will find the equation does not hold. Because Y_{A2} and Y_{A3} are set by A to deduce Y_{A4} which equals $H(m)\cdot K+r_k+(S_j\theta_n)_A$. E has not the knowledge of A's secret $(S_j\theta_n)_A$, K, and r_k to correctly construct Y'_{A4} which is computed by $H(m')\cdot Y_{A2}'+Y_{A3}'$. Therefore, E cannot accurately execute step (3). Hence, step(4) will fail.

From the above security analyses, we have proved that the proposed scheme can resist forgery attacks.

4. 2 The signer cannot deny the message he signed

B can't deny that $|uBS\rangle_B$ is the signature he signed, because the state $|z'\rangle_B$ in step (3) of Section 3.4 is finally measured and compared with the resultant measurement outcome of state $|uBS\rangle_B$.

4. 3 Anyone can verify the validity of the blind signature

Anyone, who we named Charles in this proposal, only needs to perform the steps shown in Section 3. 4 to see whether or not $|uBS\rangle_B$ is B's valid signature on H(m), without the necessity to pre-share any information between any parties. So, our scheme possesses this property.

4. 4 Traceability

Once there is a dispute, signer B simply needs to present Y_B to FC, FC can then search Y_B in the database to find the message H(m) owner, ID_A.

4. 5 blindness

Because of the random number r_1 added by A, signer B could not know what the original message is from M_A and all the parameters transmitted through the open network. Thus, our scheme satisfies this property.

5. Discussions and Comparisons

In this section, we discuss our proposed scheme in the aspect of applications. Then, compare it with the state-of-the-art to show the reason why our scheme outperforms the others.

5. 1 Discussions

This research uses asymmetric quantum public key system to design a quantum blind signature. Through the security analyses, we conclude that our scheme satisfies the security requirements of such a protocol. They are unforgeability, non-repudiation, verifiability, traceability, and blindness which stresses that the signer cannot know what the original of the signed message is. Therefore, our solution can be applied to the real life worldwide in several applications which need the behavior of a blind signature, such as quantum money, quantum government, and quantum voting, etc.

5. 2 Comparisons

Compared with the other quantum blind signature schemes proposed, only our method is purely designed with asymmetric quantum public key, which makes our method satisfy all the properties of a quantum blind signature as mentioned in Section 4. In addition, the concept of our proposal is simple and obeys the way of human beings thinking logic. In summary, our method is easy to understand and meets the five characteristics of such a signature scheme. Below, we use Table 1 to list the comparison results among our scheme and the state-of-the-art.

Table 1: Comparison with other blind signature schemes

Methods	Asymmetric	Meet the five needed properties of a quantum blind signature
Ours	✓	✓
[95]	×	×
[96]	×	×
[97]	×	×
[98]	×	×
[99]	×	×

From Table 1, we know that our approach is superior to the other similar solutions today.

6. Conclusion

In this paper, we presented a publicly verifiable quantum blind signature scheme. After security analysis, we confirmed that our solution not only resist forgery attacks, but also possess the properties of unforgeability, non-repudiation, verifiability, traceability, and blindness. Compared with the other blind signature proposed, our solution needs not to specify a specific verifier. Anyone can verify where the blind signature from. Therefore, it is more suitable for the applications in real life than the state-of-the-art.

7. 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 scheme for ECC-based anonymous signcryption,” Computer Standards and 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—Transactions on Fundamentals of Electronics, vol. E79-A, no. 9, pp. 1338–1354, 1996.

[9] R. Lu, Z. Cao, and Y. Zhou, “Proxy blind multi-signature scheme without a secure channel,” Applied Mathematics and Computation, 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 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 anonymous proxy signature scheme with provable security," Computer Standards 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 and W. 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 verifier proxy signature scheme without random oracles," Computers and 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 secure multi-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 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 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,"Concurrent zero-knowledge."Proceedings of 30th ACMSTOC'98, 1998, pp. 409–418.

[37]Y.Aumann,M.Rabin,"Efficient deniable authentication of long messages."Int. Conf. on Theoretical Computer Science in Honor of Professor Manuel Blum'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 Internet Protocols."11th International Workshop on Security Protocols, Cambridge （UK）, April 2003.

[40] C. Boyd&W. Mao,"Key agreement using statically keyed authentication." Applied Cryptology and Network Security（ACNS'04）, LNCS 3089, pp.248-262.

[41]Z.Shao,"Efficient deniable authentication protocol based on generalized ElGamal signature scheme."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,"An efficient ID-based deniable authentication protocol frompairings,"Proceedings of the 19th International Conference on Advanced Information Networking and Applications（AINA'05）, IEEE, 2005.

[45]Wei-Bin Lee, Chia-Chun Wu and Woei-JiunnTsaur,"A novel deniable

authentication protocol using generalized ElGamal signature scheme," 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] 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, "Privacy preserving computation 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. Bellare and S. Micali, “Non-interactive oblivious transfer and application,” in Proceedings of the International Conference on Advances in Cryptology （CRYPTO ‘89）, vol. 435 of Lecture Notes in Computer Science, pp. 547–557, 1989.

[58] 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.

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

[60] 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.

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

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

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

[64] 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 of Lecture Notes in Computer Science, pp. 395–405, 2002.

[65] 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.

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

[67] 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.

[68] 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.

[69] 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.

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

[71] 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.

[72] 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.

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

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

[75] J. Camenisch, G. Neven, and A. Shelat, “Simulatableadaptiveoblivious 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.

[76] M. Green and S. Hohenberger, “Blind identity-based encryption and simulatable oblivious transfer.”Cryptology ePrint Archive 2007/235, 2007.

[77] 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.

[78] 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.

[79] 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.

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

[81] 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）

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

[83] 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.

[84] 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.

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

[86] Wen, Xiaojun, et al. "A weak blind signature scheme based on quantum

cryptography." Optics Communications 282.4 （2009）: 666-669.

[87] 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.

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

[89] 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.

[90] 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.

[91] 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.

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

[93] 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.

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

[96] Tian-Yin, Wang, and Wen Qiao-Yan. "Fair quantum blind signatures." Chinese physics B 19.6 (2010): 060307.

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

[98] Shi, Wei-Min, et al. "A new quantum blind signature with unlinkability." Quantum Information Processing 14.8 (2015): 3019-3030.

[99] Srinath, M. Seshadri, and Venkatachalam Chandrasekaran. "Isogeny-based Quantum-resistant Undeniable Blind Signature Scheme." IACR Cryptology ePrint Archive 2016 (2016): 148.

[100] Xu, Rui, et al. "Quantum group blind signature scheme without entanglement." Optics Communications 284.14 (2011): 3654-3658.

[101] 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.

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

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