Optik 142 (2017) 9–12

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Original research article

A restricted quantum deniable authentication protocol applied in electronic voting system

Wei-Min Shi*, Yi-Hua Zhou, Yu-Guang Yang, Nan Jiang

College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China

ARTICLE INFO

Article history:
Received 14 February 2017
Accepted 16 May 2017

Keywords:
Quantum deniable authentication
Restricted
Asymmetric quantum cryptography

ABSTRACT

In some actual network such as electronic voting system, in order to count the number of the participants, the voters cannot deny taking part in a certain voting activity but the voters need deny the content of the voting. However the proposed quantum deniable authentication protocols cannot meet the above specific needs. Hence a restricted quantum deniable authentication protocol based on asymmetric quantum cryptography is proposed in this paper. Utilizing single-qubit rotations and one-way functions, this protocol can provide that the voter can deny the content of the sent message, but cannot deny taking part in electronic voting. Compared with our previous schemes, this new scheme has the remarkable advantages. Finally, security analysis results show that this protocol satisfies the basic security requirements of restricted deniable authentication protocol such as completeness, restricted deniability and no-counterfeiting.

1. Introduction

In 2014, we first proposed a quantum deniable authentication protocol [1]. Based on the property of unitary transformation and quantum one-way function, this protocol can provide that only the specified receiver can identify the true source of a given message and the specified receiver cannot prove the source of the message to a third party by a transcript simulation algorithm, where it can be used in many specialized application such as providing security of negotiation and providing freedom from coercion in electronic voting systems over the internet [2–4]. Afterword, we again proposed a quantum deniable authentication protocol based on signature, namely, a quantum designated verifier signature scheme [5]. In this scheme, the designated verifier cannot prove to a third party that the signature was produced by the signer through a transcript simulation algorithm. However, the two quantum deniable authentication schemes need the entanglement GHZ states and their quantum efficiency is only 1/4. Hence, we proposed a novel quantum deniable authentication protocol without entanglement [6] to improve the efficiency of the previous scheme. In Ref. [6] scheme, the message sender and the specified receiver will first agree a new shared secret key by key update phase with the help of a third center, where only they can encrypt and decrypt the message by using the new shared secret key. However, these schemes don't apply some special application. For example, in electronic voting system, the counter needs some evidence to prove the number of the participants. That is, the voters can deny the content of the voting but he cannot deny participating in a certain voting activity. Thus the restricted deniability is defined in refs. [7,8] to describe this kind of deniability.

* Corresponding author.
E-mail address: shiweimin@bjut.edu.cn (W.-M. Shi).

http://dx.doi.org/10.1016/j.ijleo.2017.05.050
0030-4026/

In this paper, motivated by the above-mentioned cases, we proposed a restricted quantum deniable authentication protocol applied in electronic voting system. The proposed protocol has restricted deniability and satisfies the basis security requirements of deniable authentication protocol.

(1) Completeness: Completeness of an authenticated protocol means that if the voter and the intended counter follow the protocol, the counter can always authenticate the source of the message;

(2) Restricted Deniability: The voter can deny the content of the sent message, but cannot deny taking part in a certain communication.

2. A restricted quantum deniable authentication protocol applied in electronic voting system

Our restricted quantum deniable authentication protocol involves two entities, this is, a voter Alice and a counter Bob who counts the votes. Key generation, Authentication and Verify are included in this protocol.

2.1. Key generation

According the description of Ref. [9], the cryptosystem generates a pair of public and private keys for the voter Alice and the counter Bob, respectively.

Key_generation_1: Choose randomly three positive integers $n_A \square 1$, $n_B \square 1$ and $n_{AB} \square 1$.

Key_generation_2: Choose randomly two integer strings $s_A = (s_1^A, s_2^A, ..., s_N^A)$ and $s_B = \left(s_1^B, s_2^B, \ldots, s_N^B\right)$ of length N, where $s_j^A, s_j^B (j = 1, 2, ..., N)$ are independent from $\square_{2n}$.

