Group Signature Entanglement in E-voting System

Hamoud Alshammari, Khaled Elleithy, Khaled Almgren, Saleh Albelwi

Computer Science and Engineering, University of Bridgeport
halshamm@my.bridgeport.edu, elleithy@bridgeport.edu, kalmgren@my.bridgeport.edu, salbelwi@my.bridgeport.edu

Abstract—In any security system, there are many security issues that are related to either the sender or the receiver of the message. Quantum computing has proven to be a plausible approach to solving many security issues such as eavesdropping, replay attack and man-in-the-middle attack. In the e-voting system, one of these issues has been solved, namely, the integrity of the data (ballot). In this paper, we propose a scheme that solves the problem of repudiation that could occur when the voter denies the value of the ballot either for cheating purposes or for a real change in the value by a third party. By using an entanglement concept between two parties randomly, the person who is going to verify the ballots will create the entangled state and keep it in a database to use it in the future for the purpose of the non-repudiation of any of these two voters.

Index Terms—Entanglement, Entangled State, E-voting System, Qubit, Quantum Computing.

I. INTRODUCTION

In modern societies, automatization has been employed in different aspects of social life, such as voting and e-commerce. Consequently, this led to the development of a number of protocols for electronic voting to work successfully. Those protocols are designed to solve security issues, such as confidentiality, data integrity and authentication [1]. Most voting protocols implement public-key cryptography to guarantee the inability of the adversary to solve the difficult computations, such as factoring large numbers, but the advent of quantum computing has made factoring easier [2]. The authentication of receivers and senders is very important in any system, and some even consider authentication to be the most important aspect of security services. The authentication process is used to validate the identity of the sender, the identity of the receiver, or the content of the message [3]. Authenticating the identity of the receiver to the sender is called non-repudiation. It is also a very important process because it guarantees both the sender's and receiver's rights. Many security solutions, such as digital signature, can be used to achieve authentication and non-repudiation. In order to achieve non-repudiation, the receiver has to authenticate the identity of the sender using a security solution, such as digital signatures [4].

Quantum computing opens a new door in computer science. It can enhance the computational complexity of many hard computer science problems. However, some classical computing issues still have not been improved practically using quantum computing. Quantum computing depends on physics through the power of atoms [2]. It introduces qubits and superposition. Qubits represent two states at the same time, and a quantum computer can be in a superposition of two basic states at the same time [5].

Blind signature was introduced by David Chaum [6]. It is the process of blinding messages before signing them, where the message owner and the signer are different. It is used in privacy-related protocols. For example, it can be used in E- voting systems, where the ballot is confidential [7]. Also, group signature was introduced by David Chaum. It is basically done when a group member signs a message on behalf of the group to maintain anonymity among that group. It aims to hide the signer's information [8].

In quantum computing, there is a method that allows two particles to act as one object, even though they are two different physical objects. This concept is called entanglement [9]. Thus, when you know the state of one particle, you will know the state of the other particle. Further, changes in one particle state will affect the other entangled particle. The entanglement concept provides the availability of checking back the anonymity in the e-voting process by creating an entangled state between two voters [10]. In other words, the voter can follow and know whether his/her ballot has been changed by checking the entangled state through calculating a new one and comparing it with one that they already have.

In this paper, we propose a mechanism that gives a third party, such as a group manager, the ability to verify and determine the value of the qubits between two voters. This process is executed using a two-particle entangled quantum system. The first part of the paper defines the problem of the e-voting security system. The second part describes some related work that discusses different points that are related to the proposed problem in this work. The third part proposes a solution that could be applied to solve the non-repudiation problem. Then we discuss some security-related points regarding the integrity of the ballot and non-repudiation process itself. The last section offers conclusions

II. PROBLEM IDENTIFICATION

In the e-voting system, there are many challenges that face voters and verifiers. When voters generate the ballots, they need to keep their information private and the message itself anonymous and not changed in transmission. Thus, by applying the concept of entanglement in quantum computing, some schemes solved the problem of checking back the value by generating an entangled state from two qubits of two different voters who keep the entangled state for future checking.

In the existing e-voting schemes, no one can ensure the value of the ballot except the voter himself. So in the case of repudiation, it prevents the voter from denying his/her vote. In our scheme, we propose extending the existing scheme that can determine the original value of the ballot when the signer was signed in the first time.

