Future Generation Computer Systems ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

Quantum digital signature for the access control of sensitive data in the big data era

Lirong Qiu *, Feng Cai, Guixian Xu

School of Information Engineering, Minzu University of China, Beijing, China

HIGHLIGHTS

- We introduce partially trusted arbitrator to quantum digital signature.
- We apply the quantum digital signature method to cognitive area.
- The arbitrator cannot know the signed message, keep the message safe.
- The signature cannot be forged by an attacker.
- The signer cannot repudiate his signature if he indeed signed it.

ARTICLE INFO

Article history:
Received 22 January 2018
Received in revised form 19 March 2018
Accepted 26 March 2018
Available online xxxx

Keywords:
Quantum
Signature
Access control
Healthcare

ABSTRACT

In our paper we focus on the application of quantum digital signature in the access control of sensitive data such as those data appears in areas like healthcare in order to protect users personal information. There are three parties in our protocol: the signer, the arbitrator and the receiver. Different from most existing protocols developed in arbitrated quantum signature, in which the arbitrator is either assumed to be honest or dishonest, in our protocol we assume the arbitrator is partially honest in the sense that the arbitrator is honest-but-curious. The quantum protocol we propose in this paper have various advantages over existing protocols of the same purpose. The technology we proposed can guarantee the unconditional secure, and it is implementable by the current technology, so the method we proposed can guarantee the security of user' personal information in the big data era.

1. Introduction

In our paper, we aim to propose a method that the arbitrator is partially trust, which can guarantee unconditional secure.

In attribute-based access control systems, access control decisions are based on attributes of users, which in turn are documented by certificates issued by some certificate authorities. Each certificate authenticates the user's attributes such as birthdate, income, credit card information, and so on. In cryptography, certificates are usually created by digital signatures.

Digital signatures are widely used to ensure the identity of a signer, the authenticity of a message and to guarantee that a message is transferable. In recent years, quantum signature has become a growing area of research [1–3]. There are two requirements that a secure access control scheme must satisfy: one of them is that the signature must be safe so that it cannot be forged by the people who want stole the information, the other is that the message cannot be disavowal by the signer and the receiver.

The existing quantum signature schemes [1,4,2,5,6] assume the arbitrator to be either trusted or untrusted. However, we believe on the one hand it is not realistic to assume the arbitrator to be fully trusted, on the other hand it is over concerned to assume the arbitrator to be completely untrusted. We therefore assume the arbitrary to be partially trusted and develop a quantum signature protocol under such assumption. Under this assumption, our protocol involves an arbitrator who helps to verify a signature but throughout the protocol, the arbitrator does not know the content of the signature. This feature fits quite well with the context of access control of sensitive data such as healthcare. We give the definition of Quantum Digital Signature and Access Control of Sensitive Data, as well as some example of the scheme application in below.

Quantum Digital Signature: Quantum Digital Signature refer to the quantum mechanical equivalent of either a classical digital signature, more generally, a handwritten signature on a paper document. Like a handwrite signature, a digital signature is used to protect a document, such as a digital contract, again forgery by an another party or by one of the participating parties. There are three

* Corresponding author.
E-mail address: qiu_lirong@126.com (L. Qiu).

https://doi.org/10.1016/j.future.2018.03.053
0167-739X/

requirements for a good signature scheme: Firstly, the scheme has to provide security against tampering by eht sender, the receiver, and a third party; Secondly, the scheme must satisfy that creating a signed message has to be easy; Finally, every recipient has to get the same answer, when testing the message for validity.

Access Control of Sensitive Data: Access control is the selective restriction of access to a place or other resource. The act of accessing may mean requiring entering or permission to access the resources that is called require Authorization. Based on this, when people transfer sensitive data in the process, we can call the access control as the access control of sensitive data.

Example 1. Suppose according to the policy of social welfare, some special healthcare service are offered to some disabled or unhealthy citizens. To access to those special service, the applicant is asked to provide a certificate issue by some certificate authorities to indicate their disease. Bob is a man with a disease which qualifies his access to the special healthcare service. But Bob prefer to disclose his disease to as less people as possible, because the disease is HIV (or some other notorious disease, or some awkward unhealthy such as sexual inability). Then Bob would prefer a certificate which does not disclose his disease.

Example 2. According to the provisions of the Patent Law, patent rights must be issued by state organs. Namely, to obtain the patent right, the applicant shall apply to the national patent office for approval, when the patten office passed, the applicant will get the certificate. Nancy is a women who owns an invention that has unique innovations in one area and the patent complies with all the documents. Nancy want to apply for a patent, but she prefer disclose the patent file to as less people as to prevent disclosure. Then Nancy would prefer a certificate which does not disclose her patent file.

