Practical Threshold Signatures Without Random Oracles

Jin Li[1,⋆], Tsz Hon Yuen[2], and Kwangjo Kim[1]

[1] International Research center for Information Security (IRIS)
Information and Communications University(ICU)
103-6 Munji-Dong, Yuseong-Gu, Daejeon, 305-732, Korea
sysjinli@hotmail.com, kkj@icu.ac.kr
[2] School of Information Technology and Computer Science
University of Wollongong, NSW 2522 Australia

Abstract. We propose a secure threshold signature scheme without trusted dealer. Our construction is based on the recently proposed signature scheme of Waters in EUROCRYPT'05. The new threshold signature scheme is more efficient than the previous threshold signature schemes without random oracles. Meanwhile, the signature share generation and verification algorithms are non-interactive. Furthermore, it is the first threshold signature scheme based on the computational Diffie-Hellman (CDH) problem without random oracles.

Keywords: Threshold Signature, Bilinear groups, CDH problem.

1 Introduction

Digital signatures can be produced by a group of players rather then by one party by using a threshold signature scheme. In contrast to the regular signature schemes where the signer is a single entity which holds the secret key, in (k, n)-threshold signature schemes the secret key is shared by a group of k players. In order to produce a valid signature on a given message m, individual players produce their partial signatures on that message, and then combine them into a full signature on m. A distributed signature scheme achieves threshold k, if no coalition of $k-1$ (or less) players can produce a new valid signature, even after the system has produced many signatures on different messages. A signature resulting from a threshold signature scheme is the same as if it was produced by a single signer possessing the full secret signature key. In particular, the validity of this signature can be verified by anyone who has the corresponding unique public verification key. In other words, the fact that the signature was produced in a distributed fashion is transparent to the recipient of the signature.

Threshold cryptography and secret sharing have been given considerable attention since they were proposed. The first threshold secret sharing schemes,

⋆ This work was partially supported by the 2nd stage of Brain Korea 21 Project sponsored by the Ministry of Education and Human Resources Development, Korea.

W. Susilo, J.K. Liu, and Y. Mu. (Eds.): ProvSec 2007, LNCS 4784, pp. 198–207, 2007.

based on the Lagrange interpolating polynomial and linear project geometry, were proposed by Shamir [11]. Many efficient digital signature and threshold signature schemes are proved secure in the random oracle model. However, several papers proved that some popular cryptosystems previously proved secure in the random oracle are actually provably insecure when the random oracle is instantiated by any real-world hashing functions [2]. Therefore, provably secure threshold signature scheme in the standard model attracts a great interest.

Related Work. Recently, [13] gave the first threshold signature without random oracles. However, the threshold signature scheme requires that the users generate the signature interactively. Meanwhile, the correctness of these generated signature shares cannot be verified. Ideally, there is no other interaction in the threshold signature scheme, namely the players need not talk to each other during signing. Such threshold systems are called non-interactive. Often one requires that threshold signature be robust [8], namely if threshold signature fails, the combiner can identify the signing players that supplied invalid partial signatures. In [12], a practical threshold signature scheme based on RSA was proposed, which is non-interactive. However, it required a trusted dealer.

Contributions. In this paper, we propose a new practical threshold signature scheme without trusted dealer. The threshold signature has the following properties:

1. It is provably secure without relying on the random oracle model;
2. Signature share generation and verification are completely non-interactive;
3. The scheme is the first threshold signature scheme based on the CDH problem without random oracles;
4. Signature share generation and verification algorithms are very efficient.

2 Preliminaries

2.1 Security Definitions and Notions

We shows the definition as follows:

Definition 1. *A (k, n)-threshold signature scheme consists of algorithms (DKG, SS, SV, SC, Vrfy). These algorithms are specified as follows:*

1. *DKG is the distributed key generation algorithm. On input security parameter 1^λ, k, n it outputs public key pk and secret key sk. Meanwhile, it also outputs the private value sk_i and verification key vk_i of player i such that the values $(sk_1, \cdots, sk_n)$ form a (k, n)-threshold secret sharing of sk. The public output of the protocol contains the public key pk and verification key $VK = (vk_1, \cdots, vk_n)$.*
2. *SS is the signature share generation algorithm run by player i, on input secret share sk_i, a message m, it returns σ_i as the shared signature.*
3. *SV is the signature share verification, on input public key pk, verification key vk_i, a message m, σ_i, output 1 if it is valid. Otherwise, output 0.*