Quantum Group Proxy Digital Signature based on Quantum Fourier Transform by Using Blinded and Non Blinded Trent

İhsan YILMAZ

Çanakkale Onsekiz Mart University, Engineering Faculty,Computer Engineering Department
e-mail: iyilmaz@comu.edu.tr

Abstract—In this study, quantum proxy group signature protocol based on the Quantum Fourier Transformation (QFT) is suggested. In this protocol, QFT is used to share signature with group members. So all proxy group members know only their part of the signature information which are encrypted output of the QFT. This improves the security of the protocol. In addition, the security of the quantum proxy group signature is provided by using reorder QFT output qubits with permutation of the Trent, blinded and non-blinded . The security analysis expresses higher efficiency, effective secret key usage and security of the proposed protocol.

Keywords—Quantum cryptography, Quantum group signature, Quantum fourier transformation.

1. Introduction

There are difficulties in application of quantum technologies because quantum states interact quickly with the environment. Since, neutrinos are not effected by the external influences, designing quantum computers using neutrinos will be much more useful. Quantum computers have many advantages such as super position and entanglement according to classical computers. In this respect, there are many applications of quantum information technologies. One of them is quantum cryptography.

Classical cryptography techniques use some assumptions about mathematically hard problems to obtain security and create some communication protocols. However, these hard problems can be easily solved with the quantum computer and quantum algorithms [1], [2], [3].

The aspects of the quantum mechanics were adopted to improve the security of the cryptography. So, quantum cryptography research area has been developing. Especially, secure communication based on quantum cryptography is extremely important in quantum cryptography.

Quantum key distribution (QKD) has been developed instead of the classical version [4]. Ekert [5] also designed QKD based on the Bell's theorem. Gao [6] proposed quantum key distribution protocol based on entanglement swapping. Mayers [7] described unconditional security of the QKD.

Quantum Secret Sharing (QSS) is another concept and it is used to share data between participants in securely way. Cleve et. al [8] defined (k, n)

threshold scheme to share a quantum secret. Hillery et al. [9] defined a quantum sharing mechanism based on GHZ-states. Chen et. al [10] presented a three-party quantum secret-sharing by using GHZ-states. Huang et. al. [11] used Quantum Fourier Transform(QFT) to share secret.

Besides these developments, quantum cryptography techniques are also applied in the digital signatures. Gottesman and Chuang [12] were firstly presented quantum digital signature protocol. Buhrman et. al. [13] defined quantum finger prints to compare string which is very useful in the quantum digital signatures. Zeng and Keitel [14] suggested an arbitrated quantum signature scheme which uses symmetrical quantum keys, GHZ-states and quantum one-time pads [15]. Lee et. al [16] also proposed an arbitrated quantum digital signature scheme with message recovery. Li et. al [17] proposed Bell-states version of the protocol of Zeng and Keitel [18].

Chaum [19] has firstly defined the concept of the group signatures. In these signatures, some members of the group can sign the messages. Membership authentication schemes such as E-payment systems [20] can be generalized as group signatures.

Yang [21], [22] proposed threshold proxy group signature scheme. Shi et. al [23] analyzed Yang and Wen's quantum proxy group signature [24] and proposed some methods to improve the security of the protocol.

Wen et. al [25] presented a group signature protocol based on the quantum teleportation. Then Wen [26] also defined an e-payment system which uses proposed group signature scheme [27].

Shi et. al [26] proposed multi-party quantum proxy group signature based on QFT transform. The group members cooperate to sign the message with QFT with authorization of the owner. These group members use QFT^{-1} to restore the message with authorization of the receiver. All participants use quantum circuits to perform all operations.

In this study, quantum proxy group signature protocol based on the QFT is suggested. In this protocol, QFT is used to share signature with group members. The paper can be outlined as follows; in Sect.2, basic concepts of QFT are explained. In Sect.3, base stages of the protocol are introduced. In Sect.4, the blinded version of the group signature protocol is defined. In Sect.5, the security analysis of the protocol based on forgery and disavowal concepts are given. In the conclusion, some results are discussed.

