Chapter 18
Group Signature System Using Multivariate Asymmetric Cryptography

Sattar J. Aboud
University of Bedfordshire, UK

ABSTRACT

This chapter presents a new group signature scheme using multivariate asymmetric cryptography. Compared with the exited signature schemes, the proposed scheme is applicable to e-voting schemes and can convince the requirements of e-voting schemes because it has two important characteristics, traceability and unlinkability. Traceability denotes that a group director cannot open the signature alone. He has to collaborate with a verifier to disclose an identity of the signer. Unlinkability denotes that the group signature can be split accordance to time durations. Then signatures are linkable in the same time range but un-linkable between dissimilar time periods. Therefore, the count authority can notice the double votes prior to opening them. Thus, there are two features in the proposed signature for count and supervision authority. Also, the size of signatures and the calculation overhead are private from the group members in the proposed scheme. So, it is efficient for large groups.

INTRODUCTION

The group signature lets the group of people to sign document anonymously on behalf of other group. In the case of the dispute, the designated director can open the signature to disclose the identity of its generator. To the degree that we know the majority of the group signatures are relied on the known schemes, such as RSA and ElGamal. However, these schemes could be broken when quantum computers appear. The problem typed multivariate asymmetric key cryptography is the notable option to common asymmetric schemes for its possible to withstand future attacks of quantum computers. The initial group signature scheme relied on the multivariate asymmetric cryptography that is introduced in this chapter.

DOI: 10.4018/978-1-5225-7492-7.ch018

The proposed scheme have two extraordinary attributes. In the first one, the group signatures are divided to dissimilar time intervals. The signatures are linkable in the same time interval, but un-linkable among dissimilar time intervals. In the second one, the duties of the group director is restricted. The group director does not allow him to open the signature without the assist from the verifier. These attributes are vital in selected uses such as e-voting schemes. The concept of the proposed scheme is straightforward and its security bases on both an arbitrary hash function and an isomorphism of polynomial problem.

In 1991, Chaum-Heyst presented the first idea of group signature. The group signature scheme give permission to the group of people to sign the documents on behalf of the group. The verifier can only inform that the signature is signed by the person from the group, but cannot determine the identity of the signer. In addition, the verifier cannot differentiate if the two signatures are published by the same person of the group. But, in special case such as official dispute, the designated group director can open the signature to disclose the identity of its generator. At the same time, no one even the group director can forge the signature of other group people.

The characteristics of group signature construct it smart for many specific applications, like e-voting, e-cash and e-games. For instance, in e-voting systems, the electorate are not allowable to vote many times. Thus the count authority should be capable to differentiate the reduplicate votes without opening an election. Furthermore, there is a rule exist supervision authority to constraint the duties of the count authority and promise the fairness of the voting in the voting system. Thus, the group signature schemes cannot be employed the e-voting systems straight. Most of the group signatures are using known cryptography schemes, such as RSA and ElGamal. However, the algorithm proposed by Shor illustrates that solving the factoring integers and the discrete logarithms can be achieved in polynomial time on the quantum computer. If the quantum computers become a reality, the common asymmetric key cryptography under these problem, such as RSA and Elliptic curve will be broken. multivariate asymmetric key cryptography is studied to be one of the best option. The security basis of multivariate asymmetric key cryptography is the information that solving the set of multivariate polynomial formulas over the finite field is the NP-hard problem. Quantum computers do not seem to have any benefit if managing this NP-hard problems, and it appears that we cannot recover the solution to the set of polynomial formulas efficiently even in the future. Furthermore, multivariate asymmetric key cryptography schemes are more efficient than common asymmetric key cryptography. It makes them appropriate for restricted computing tools, for example smart cards. Different multivariate asymmetric key cryptography schemes have been presented.

QUANTUN COMPUTING THREATENS

Quantum computing threatens definite techniques and does not threaten others. Public key encryption, is being used considerably for securing the internet payments, banking transactions, and also emails and webs. The majority of today cryptography schemes are using public-key cryptography, that is in fact secure anti-attacks from contemporary computers.

Suppose that quantum cryptography can easily break many schemes by inverse the computing private-keys and quicker than the classical computer. While quantum cryptography are still in their early stages and non- equipped, with publicly known new quantum computers, small to attack traditional cryptography algorithms, many public authorities have begun to know the risk included if this technology becomes the practical applications. Since quantum computers is to process huge amounts of information in the quite short of time.