We all know that in the era of big data, users' information, such as dietary habits, medical conditions, driving information etc., will more or less disclose the privacy of users. We have to frequently exchange information with people in this era, but we do not want to let the information leaked, the method we proposed provide a feasible method for this problem.

This paper is organized as follows. In Section 2 we review the background knowledge on quantum computation to make this paper self-contained. Then in Section 3 we describe our proposed quantum protocols for digital signature. Section 4 we introduce the applications of the Signature in Cognitive IoT, and in Section 5 we discuss related works, besides highlighting the improvements introduced by our proposal with respect to such works. Finally, in Section 6 we draw the conclusions of the paper.

2. Discussion and related work

In Cryptography domain, one of the most important part is the whether the message is reliable to its receiver. A Signature a specific people has signed or noted to a information appears to be useful in many cases. Under this purpose, as an addition to information to make sure the message can neither be repudicated by the signer nor forged by an attacker, Signature schemes are developed rapidly so far [4].

Quantum cryptography is related to many classical cryptography and quantum theory. It is focus on provide unconditionally secure information communication with the help of quantum effects. In the process of information exchange, in order to guarantee the effectiveness of this process, we need to encrypt. But this is not enough, if someone forge the Signature, it must be found in time, so the arbitrator is introduced. The arbitrator is to detect whether the signatures have been altered or forged by attackers during the transmission of information.

Many quantum signature schemes [1,4,2,5,6] have been developed in recent years. An important issue in cryptography is the credibility of arbitration. An influential signature protocol, named *arbitrated quantum signature*, which proposed by Zeng and Keitel [1]. Zou and Qiu [2] simplifies the protocol of Zeng and Keitel by achieving arbitrated quantum signature without using quantum entangled states. A trusted arbitrator is assumed in both [1] and [2]. Li et al. [7] give an example of scheme which using two-particle entangled Bell states [1].

Deniel et al. [8] present a quantum digital signature scheme in which the security is based on fundamental principles of quantum physics, the method allows a sender can sign a message that the signature can be validate by many different people, and the people can easily figure the message came from the Sender or deny the tempered signature. In their study, they make each recipient of the process own the copy of the sender's "public key", but they only own the set of quantum states, only the sender know the exact identity. Jeong et al. [9] thought that the previous study assume the quantum signature schemes implemented by the third party, based on this condition, they point out that the previous schemes provide security only against a total break attack, and the message transfer process is not unconditional secure. They provide a simple method to cover the potentional loophole.

In real applications, however, typically there can hardly find a person who can get all of the persons trusted in a commercial activity. Ingemarsson and Simmons [10] indicate that in commercial or international application, nobody can get trusted by all person. Yang et al. [11] believe in signature scheme which need arbitrated, the security of the information exchange process is heavily needs on the trustworthiness of arbitrators. And the Arbitrator can also get the influence of the circumstance, that is, the arbitrated schemes in the previous study that believe in the arbitrator is fully trusted cannot guarantee the arbitrator safe. Consider this situation, they proposed a situation that the arbitrator cannot be trusted in signature scheme. Under the same purpose, Zou et al. [5] study the issue of an untrusted arbitrator in quantum arbitrated signature and illustrate it is insecure with an untrusted arbitrator in AQS scheme, and proposed the scheme can be a good solution to the two problems that the signer who is dishonest can deny the signature and when the malicious attacker receive the signature message, he can easily forge the signature.

The method can be applied in many field, Xiao et al. propose a self-evolving trading strategy based on neural network for futures market [12], Shi et al. propose a method which through using clinical notes to assess the rank of risk [13], Zhang et al. proposes an SDN-based approach to develop a safety-oriented vehicular *CAN (SOVCAN)* [14], a hybrid recommendation algorithm, on the basis of time sequenced topic and social relations [15], the information in the above field all can be protected by the method we proposed.

As we have mentioned in the introduction of this paper, we believe that assuming an untrusted arbitrator is also not realistic. As far as we know, our paper is the opening one which studies quantum digital signature with partially trusted arbitrator.

3. Terminology

3.1. Basic quantum computation

3.1.1. Qubits

Quantum bit is the fundamental of the quantum information, abbreviated as short. Qubits are the basis units of message in the process of quantum information, just like in classical message processing, the bits are the basis units of information.

Please cite this article in press as: L. Qiu, et al., Quantum digital signature for the access control of sensitive data in the big data era, Future Generation Computer Systems (2018), https://doi.org/10.1016/j.future.2018.03.053.