2. Quantum Fourier Transform

Quantum Fourier transform is a quantum version of classical discrete Fourier transform [21]. The QFT transform of an orthonormal basis set $|0\rangle, |1\rangle, ..., |N-1\rangle$ can be defined as follows [21]:

$$|x\rangle = \frac{1}{\sqrt{N}} \sum_{y=0}^{N-1} e^{2\pi i xy/N} |y\rangle \qquad (1)$$

If we define QFT of n qubits, then $N = 2^n$ and orthonormal basis set is $|0\rangle, |1\rangle, ..., |2^n - 1\rangle$. The $|x\rangle$ state can be written in binary form as $x = x_0 x_1 ... x_{N-1}$. The circuit of Quantum Fourier Transform for x can be seen in Fig.1. The $|x\rangle$ state is transformed into the phase of qubits which are results of the QFT transform.

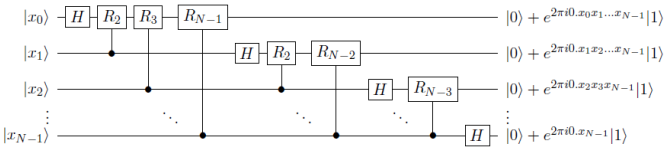

Fig. 1. Quantum Fourier Transform Circuit QFT

3. Group Signature Protocol with QFT

The participants of the protocol are Alice, Bob, Trent and proxy group members $\{G_1, G_2, ..., G_N\}$. Alice would like to send data $m = \{m_0 m_1 ... m_{N-1}\}$,$m_i \in \{0, 1\}$ with her signature of m to Bob. Alice can cooperate some group members $G_i \in \{G_1, G_2, ..., G_N\}$ to create her signature. Trent is assumed as a group manager of the protocol and he is trusted. Trent manages some communication to provide security of the protocol. Bob can obtained data m and verify the signature of the data with the help of these group members and Trent. The protocol can be described with following phases.

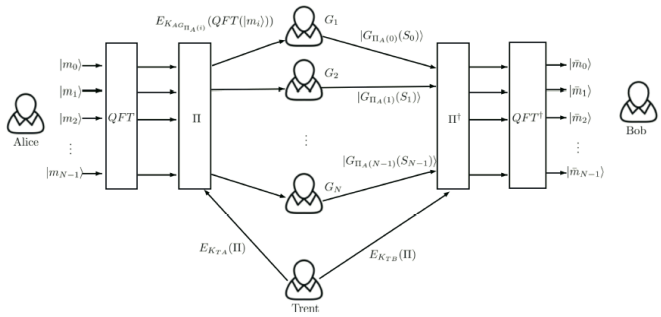

Fig. 2. Proxy Group Signature With QFT

3.1. Initialization Phase

1) Alice shares secret keys $K_{AG_i}, i = 1..N$ with group members G_i and K_{AB} with Bob. Bob shares secret keys $K_{G_iB}, i = 1..N$ with group members G_i. Also Trent shares secret key K_{TA} with Alice and secret key K_{TB} with Bob. Participant's secret keys $K_{AB}, K_{TA}, K_{TB}, K_{AG_i}, K_{G_iB}, i = 1..N$ are obtained by using quantum key distribution(QKD) protocol [3]-[5]. Mayers [7] showed unconditionally security of the QKD protocol. The secret keys are used to encrypt quantum data to prevent any attackers.The encryption algorithm is given in Eq. 9. The length of the all keys are $|K| = 4N$. The method of using secret keys can be defined as follows.
The length of the all data to be sent may be larger than N. In this case, the data can be divided into N length parts. Each part can send in different sessions. Every participant of the protocol uses 4-bits of the owned secret key to encrypt quantum data.
   a) $K_{AB}, K_{TA}, K_{TB}, K_{AG_i}, K_{G_iB}, i = 1..N$ secret keys are only once created. Then the secret keys can be divided into 4-bit pieces. These different pieces of the secret keys can be used in encryption respectively for consecutive sessions by participants.
   b) Different $K_{AB}, K_{TA}, K_{TB}, K_{AG_i}, K_{G_iB}, i = 1..N$ secret keys are created for every different sessions. Every created secret keys can be divided into 4-bit pieces. The piece corresponding to the session number can be used in encryption by participants.
2) Alice expresses her data m with quantum computational bases as $\{0 \rightarrow |0\rangle, 1 \rightarrow |1\rangle\}$. We assume that the length of the m is $|m| = N$.

$$|m\rangle = \otimes_{i=0}^{N-1} |m_i\rangle \tag{2}$$

   Where $|m_i\rangle \in \{|0\rangle, |1\rangle\}$.
3) Trent creates a permutation $\Pi : \{1, 2, ..., N\} \rightarrow \{1, 2, ..., N\}$ as follows:

$$\Pi = \begin{bmatrix} 1 & 2 & ... & N \\ \Pi(1) & \Pi(2) & ... & \Pi(N) \end{bmatrix} \tag{3}$$

   Trent creates encrypted versions of that permutation as follows:

$$\Pi S_A = E_{K_{TA}}(\Pi) \quad (4)$$

$$\Pi S_B = E_{K_{TB}}(\Pi) \quad (5)$$

Then, Trent sends ΠS_A to Alice by using authenticated classical channel or quantum channel.

