An Approach to Secure Authentication Protocol with Group Signature based Quantum Cryptography

V. Padmavathi, M. Madhavi, N. Nagalakshmi

Abstract*-This paper proposes a secure authentication protocol in a new direction with group signature based Quantum cryptography for a networked organization. The group signature setting has a group with copious members and one manager. The proposed protocol uses a trusted centre TC generates a large heap of public/private key pairs. Every member of the group has a different list of unique private keys which is distributed by TC to sign a document. The keys are immunable using quantum key distribution protocol which acquires the properties of quantum mechanics.

***Keywords*- group signature, public/private key, quantum cryptography, quantum key distribution protocol QKDP, Trusted Center TC.**

I. INTRODUCTION

Group signature is an electronic signature used to authenticate the sender's identity of a message or signer of the document. It ensures the integrity of the message. Group signatures introduced by Chaum and van Heyst [13] in which a member anonymously signs a document on behalf of the group. Group signatures have abundant applications in the space of authentication and privacy. The document gets attestation by trusted third party which the most eminent one for authentication. This paper proposes group signatures based quantum cryptography.

Quantum cryptography is an arising technology which emphasizes the phenomena of quantum physics in which two parties can have secure communications over network is based on the invulnerability of the laws of quantum mechanics. The two important elements of quantum mechanics on which quantum cryptography depends are Heisenberg Uncertainty principle and photon polarization principle [14]. The Heisenberg Uncertainty principle refers that, certain pairs of physical properties are pertained in such away that measuring one property prevents the eavesdropper from simultaneously knowing the value of the other.

Manuscript published on 30 December 2012.
***Correspondence Author(s)**

V. Padmavathi, Associate Professor , Department of Electronics & Computer Engineering, Sreenidhi Institute of Science & Technology, JNT University, Hyderabad, Andhra Pradesh, India.

M. Madhavi , Associate Professor, Department of Computer Science & Engineering, Anurag Engineering College, Kodad, Nalgonda, Andhra Pradesh, India.

N. Nagalakshmi , Assistant Professor, Master of Computer Applications Department, Anurag Group of Institutions, JNT University, Hyderabad, India.

II. EXISTING SYSTEM

The principle of photon polarization refers that, an eavesdropper cannot copy unknown qubits i.e. unknown quantum states, due to no-cloning theorem [2], [4]. If an attempt is made to measure the property, it disturbs the other. The system which is existing implements authentication protocol with group signature is based on classical cryptography methods in wired and wireless security and have been found to have vulnerabilities. The system uses classic communication channel in which eavesdropper activity can be done quite often and more possibilities to extract the signature.

III. PROPOSED PROTOCOL

The proposed authentication protocol with group signature based quantum cryptography is where it uses quantum mechanical principles. Along with communication channel, quantum channel is used. This channel is used for sending qubits. The attacks can be identified with the properties of quantum and infeasible to extract the signature.

IV. QUANTUM MEASUREMENT

Quantum cryptography was first proposed in 1984 by Bennet and Brassard and is known as the BB84 protocol [1]. In the BB84 protocol, two bases namely, rectilinear R and diagonal D and four states of polarized photons are defined. A binary 0 is 0 degrees polarization in the rectilinear bases or 45 degrees polarization in the diagonal bases. A binary 1 is 90 degrees polarization in the rectilinear bases or 135 degrees polarization in diagonal bases [1], [7]. It uses quantum communication channels between communicating entities. On the quantum channel, polarized single photons, i.e. qubits, are transmitted from sender i.e. TC to receiver i.e. members of the group [5].

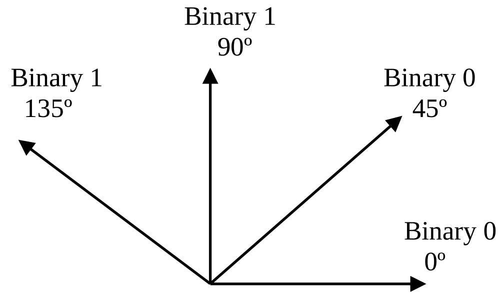
A. Notations

If TC wants to send a classical bit b, then he/she creates a qubit [6] and sends it to group members based on the following rules:

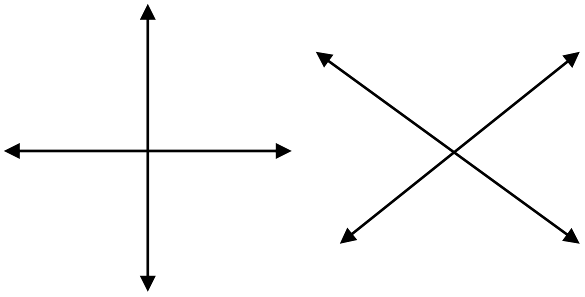
R: The rectilinear basis which is polarized with two orthogonal directions, $|0>$ and $|1>$.

