A Study of Threshold Signature and Authenticated Encryption Schemes based on the Elliptic Curve Cryptosystem

黃國軒、陳澤雄、余心淳

E-mail: 9225039@mail.dyu.edu.tw

ABSTRACT

The concept of threshold is broadly used in the group-oriented signature schemes. So far there are numerous studies on the investigation and development of threshold signature. Since the idea of threshold verification is initiated in recent years, it increasingly attracts many researchers' attentions. In the thesis, these two ideas are integrated into a specified-verifier group-oriented threshold signature scheme. In the proposal, no matter the generation and verification of signature, a threshold value is used in qualifying the number of participants instead of all members' participance. Moreover, for the part of verifier, no one except for the specific verifier is able to verify a signature. Such a characteristic can be fit to some certain situation. Furthermore, a new type of authenticated encryption scheme is proposed for achieving the security requirements of privacy, integrity, and authenticity at the same time. Such a kind of scheme is not only provided with the functions and characteristics of the above-mentioned threshold signature and threshold verification schemes, but also with the low-operation and low-communication advantages. Besides, take the size of messages into account, especially the over-large messages, the concepts of labor division and message linkage are inducted into the proposal ─ a division-labor signature threshold authenticated encryption scheme with message linkage. In the proposal, an over-large message is divided into several readable sub-messages in advance so as to assign these sub-messages to the participant for being examined and signed. Following the way, the workload of signer can be reduced, and the efficiency of performance is also promoted. According to the characteristic of message linkage, a verifier is able to determine whether the content of received group-signature block has been maliciously permuted or altered. For offering higher efficiency in performance, the elliptic curve cryptosystem is used in the proposals. The security is based on the difficulty for solving the elliptic curve discrete logarithm problem.

Keywords : threshold signature ; authenticated encryption scheme ; division-labor signature ; message linkage ; elliptic curve cryptosystem

Table of Contents

Chapter 1 Introduction

Chapter 2 The Elliptic Curve Cryptosystem

Chapter 3 Integrated Application of Threshold Signature and Threshold Verification

Chapter 4 An Authenticated Encryption Scheme

Chapter 5 Extend Application of Division Labor and Message Linkage to Authenticated Encryption Scheme

Chapter 6 Conclusions

REFERENCES


[35] Lee, W.B. and Chang, C.C., "Authenticated encryption schemes with linkage between message blocks," Information Processing Letters,