4) Alice decrypts ΠS_A and obtains Π_A.
5) Alice applies QFT to her data ($\otimes_{i=0}^{N-1} |m_i\rangle$) and obtains following state:

$$|m_0 m_1 m_2 ... m_{N-1}\rangle = \frac{1}{\sqrt{2^{N-1}}} \left(|0\rangle + e^{2\pi 0.m_{N-1}} |1\rangle\right) \otimes \left(|0\rangle + e^{2\pi 0.m_{N-2} m_{N-1}} |1\rangle\right) \otimes ... \otimes \left(|0\rangle + e^{2\pi 0.m_0 m_1 ... m_{N-1}} |1\rangle\right) \quad (6)$$

$$|m_0 m_1 m_2 ... m_{N-1}\rangle = \frac{1}{\sqrt{2^{N-1}}} \otimes_{i=0}^{N-1} QFT(|m_i\rangle) \quad (7)$$

3.2. Signing Phase

1) Alice encrypts all qubits of Eq. 7 with secret keys which are shared with group members.

$$|A(S_i)\rangle = E_{K_{A G_{\Pi_A(i)}}}(QFT(|m_i\rangle)), i = 0..N-1 \quad (8)$$

Here, $E_K(.)$ is a quantum one-time pad encryption algorithm which is firstly defined by Kim et al [26] and used by Zhang et al. [27] to improve security of the protocol against forgery attacks. That quantum encryption algorithm can be defined as follows [27]:

$$E_K(|m\rangle) = \otimes_{i=0}^{N-1} {\sigma_x}^{K_{4i}} {\sigma_z}^{K_{4i-1}} T {\sigma_x}^{K_{4i-2}} {\sigma_z}^{K_{4i-3}} |m_i\rangle \quad (9)$$

$$T = \frac{i}{\sqrt{3}}(\sigma_x - \sigma_y + \sigma_z) \quad (10)$$

Due to using T, encrypted message cannot be forged [24]. Where the key length is $|K| = 4n$.

2) Alice sends $|A(S_i)\rangle$ to proxy group member $G_{\Pi_A(i)}$ by using permutation of Trent.
3) Alice encrypts $|m\rangle$ with secret key $K_T A$ with above encryption algorithm and send to Trent via quantum channel.

$$|AT(S_i)\rangle = E_{K_{TA}}(|m_i\rangle) \quad (11)$$

4) Trent decrypts the $|AT(S_i)\rangle$ with secret key K_{TA} and obtains $\tilde{m}$. Trent saves $\tilde{m}$.
5) After receiving $|A(S_i)\rangle$, proxy group member $G_{\Pi_A(i)}$ decrypt $|A(S_i)\rangle$ and obtains $|QFT(m_i)\rangle$. But any proxy group member does not know the order of $|QFT(m_i)\rangle$. Then $G_{\Pi_A(i)}$ encrypt $|QFT(m_i)\rangle$ with secret $K_{G_{\Pi_A(i)}B}$.

$$|G_{\Pi_A(i)}(S_i)\rangle = E_{K_{G_{\Pi(i)}B}}(QFT(|m_i\rangle)) \quad (12)$$

6) $G_{\Pi_A(i)}$ sends $|G_{\Pi_A(i)}(S_i)\rangle$ to Bob.

3.3. Verification Phase

1) Bob decrypts all $|G_{\Pi_A(i)}(S_i)\rangle$ by using secret key $K_{G_{\Pi_A(i)}B}$ and obtains $QFT(|m_i\rangle)$.
2) Bob asks Trent for permutation and m of Alice.
3) Trent sends ΠS_B to Bob by using authenticated classical channel or quantum channel.
4) Bob decrypt the ΠS_B and obtains Π_B permutation.
5) Bob reorder $QFT(|m_i\rangle)$ states with permutation of Trent and then applies $QFT^{-}1$ and gets $|\bar{m}_0 \bar{m}_1 \bar{m}_2 ... \bar{m}_{N-1}\rangle$. Then makes computational basis measurement onto that states and obtains $\bar{m}$.
6) Trent encrypts $|\tilde{m}\rangle$ with secret key $K_T B$ with above encryption algorithm and send to Bob via authenticated quantum channel.

$$|TB(S_i)\rangle = E_{K_{TB}}(|\tilde{m}_i\rangle) \quad (13)$$

7) Bob decrypts the $|TB(S_i)\rangle$ with secret key K_{TB} and obtains $|\tilde{m}\rangle$. Bob measures $|\tilde{m}\rangle$ with computational basis and saves $\tilde{m}$.