Key_generation_3: Generate two qubits sequences $|0_z\rangle^{\otimes N}$.

Key_generation_4: Perform a rotation $\hat{R}^{(j)}(s_j^A \theta_{n_A})$ on the first particle sequence $|0_z\rangle^{\otimes N}$ and perform a rotation $\hat{R}^{(j)}(s_j^B \theta_{n_B})$ on the second particle sequence $|0_z\rangle^{\otimes N}$, where $\theta_{n_A} = \pi/2^{n_A - 1}$ and $\theta_{n_B} = \pi/2^{n_B - 1}$. That is

$$|\Psi_{pk_A}\rangle = \otimes_{j=1}^{N} \hat{R}^{(j)}(s_j^A \theta_{n_A})|0_z\rangle \tag{1}$$

$$|\Psi_{pk_B}\rangle = \otimes_{j=1}^{N} \hat{R}^{(j)}(s_j^B \theta_{n_B})|0_z\rangle \tag{2}$$

At last, the private and public keys of Alice are $d_A = \{n_A, s_A\}$ and $e_A = \{N, |\Psi_{pk_A}\rangle\}$, and the private and public key of Bob are $d_B = \{n_B, s_B\}$ and $e_B = \{N, |\Psi_{pk_B}\rangle\}$. Moreover, Alice and Bob share the secret integer n_{AB}.

2.2. Authentication

According to the following steps, the voter Alice can obtain the authentication information *MAC* of the message *M*.

Authentication_Step1: Alice applies rotation operation on Bob's public key $|\Psi_{pk_B}\rangle$ by her private key d_A, namely

$$|K_{AB}\rangle = \otimes_{j=1}^{N} \hat{R}^{(j)}(s_j^A \theta_{n_A})|\Psi_{pk_B}\rangle_j \tag{3}$$

Authentication_Step2: Alice applies rotation operation by her private key d_A on $|0_z\rangle^{\otimes N}$ and obtains two photon states $|U^j\rangle$ $(j = 1, 2)$, namely

$$|U^i\rangle = \otimes_{i=1}^{N} \hat{R}^{(j)}(s_j^A \theta_{n_A})|0_z\rangle (i = 1, 2; j = 1, 2, ..., n) \tag{4}$$

Authentication_Step3: Alice transforms n-bit classical message M into n-qubit photon states $|Q\rangle = \{|q_1\rangle, |q_2\rangle, ..., |q_n\rangle\}$.

Authentication_Step4: Alice obtains message authentication code *MAC* by $|K_{AB}\rangle$, namely

$$MAC = |f(Q||K_{AB}||U^1)\rangle \tag{5}$$

where $f: |Q\rangle \rightarrow |f(Q)\rangle$ denotes quantum one-way functions proposed by Gottesman and Chuang in Ref [10], and || denotes the concatenate operation.

Finally, Alice sends $\{|U^2\rangle, MAC, M\}$ to Bob by a secure channel such as eavesdropping check mechanism in Refs. [11,12].

2.3. Verify

The counter Bob will execute the following verify steps after receiving $\{|U^2\rangle, MAC, M\}$ from the voter Alice.

Verify_Step1: Bob performs rotation operation by utilizing his private key d_B on Alice's public key $|\Psi_{pk_A}\rangle$, namely

$$|K_{BA}\rangle = \otimes_{j=1}^{N} \hat{R}^{(j)}(s_j^B \theta_{n_B})|\Psi_{pk_A}\rangle_j \tag{6}$$

Verify_Step2: Bob transforms n-bit classical message M into n-qubit photon states $|Q\rangle = \{|q_1\rangle, |q_2\rangle, ..., |q_n\rangle\}$.

Verify_Step3: Bob computes $MAC' = |f(Q||K_{BA}||U^2)\rangle$. If the testing condition $MAC' = MAC$ is satisfied, Bob accepts M. Otherwise, Bob drops the messages M.