D: The diagonal basis which is polarized with two orthogonal directions, $1/\sqrt{2}\,(|0> + |1>)$ and $1/\sqrt{2}\,(|0> - |1>)$ [13].

When members of the group receive the qubit, they randomly choose either the basis R or the basis D and they measures the qubit to get the measuring result. Observe that member cannot simultaneously measure the qubit in an R basis and D basis and also any passive attack like eavesdropper action is identified since one measure the qubit, the polarization state of that qubit will be disturbed [3].



Photon Polarization



Rectilinear Basis Diagonal Basis

V. AUTHENTICATION

The protocol standardized by the Trusted Center TC. Associated to the group is a single signature-verification key *vk* called the group public key. Each group member *i* has its own secret signing key based on which it can produce a signature relative to *sk*. The core requirements as per are that the group manager has a secret key *gmsk* based on which it can, given a signature σ, extract the identity of the group member who created *σ* and on the other hand an entity not holding *gmsk* should be unable, given a signature *σ* to extract the identity of the group member who created *σ* [9]. Authentication is carried based on the properties of group signature.

Group signature properties:

- Only members of the group can sign the messages.
- The signature can be verified by receiver.
- The receiver of the signature cannot arbitrate which member of the group is the signer.
- In the case of a conflict, the signature can be opened to reveal the identity of the signer [8], [11].

A group signature scheme involves three types of parties: members, non-members and a group manager. It further consists of five algorithms KeyGen, Sign, Verify, Open, and Revoke [7], [9], [10].

A. *Key Generation Phase*

This proposed protocol uses Trusted Center TC to generate a large heap of public/private key pairs and distributes every member of the group different list of unique private keys to sign a document. The key distribution phase involves setup phase. Let two users would like to establish a session key:

- K_{TA} is the secret key shared between TC and member$_1$. Similarly K_{TB} is the secret key shared between TC and member$_2$.
- Bit sequence in K_{TA} is treated as the measuring bases between member A and the TC. If $(K_{TA})_i$ =0, D basis is chosen; otherwise, R basis.

Note that $(K_{TA})_i$ denotes the i^{th} bit of the secret key K_{TA}.

The following explains the details of key distribution phase. Assume that the TC has been announced to start the QKDP with n members. TC and the members have to perform the QKDP as follows:

1. The TC generates a random number r_{TA} and a session key SK. TC then computes $R_{TA} = h\ (K_{TA},\ r_{TA})$ XOR $(SK||U_A||U_B)$ for member$_1$ and, similarly r_{TB} and $R_{TB} = h\ (K_{TB},\ r_{TB})$ XOR $(SK||U_B||U_A)$ for member$_2$ and so on for n members.

2. The TC creates the qubits, Q_{TA}, based on $(r_{TA}\ ||R_{TA})_i$ and $(K_{TA})_i$ for member1 where i = 1;2;……………..;n and $(r_{TA}\ ||R_{TA})_i$ denotes the ith bit of the concatenation $r_{TA}\ ||R_{TA}$.

- If $(r_{TA}||R_{TA})_i$=0, $(K_{TA})_i$= 0,

then $(Q_{TA})_i$ is $(1/\sqrt{2}(|0) + (|1))$.

- If $(r_{TA}||R_{TA})$i=1, $(K_{TA})_i$=0,

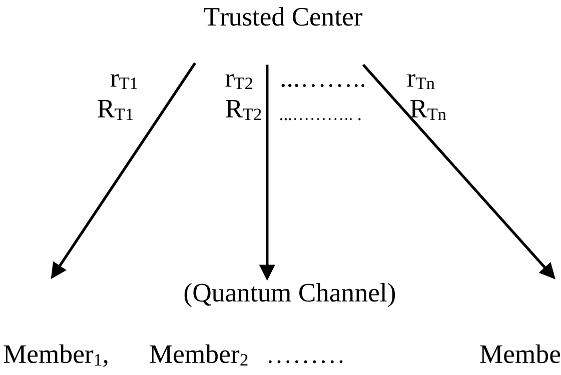
then $(Q_{TA})_i$ is $(1/\sqrt{2}\ (|0) - (|1))$.

- If $(r_{TA}\ ||R_{TA})_i = 0$, $(K_{TA})_i$= 1,

then $(Q_{TA})_i$ is $(|0)$

- If $(r_{TA}\ ||R_{TA})_i = 1$, $(K_{TA})_i$= 1,

then $(Q_{TA})_i$ is $(|1)$ [14].



TC then sends Q_{TA} to member$_1$. TC creates qubits member$_2$ in the same way.

Member$_1$ measures the received Q_{TA} qubits depending on K_{TA}. If $(K_{TA})_i$=0, then the qubit is measured based D basis otherwise, R basis. Similarly, remaining members of a group.