8) Bob checks equality of $\tilde{m}$ and $\bar{m}$. If $\tilde{m} = \bar{m}$, Bob will announce that the signature is valid, otherwise the signature is rejected and the protocol aborted.
9) If the signature is valid, then the Trent stores the message m with Alice's and proxy group participants identifications for later traceability.

4. Group Signature Protocol with QFT and Blinded Signature

In the first protocol, trusted participant Trent can see the message m in the step-3 of the signing phase. To blind the message the participants can forward following steps instead of the above protocol.

4.1. Signing Phase

The first two steps are the same as in the signing phase of Sect.3. 1)

3) Alice encrypts $|m\rangle$ with secret key K_AB with the encryption algorithm and send to Trent via quantum channel.

$$|AT(S_i)\rangle = E_{K_{AB}}(|m_i\rangle) \tag{14}$$

4) Trent encrypts the $|AT(S_i)\rangle$ with the secret key K_{TB}.

$$|TB(S_i)\rangle = E_{K_{TB}}(|AT(S_i)\rangle) \tag{15}$$

Then, Trent sends the above encrypted state to Bob via quantum channel.

5) Bob decrypts $|TB(S_i)\rangle$ with the secret key K_{BT} and gets $|AT(S_i)\rangle$. Then, Bob decrypts the states $|AT(S_i)\rangle$ and gets $|m_i\rangle$ states. Bob measures the $|m_i\rangle$ states with computational basis and saves the results as $\tilde{m}$.

The other steps are the same as in the signing phase of Sect.3.

4.2. Verification Phase

The first step is the same as in the verification phase of Sect.3. 1)

2) Bob asks Trent for permutation.
3) Trent sends ΠS_B to Bob by using authenticated classical channel or quantum channel.
4) Bob decrypt the ΠS_B and obtains Π_B permutation.
5) Bob reorder $QFT(|m_i\rangle)$ states with permutation of Trent and then applies $QFT^{-}1$. So Bob gets $|\bar{m}_0\bar{m}_1\bar{m}_2...\bar{m}_{N-1}\rangle$. Then Bob makes computational basis measurement onto that states and obtains $\bar{m}$.
6) Bob checks equality of $\tilde{m}$ and $\bar{m}$. If $\tilde{m} = \bar{m}$, Bob will announce that the signature is valid, otherwise the signature is rejected and the protocol aborted.
7) If the message is valid, then Bob encrypt the valid message m with encryption algorithm.

$$|BT(S_i)\rangle = E_{K_{BT}}(|m_i\rangle) \tag{16}$$

Then Bob sends $|BT(S_i)\rangle$ to Trent.

8) Trent decrypts $|BT(S_i)\rangle$ with secret key K_{BT} and measures the states with computational basis and obtains $\bar{m}$.
9) Trent also asks Alice for sending m to him.
10) Alice encrypt the valid message m with encryption algorithm.

$$|AT(S_i)\rangle = E_{K_{AT}}(|m_i\rangle) \tag{17}$$

Then Alice sends $|AT(S_i)\rangle$ to Trent.

11) Trent decrypts $|AT(S_i)\rangle$ with secret key K_{AT} and measures the states with computational basis and obtains $\tilde{m}$.
12) Trent checks the equality of the $\tilde{m}$ and $\bar{m}$. If they are equal then stores the message $\tilde{m}$ with Alice's and proxy group participants identifications for later traceability.

5. Security Analysis

Main requirements of the quantum digital signature protocols to provide unconditionally security are that the signature should not be disavowed by the signatory, and any attacker cannot forgery signatory's signature.

5.1. Impossibility of Forgery

Firstly, we consider insider attacker. We assume that Bob is illegal participant and wants to create a signature of Alice. Even if Bob knows the details of the signature protocol he cannot create Alice's signature because of trusted group manager Trent. Bob cannot create Alice's signature without knowledge of Trent. After the end of the legal signature protocol , Bob may change correct data m to $\bar{m}$. Because of the knowledge about correct m of Trent, Bob cannot achieve forgery.