III. RELATED WORK

Xu *et al.* [4] proposed a scheme which supports anonymity of the voters in the e-voting system by applying the concept of blinding and grouping signature. This scheme seems to be easier than the other quantum signature schemes because it does not involve entanglement. In the e-voting system, the message has to be signed by the manager of the office. However, the content of the message does not have to be readable by any person other than the owner of the message (blind signature scheme).

Also, Xu's paper uses the grouping signature to provide anonymity of voters in the e-voting system, whereas the voter information, such as location information, has to be secure and non-readable by any person. Some e-voting systems could be applied in different branches and offices in different locations, so signing the message from a specific manager might reveal the location information of the voter. Thus, by applying grouping signature with different managers on the same message, f tracing the sender could be eliminated.

However, the verifier cannot know the identity of the signer; he/she can only verify the validity of the signature. This paper is different than some other schemes that propose different services. Xu *et al.* [4] proposes a blind signature scheme using a group signature scheme for a distributed e-voting system without using the entangled state concept, and this scheme can represent a high level of efficiency. The authors explained some disadvantages, such as using a symmetric scheme. Also, the inspector in this scheme is the only person who can verify the message which makes the scheme elastic with only e-voting systems.

In [10], the authors proposed a new quantum protocol that provides anonymous voting with anonymity check. This protocol has two main characteristics. First, the value of a voter's vote is unknown to other voters and the tallyman. Second, a non-exaggeration technique has been implemented to prevent malicious voters from voting twice. Each voter makes a binary decision (0,1); 0 means no and 1 means yes. There is a tallyman who collects the ballots and announces the results. The main idea, after the voting process, is that the ballots are returned to voters again to allow for two voters to check the anonymity of the vote counting process by preparing an entangled state of two ballots. Thus, any attempt by a curious tallyman to gain information about voting results leads to the destruction of the entanglement, which can be detected by the voters. The entangled state is generated using one of four Bell bases to create a Bell state as follows:

The four Bell bases are:

$$|\varphi^{+}>=\frac{1}{\sqrt{2}}(|00i>+|11i>) \dots\dots (1)$$

$$|\varphi^{-}>=\frac{1}{\sqrt{2}}(|00i>-|11i>) \dots\dots (2)$$

$$|\psi^{+}>=\frac{1}{\sqrt{2}}(|01>+|10i>) \dots\dots (3)$$

$$|\psi^{-}>=\frac{1}{\sqrt{2}}(|01i>+|10i>) \dots\dots (4)$$

The voters carry out the ballot test:

- The voters who have chosen to vote measure their qubits in computational basis. If there is a difference from the sent ballot, they state the ballot test failure.

- On the other hand, the voters who have chosen to check the anonymity make the measurement of their qubits in the Bell basis. If there is a difference from the Bell state, they state the ballot test failure.

Suppose a curious tallyman makes an additional measurement of qubits to gain information about voters. For example, to learn the vote of voter *i*, the easiest way is by measuring the ith qubit in computational basis. If voter *i* has chosen to vote, this attack will be unnoticed. But if voter *i* has chosen to check the anonymity with voter *j*, this leads their state to be transformed into (0,1) or (1,0) with equal probability of 0.5, which means anonymity check test failure. Therefore, the curious tallyman will be detected.

Xiaoqiang proposed in [11] a blind signature scheme that is based on quantum computing. The scheme combines proxy and blind signatures. The scheme consists of four parties. They are Bob, who is the message signer; Charlie, who is the message owner; Alice, who prepares the proxy warrant message; and Trent, who is responsible for delivering the two particles to Bob and Charlie and verifying the signature. The authors used BB84 quantum protocol for key distribution. They applied quantum entanglement for the signature generation and verification process. Using a one-time pad encryption algorithm provides unconditional security and prevents eavesdropping.

In [12], the authors propose a blind quantum scheme based on a two-particle entangled system. It combines proxy and blind signatures and consists of three parties. Alice is the message owner, Bob is the message signer, and Charlie is the message arbitrator and Bob's proxy. This scheme can be used in privacy-related protocols. The authors used entanglement to the blind signature generation process and the verification process. The key distribution method is not explained in this paper.

IV. PROPOSED SOLUTION

Horoshko and Kilin [10] proposed a scheme that imple ments the concept of Entanglement between two voters to allow them to check back their ballots' statuses in order to detect possible cheating. Xu and Huang [4] proposed a scheme in the e-voting system that implements the concept of group signature to keep the information of the voter more secure by granting the privileges to the manager to sign the ballot on behalf of the group.

