Optik 164 (2018) 753–759

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

A scheme on converting quantum signature with public verifiability into quantum designated verifier signature

Wei-Min Shi*, Yan-Mei Wang, Yi-Hua Zhou, Yu-Guang Yang, Jan-Biao Zhang

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

ARTICLE INFO

Article history:
Received 9 February 2018
Accepted 13 March 2018

Keywords:
Quantum signature with public
Quantum designated verifier signature
Deniability

ABSTRACT

To solve the conflict of certification and privacy such as the electronic election, online bidding and other such network applications, a quantum signature scheme with public verifiability is converted into a designated verifier signature by introducing the classic ideas of Diffie-Hellman (DH) key exchange, in which the signer first generates a public verifiability initial signature with the help of a trusted third party according the quantum signature scheme, and then the signer and verifier agree a secret key, finally generates the value of signature through the secret key shared between the signer and verifier and the initial signature. This designated verifier signature scheme can make that only a verifier designated by a signer can verify the "validity of a signature" and the designated verifier cannot prove to a third party that the signature was produced by the signer or by himself through a transcript simulation algorithm. The final research results will not only provide a new way for the research methods of quantum designated verifier signature, but also provide a useful supplement for identity privacy protection methods.

1. Introduction

A general digital signature scheme has the characteristics that signatures can be universally confirmed, and anyone who know the signer's public key can verify the validity of the signature. With the rapid development of computer and internet, a general digital signature scheme cannot meet the requirements of various special environments. For example, in e-commerce, if each bank issues its own electronic money signed by using the ordinary digital signature scheme, the identity of the bank to which the electronic money belongs will be known by anyone in each transaction, so the public information may make the opponent obtain business secrets. Obviously, banks are reluctant to let each consumer know this information. There also exist the conflict of certification and privacy such as the electronic election, online bidding and other such network applications.

In order to solve the above problem, the designated verifier signature scheme is first presented by Jakobsson et al. [1]. In this scheme, a signer S can confirm to the designated verifier V that he has signed a declaration and that V cannot prove the validity of the signature to the other party because V has the capability of simulating the S signature. In quantum cryptography, the research of quantum signatures is mainly focused on the following two aspects: (1) Quantum Arbitration Signatures [2–10]; (2) Special Quantum Signatures [11–23]

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

https://doi.org/10.1016/j.ijleo.2018.03.048
0030-4026/

Firstly, refs. [2–5] proposed a quantum arbitration signatures(QAS) based on B, χ-type, Cluster states, respectively. In order to improve the quantum efficiency, an efficient QAS based on single photon is proposed in ref. [6] by combining quantum cryptographic techniques and some ideas in classical cryptography, and a QAS without entangled states is proposed in ref. [7] by using a classical hash function and random numbers, in which the secret keys of signer and receiver can be reused. Refs. [2–5,7] exit that the receiver can forge the sender's signatures under the known message attack and the sender can successfully disavow any of her/his signatures by a simple attack because of these scheme based on the Leung quantum one-time pad (L-QOTP) algorithm. Hence, ref. [8] designs a new QOTP algorithm relying largely on inserting decoy states into fixed insertion positions, and then present an AQS scheme with fast signing and verifying by using the new QOTP algorithm. Ref. [9] based on the chained CNOT operations encryption presents a QAS which cannot be forged and disavowed under the existing attacks. Unfortunately, previous schemes cannot against Trojan horse attack and DoS attack, so ref. [10] propose an improved arbitrated quantum signature to address these secure issues without entanglement. The above AQS schemes belongs to the discrete-variable quantum cryptography, so ref. [11] presents a AQS based on the continuous-variable (CV), namely, the generation of the shared keys via the CV-based quantum key distribution (CV-QKD) and the implementation process of the CV-based quantum teleportation.

Secondly, in order to meet the requirements of various special environments such as electronic election and e-commerce, some special quantum signature schemes were presented in refs. [12–25], where mainly study in quantum blind signature (QBS) [12–18]. For example, refs. [12–14] with a trusted third party present based on GHZ, Bell, Cluster states, respectively, in which meet the trusted third party with online functionality. In the trusted third party with offline functionality, a security QBS was presents by quantum key distribution based the quantum one-time pad. Afterword, ref. [16] proposed a quantum blind dual-signature scheme without arbitrator. Different from other schemes, legal messages are signed not only by the blind signatory but also by the sender in the signing phase. To overcome the drawback of unlinkablity in the previous schemes, ref. [17] proposed a new quantum blind signature based on Bell states with the help of an authentic party through a method to inject a randomizing factor into a message when it is signed by the signer and then get rid of the blind factor from the blinded signature when it is verified by the verifier. Even the message owner publishes the message-signature pair, the signer cannot identify the association between the message-signature pair and the blind signature he generated. However, these QBS schemes just consider the situation for bit messages, and the signing-verifying of one-bit modality. So, their signature efficiency is very low. Ref. [18] propose a scheme based on an application of Fibonacci-, Lucas- and Fibonacci-Lucas matrix coding, in which can sign a large number of digital messages every time. Moreover, some mixed signatures were presented such as quantum proxy signature [19,20], quantum group signature [21,22], quantum proxy blind signature [23–25] and quantum proxy group signature [26].

The above schemes have a common characteristic that the verifier verifies the signature by using shared key with the signer, so these quantum signature schemes can be verified by a designated person, but they aren't the real traditional designated verifier signature schemes, because the designated person hasn't the capability to efficiently simulate a signature which is indistinguishable from a signer, which cannot satisfy the signer's deniability.

Therefore, by introducing the classic ideas of Diffie-Hellman (DH) key exchange, a quantum signature scheme with public verifiability will be converted into a quantum designated verifier signature, in which can make that only a verifier designated by a signer can verify the "validity of a signature" and the designated verifier cannot prove to a third party that the signature was produced by the signer or by himself through a transcript simulation algorithm. The above research results will not only provide a new way for the research methods of quantum designated verifier signature, but also provide a useful supplement for identity privacy protection methods used in the electronic election, online bidding and other such network applications.

The rest of the paper will be constructed as follow: Section 2 gives the basis security requirements of designated verifier signature. Section 3 introduces the quantum signature scheme with public verifiability. Section 4 gives details of the quantum designated verifier signautre scheme by converting a quantum signature scheme with public verifiability. The security is analyzed in Section 5. Finally, a short conclusion is given in Secion 6.

2. The basis security requirements of designated verifier signature

As defined in [27,28], a DVS scheme should satisfy several main security properties, they are described as follows:

(1) Correctness: if the signer properly produces the DVS signature by the sign algorithm, then the produced signature must be accepted by the DVVerify algorithm;
(2) Non-Transferability: The non-transferability means that any designated verifier cannot transfer the conviction to any third party, that is, the designated verifier cannot prove to a third party that the signature was produced by the signer or by himself. This is accomplished by a transcript simulation algorithm through which the designated verifier can produce an indistinguishable signature from the one generated by the real signer;
(3) Source Hiding: Given a signature on message M, it is infeasible to tell apart the signature is produced by the original signer or the designated verifier on earth even if one knows both the secret keys;
(4) Unforgeability: It is computationally infeasible to construct a valid DVS signature without the knowledge of the private key of either the signer or the designated verifier.