B. *Key generation*

The probabilistic algorithm is used for key generation. The key generation algorithm produces (*vk*, *gmsk*) ← KeyGen ( ) as output, where *vk* is a public verification key and *gmsk* is the group managers secret key. If the group of members is fixed, we may assume that the algorithm also outputs a vector *sk* of secret keys to be used by the members. If, however, the group of members is dynamic, KeyGen does not output secret keys for the members. Instead the Join protocol can be used to let non-members join the group. As a result of this protocol, a new member i obtain a secret key ski, while the group manager obtains some information Yi related to the new member that he/she includes into his secret key *gmsk* [9].

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

C. Signing algorithm

To sign a message m the member runs a signature generation algorithm which is probabilistic algorithm on input a message *m*, an individual group member's secret key *sk* and the group's public key *vk which* outputs a signature σ i.e. $\sigma \leftarrow$ Sign (*m*, *sk*, *vk*) [7].

D. Verification algorithm

To verify a signature σ on message m one computes a boolean-valued algorithm Verify (*vk*, *m*, σ). A verification algorithm that on input a message *m*, a signature σ and the group's public key *vk* returns 1 if and only if σ was generated by any group member using sign on input *m*, *sk* and *vk*.

Furthermore, given a signature σ on m, the group manager can identify the originating member by computing Open (*gmsk*, *m*, σ), which outputs the identity of the member who created the signature.

Finally, using the Revoke algorithm (*vk*, *gmsk)* Revoke (*gmsk*, *vk*), the group manager can exclude the member relating to Yi from the group [9].

VI. CONCLUSION

This proposed work easily resists replay and passive attacks because of quantum measurement. The signer can't repudiate the message that he/she signed and it is infeasible to produce signatures of others messages they haven't signed. By combining the advantages of quantum cryptography with group signature, this work presents a new direction in the space of privacy protection.

REFERENCES

1. C.H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," Proc. IEEE Int'l Conf. Computers, Systems, and Signal Processing, pp. 175-179, 1984
2. W.K. Wootters and W.H. Zurek, "A Single Quantum Cannot Be Cloned," Nature, vol. 299, pp. 802-803, 1992.
3. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum Cryptography," *Rev. of Modern Physics*, vol. 74, pp. 145-190, 2002.
4. S. Imre, F. Balázs: Quantum Computing and Communications – An Engineering Approach, Published by John Wiley and Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex PO19 8SQ, England, 2005, ISBN 0-470-86902-X, 283 pages.
5. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *Journal of Cryptology*, vol. 5, no.1, 3 - 28, 1992.
6. M. Nielsen and I. Chuang, "Quantum computation and quantum information", London Cambridge University Press, 2000.
7. Jan Camenisch, Markus Michels. A group signature scheme with improved efficiency. In *Proc. of ASIACRYPT '98,* Springer-Verlag, LNCS 1514, 1998.
8. Shi Rong-Hua. An Efficient Secure Group Signature Scheme. *Proceedhgs of /EEE TENCONOZ*
9. Jan Camenisch and Jens Groth, Group Signatures: Better Efficiency and New Theoretical Aspects. C. Blundo and S. Cimato (Eds.): SCN 2004, LNCS 3352, pp. 120–133, 2005. Springer-Verlag Berlin Heidelberg 2005
10. J. Camenisch and M. Stadler. Efficient and generalized group signatures. In: *Advances in Eurocrypt'97, LNCS 1233*, pp. 465–479, Springer-Verlag, 1997.
11. Bruce Schneier, Applied Cryptography: 2/e. John Wiley & Sons, Inc, 2002.
12. G. Benenti, G. Casatti, and G. Strini, *Principles of Quantum computation*, *vol. I: Basic Concepts*, World Scientific Publishing, New Jersey, 2004.
13. T. Hwang, K. C. Lee, and C. M. Li, "Provably Secure Three- Party Authenticated Quantum Key Distribution Protocols", *IEEE Transactions on Dependable and Secure Computing*, vol. 4, no. 1, pp. 71-80, 2007.

AUTHOR PROFILE

V. Padmavathi has done her Bachelor of Engineering degree in Computer Science & Engineering, Master of Technology in Computer Science & Engineering. She is pursuing Ph.D in Computer Science & Engineering. She is having ten years of teaching experience and three years in research. Her research area is Quantum Cryptography. She has organized National Level workshops and bridge courses. Padmavathi is a member of Cryptology Research Society of India.

M. Madhavi has done her Bachelor of Engineering degree in Computer Science & Engineering, Master of Technology in Computer Science & Engineering. She has nine years of teaching experience. She has published papers on cloud computing, mesh networks, data mining, network security in international journals. She is a life member of ISTE and CSI. She has organized National Level workshops. Her interested research is network security, cloud computing, hacking.

N. Nagalakshmi has done her Bachelor degree in Computer Science and M.Sc. computers .Now she is pursuing Master of Technology in CSE. She has ten years of teaching experience. She has organized National Level workshops. Her interested areas are Data Mining, Information Security and Database Management Systems.