In this work, a new scheme is proposed to employ quantum-entangled state to ensure non-repudiation service by calculating a quantum-entangled state between two random voters. If any voter claims that the value of the ballot has been changed, the manager can verify that by checking back the entangled state between these two voters. In our scheme, we have five main parties. The first two are the voters Alice and Nancy. The third is the group manager (Bob) who signs the ballots and is responsible for creating the entangled state. The fourth is a trusted party (Trent) who creates the group signature. The fifth is the verifier (Charlie) who verifies the ballots

and calculates the values of the ballots in terms of voting statistics as shown in Figure 1.

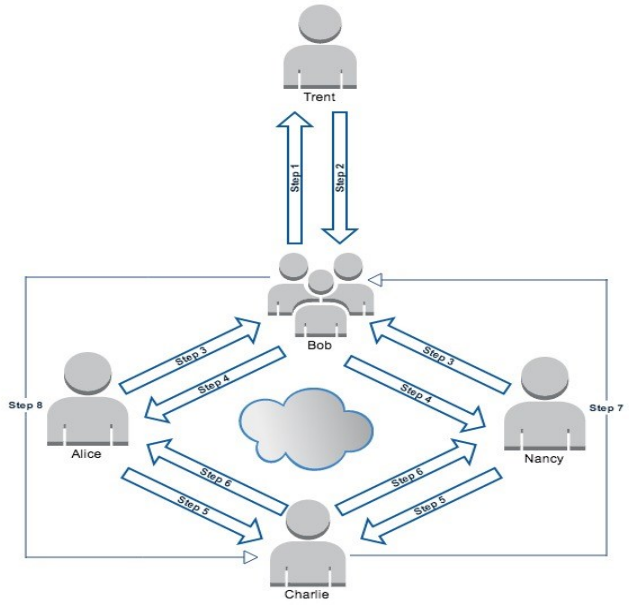

Figure 1. The Process of Quantum Digital Signature Verification Scheme.

The scheme steps are as follows:

Initial Phase

Alice, Nancy, Bob, Charlie and Trent share secret keys. Alice and Nancy share a secret key KAB, KNB with Bob. Bob and Trent share a secret key KBT. Alice and Nancy share a secret key KAC, KNC with Charlie. Trent and Charlie share a secret key KTC. The initial phase consists of two steps as follows:

1) Bob and others (Group members) send their information to Trent. All group members send their information (Info) encrypted using the shared key; for example, Bob sends his information using KBT to Trent.

$$Info = E_{KBT}\,(I_{DB}) \ldots\ldots (5)$$

2) Trent creates the group signature (GS). The group signature consists of the identities of all group members who are using the signature to sign ballots and then encrypts it using the shared key KBT and sends it back to Bob.

Voting Phase

1) Alice and Nancy create the ballots. The voting value is either yes (1) or no (0). Then the voting values are calculated and represented by a qubit. The Hadamard matrix is used to convert the bits to qubits. Then they send the qubits to Bob.

$$H(|0>) = \frac{1}{\sqrt{2}}\,(|0> + |1>) \ldots\ldots (6)$$

$$H(|1>) = \frac{1}{\sqrt{2}}\,(|0> - |1>) \ldots\ldots (7)$$

2) Bob prepares an entangled state between Nancy and Alice by using one of the Bell bases as shown in Figure 2. Then Bob saves the identities of both voters and the values of Bell states in a database as shown in Table I. Then he signs both ballots using the GS and sends them back to Alice and Nancy.

$$|\varphi^{+}> = \frac{1}{\sqrt{2}}\,(|0_{Alice}0_{Nancy}> + |0_{Alice}0_{Nancy}>) \ldots\ldots (8)$$

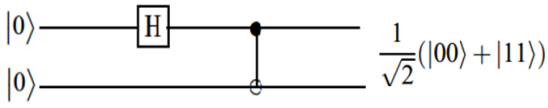

Figure 2. Generation of entangled states (Bell states).

Table 1: Entangled States Table for Bob

First Voter ID	Second Voter ID	Bell State
Alice	Nancy	$\|\phi+>$
--	--	--
--	--	--

3) Alice and Nancy send their ballots to Charlie.
4) Charlie collects the values of ballots and then sends the qubits back to Alice and Nancy.