Secondly, any proxy group member $\{G_1, G_2, ..., G_N\}$ may try to forge Alice's signature. Any individual proxy group member G_i cannot achieve forgery because of he/she can only contribute the part of the full signature. Suppose dishonest $N-1$ group of participants want to create a correct signature of Alice. But they cannot achieve that. Because, all of the $QFT(|m_i\rangle)$ state must be reordered with Trent's permutation to produce a correct signature of Alice. Even if any attacker can get the permutation, the permutation will be changed by Trent for every signature session. Trent must be part of the protocol. So any $N-1$ participant of proxy group cannot achieve collective forgery. Further, one of the proxy group member G_i may change $QFT(|m_i\rangle)$ state by applying unitary transformation. Then, Bob and Trent can decide who changed the state by comparing m and $\bar{m}$.

$$\Pi S_{AB} = E_{K_{AB}}(\Pi_A) \tag{18}$$

$$\Pi S_{BA} = E_{K_{AB}}(\Pi_B) \tag{19}$$

Thus, Alice and Bob decrypt $\Pi S_{AB}, \Pi S_{BA}$ with secret key K_{AB}. They checks equality of Π_A, Π_B.

5.2. Impossibility of Disavowal

In this protocol, all the members of the proxy group must cooperate to create a signature. Bob must get the data of the signature from the all group members to obtain valid signature. So any member of the group proxy can not disavow the signature.

Alice and Bob cannot disavow the signature because of the management of protocol by trusted Trent. Trent controls some communication steps of the protocol. If Alice can send different $|\tilde{m}\rangle$ to the Trent and claim that the signature is not mine. Trent can check the equality of the $|\tilde{m}\rangle$ from Alice and $|\bar{m}\rangle$ from Bob. Trent can decide whether the signature protocol is valid or not.

6. Conclusion

It is well known that ring signature related to group signature. However group and ring signature have advantages and disadvantaged with respect to each other. For example , in many ring signature, it is assumed honest users and honestly generated public keys of ring . There is no security in the case of users sign with respect to a ring containing even one adversarial generated public key. However, ring signature is flexible [28].

But, in group signature, the signer can be traced by a designed group manager like our scheme. Also, in our scheme, amplitudes of quantum states is transferred to the phase space due to application of quantum Fourier transformation. So, it is very

hard for attachers to get right quantum state. Furthermore, in our case like other quantum scheme, it is instantly possible to become aware of thief by quantum decoy state.

In this study, a new multi-partied quantum proxy group signature protocol based on QFT is proposed. All of the proxy group members are part of the signature creation. Alice expresses the message m into phase-space by using QFT. So the message m is expressed in phases of the output qubits of QFT. This improves the message security.Because, every member of the proxy group takes only one part of the message and thus knows only their part of the message. Alice sends every part of the message to the proxy group members to be signed. But Alice changes order of the output qubits of the QFT according to permutation information which is sent by trusted Trent. So any member of the proxy group does not know order of the qubits and also they cannot create a valid signature.

Any information (classical or quantum) in the protocol is sent by using encryption algorithm which is robust against forgery by insider/outsider attacker. Furthermore, decoy states can be used to be aware of Eve.

Bob can verify validity of the signature by the help of the trusted Trent and proxy group members. Trent must send the order of the qubits to the Bob to obtain real message m by using $QFT^{-}1$.

The above security analysis implies that given group proxy signature protocol based on QFT provides unconditionally security. In addition, our protocol provides higher efficiency, effective secret key usage and security.

Acknowledgments

I would like to thank referee for valuable suggestions and new insight. This manuscript was presented as a oral presentation at 10th International Conference on Information Security and Cryptology, On 20-21 October 2017, the Information Technologies and Communication Center Headquarters, Ankara-TURKEY.