Verification Phase

1) If Alice claims that the value of the ballot has changed, she sends a claim to Charlie. The claim consists of Alice's ID and the qubit.
2) Charlie sends the claim to Bob.
3) Bob receives the claim.
   a. Bob searches in the table for Alice's information. Then he retrieves the ID of the second voter (Nancy) and Bell state.
   b. Bob sends a request to Nancy asking for her qubit.
   c. Bob calculates the new Bell state.

V. SECURITY ANALYSIS AND DISCUSSION

There are some aspects that the scheme addresses, namely, the integrity of the ballot and the non-repudiation security services. The first service—the integrity of the ballot—has already been explained in [10], which solves the problem of any cheating that could occur regarding the value of the vote.

The other service is the non-repudiation, which was de- scribed in the verification phase that takes place after Charlie receives a claim from Alice and sends it forward to Bob. Here Bob compares the new Bell state with the Bell state in the table based on the new values. If they are equal, then the claim is correct; otherwise, it is incorrect.

When the claim is correct, that means the qubit was cheated by an eavesdropper after Bob calculated the first entangled state while sending it back to Alice or when it was sent to Charlie. Otherwise, in the event that the claim is incorrect, that means either the qubit was cheated before Bob calculated the first entangled state while sending it from Alice to Bob, or that Alice wants to change the original value, which means repudiation.

VI. CONCLUSION

We proposed a new scheme that enhanced an existing one that solves the check back e-voting anonymity to solve the problem of denying the value of the ballot. By implementing the concept of the entanglement between two random voters, the signer can determine the correct value of the ballot. However, this scheme has a simple weakness which shows up when the signer (Bob) tries to contact the second voter (Nancy) asking her for the qubit, but she does not respond. We are planning to extend this scheme to address this problem by keeping the original qubits in a separate database somewhere in the system.

REFERENCES

[1] D. Gritzalis, Secure electronic voting, Kluwer Academic Publishers Dordrecht, 2003.

[2] D. Gottesman and I. Chuang, "Quantum digital signatures," arXiv preprint quant-ph/0105032, 2001.

[3] X. Lu and D. Feng, "Quantum digital signature based on quantum one- way functions," in Advanced Communication Technology, 2005, ICACT 2005. The 7th International Conference on, vol. 1. IEEE, 2005, pp. 514–517.

[4] R. Xu, L. Huang, W. Yang, and L. He, "Quantum group blind signa- ture scheme without entanglement," Optics Communications, vol. 284, no. 14, pp. 3654–3658, 2011.

[5] Q. Li, C. Li, Z. Wen, W. Zhao, and W. H. Chan, "On the security of arbitrated quantum signature schemes," Journal of Physics A: Mathematical and Theoretical, vol. 46, no. 1, p. 015307, 2013.

[6] D. Chaum, "Blind signatures for untraceable payments." in Crypto, vol. 82, 1982, pp. 199–203.

[7] M. Ying and S. Chun-Huan, "A controllable quantum sequential signature and vote scheme," in Industrial Control and Electronics Engineering (ICICEE), 2012 International Conference on. IEEE, 2012, pp. 17–19.

[8] S. Qi, H. Zheng, W. Qiaoyan, and L. Wenmin, "Quantum blind signature based on two-state vector formalism," Optics Communications, vol. 283, no. 21, pp. 4408–4410, 2010.

[9] T.-S. Lin, C.-H. Chien, T.-H. Chang, and S.-Y. Kuo, "Quantum signature scheme for vehicular networks using entangled states," in Security Technology (ICCST), 2011 IEEE International Carnahan Conference on. IEEE, 2011, pp. 1–6.

[10] D. Horoshko and S. Kilin, "Quantum anonymous voting with anonymity check," Physics Letters A, vol. 375, no. 8, pp. 1172–1175, 2011.

[11] Y. Xiaoqiang and Z. Xiaohui, "A quantum proxy blind signature protocol," in Computer, Mechatronics, Control and Electronic Engineering (CMCE), 2010 International Conference on, vol. 1. IEEE, 2010, pp.78–80.

[12] J. Shi, R. Shi, X. Peng, and M. H. Lee, "Quantum communication scheme for blind signature with arbitrary two-particle entangled system," in Advanced Communication Technology (ICACT), 2013 15th International Conference on. IEEE, 2013, pp. 58–62.