References

[1] P. W. Shor, Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer, 1997 SIAM J. Comput. 26 14841509

[2] L.K. Grover, A fast quantum mechanical algorithm for database search, 1996 Annual Acm Symposium on Theory of Computing (ACM) pp 212219

[3] L. K. Grover, A framework for fast quantum mechanical algorithms, 1998 Proceedings of the Thirtieth Annual ACM Symposium on Theory of Com-puting STOC 98 (New York, NY, USA: ACM) pp 5362 ISBN 0-89791-962-9

[4] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distiriubition and coin tossing, 1984 Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing (India) p 175

[5] A. K. Ekert, Quantum cryptography based on Bell's theorem, 1991 Phys. Rev. Lett. 67(6) 661663

[6] F. Gao, F. Z. Guo, Q. Y. Wen and F. C. Zhu, Quantum key distribution without alternative measurements and rotations, 2006 Physics Letters A 349 53 58 ISSN 0375-9601

[7] D. Mayers, Unconditional security in quantum cryptography, 2001 J. ACM 48 351406 ISSN 0004-5411

[8] R. Cleve, D. Gottesman and H. K. Lo, How to Share a Quantum Secret, 1999 Phys. Rev. Lett. 83(3) 648651

[9] M. Hillery, V. Buzzek and A. Berthiaume, Quantum secret sharing, 1999 Phys. Rev. A 59(3) 1829-1834

[10] X. B. Chen, X. X. Niu, X. J. Zhou and Y. X. Yang, Multi-party quantum secret sharing with the single-particle quantum state to encode the information, 2013 Quantum Information Processing 12 365380 ISSN 1573-1332

[11] H. Da-Zu, C. Zhi-Gang and G. Ying, Multiparty Quantum Secret Sharing Using Quantum Fourier Transform, 2009 Communications in Theoretical Physics 51 221

[12] D. Gottesman and I. Chuang, Quantum Digital Signatures, 2001 eprint arXiv:quant-ph/0105032

[13] H. Buhrman, R. Cleve, J. Watrous and R. de Wolf, Quantum fingerprinting, 2001 Phys. Rev. Lett. 87(16) 167902

[14] G. Zeng and C. H. Keitel, An arbitrated quantum signature scheme, 2002 Phys. Rev. A 65(4) 042312

[15] P. O. Boykin and V. Roychowdhury, Optimal encryption of quantum bits, 2003 Phys. Rev. A 67(4) 042317

[16] H. Lee, C. Hong, H. Kim, J. Lim J and H. J. Yang, Arbitrated quantum signature scheme with message recovery, 2004 Physics Letters A 321 295 300 ISSN 0375-9601

[17] Q. Li, W. H. Chan and D. Y. Long, Arbitrated quantum signature scheme using Bell states, 2009 Phys. Rev. A 79(5) 054307

[18] D. Chaum and E. van Heyst 1991 Group Signatures (Berlin, Heidelberg: Springer Berlin Heidelberg) pp 257265 ISBN 978-3-540-46416-7

[19] X. Wen, Y. Tian, L. Ji and X. Niu, A group signature scheme based on quantum teleportation, 2010 Physica Scripta 81 055001

[20] W. Xiaojun, An E-payment system based on quantum group signature, 2010 Physica Scripta 82 065403

[21] Y. Yang, Multi-proxy quantum group signature scheme with threshold shared verification, 2008 Chinese Physics B 17 415418

[22] Y. Yang and Q. Wen, Threshold proxy quantum signature scheme with threshold shared verification, 2008 Science in China Series G: Physics, Mechanics and Astronomy 51 10791088 ISSN 18622844

[23] J. Shi, S. Zhang and Z. Chang, The security analysis of a threshold proxy quantum signature scheme, 2013 Science China Physics, Mechanics and Astronomy 56 519523 ISSN 18691927

[24] J. Shi J, R. Shi, Y. Tang and M. H. Lee, A multiparty quantum proxy group signature scheme for the entangled-state message with quantum Fourier transform, 2011 Quantum Information Processing 10 653670 ISSN 1573-1332

[25] M. A. Nielsen and I. L. Chuang 2011 Quantum Computation and Quantum Information: 10th Anniversary Edition 10th ed (New York, NY, USA: Cambridge University Press) ISBN 1107002176, 9781107002173

[26] T. Kim, J. W. Choi, N. S. Jho and S. Lee, Quantum messages with signatures forgeable in arbitrated quantum signature schemes, 2015 Physica Scripta 90 025101

[27] W. Zhang, D. Qiu and X. Zou, Improvement of a quantum broadcasting multiple blind signature scheme based on quantum teleportation, 2016 Quantum Information Processing 15 24992519 ISSN 1570-0755

[28] A. Bender, J. Katz and J. Morselli, Ring Signatures: Stronger Definitions, and Constructions without Random Oracles https://eprint.iacr.org/2005/304