On the Security of Probabilistic Multisignature Schemes and Their Optimality

Yuichi Komano[1], Kazuo Ohta[2], Atsushi Shimbo[1], and Shinichi Kawamura[1]

[1] Toshiba Corporation,
1, Komukai Toshiba-cho, Saiwai-ku, Kawasaki 212-8582, Japan
{yuichi1.komano,atsushi.shimbo,shinichi2.kawamura}@toshiba.co.jp
[2] The University of Electro-Communications,
Chofugaoka 1-5-1, Chofu-shi, Tokyo 182-8585, Japan
ota@ice.uec.ac.jp

Abstract. We first prove that the following three probabilistic multisignature schemes based on a trapdoor permutation have tight security; PFDH (probabilistic full domain hash) based multisignature scheme (PFDH-MSS), PSS (probabilistic signature scheme) based multisignature scheme (PSS-MSS), and short signature PSS based multisignature scheme (S-PSS-MSS). Second, we give an optimal proof (general result) for multisignature schemes, which derives the lower bound for the length of random salt. We also estimate the upper bound for the length in each scheme and derive the optimal length of a random salt. Two of the schemes are promising in terms of security tightness and optimal signature length.

Keywords: Multisignature, Aggregate signature, Provable security, Optimal security, Random oracle model

1 Introduction

1.1 Background

The notion of multisignatures was derived by Itakura and Nakamura [5], and a great deal of research has been done on this subject. In multisignature schemes, two or more signers generate one multisignature for some message: the same result is accomplished by concatenating each signer's signature; however, the multisignature scheme decreases the (total) length of the signature and/or the signing (verification) costs.

In respect of provably secure multisignatures (in the sense of the security model of [9]) based on a trapdoor (one-way) permutation (*e.g.*, RSA), Mitomi and Miyaji in Appendix A of [10] and Kawauchi and Tada [6] proposed FDH based multisignature scheme and probabilistic multisignature scheme based on PSS, respectively. In these schemes, the signing order is restricted by a key length of each signer. Moreover, as the signing order proceeds, the computation cost is enlarged (because of the increase of key length).

E. Dawson and S. Vaudenay (Eds.): Mycrypt 2005, LNCS 3715, pp. 132–150, 2005.

With regard to optimal security and optimal length of a random salt utilized in probabilistic signature schemes, Coron [4] introduced the notion of "reduction" and claimed that (1) the security of PSS is not improved if the length of a random salt exceeds a certain value (upper bound), (2) a lower bound for the length of a random salt, with which we guarantee the security of probabilistic signature schemes (general result), is derived from the optimal proof utilizing the notion of the "reduction", and, (3) the upper bound (of PSS) derived from (1) equals the lower bound derived from (2); which gives the optimal length of a random salt.

1.2 Our Contribution

This paper deals with three multisignature schemes based on the trapdoor permutation; PFDH (probabilistic full domain hash, [4]) based multisignature scheme (PFDH-MSS, [7]), PSS (probabilistic signature scheme, [2]) based multisignature scheme (PSS-MSS), and short signature PSS based multisignature scheme (S-PSS-MSS). The construction of PFDH-MSS and PSS-MSS is a similar to that of the sequential signature scheme (hereafter, we call the scheme FDH-MSS[1]) based on the full domain hash (FDH, [1]) constructed by Lysyanskaya et al. [8]. For simplicity, we give a description of the schemes with the RSA function [11] as the trapdoor permutation in section 3.

We first prove that these three multisignature schemes have tight security under the random oracle model [1]. We then show that PFDH-MSS and S-PSS-MSS have optimal length of signature; an increase of signature size per signer is the same as the length of a random salt. Since the random salt is necessary for ensuring tight security and the salt should be recovered in the verification step, it is inevitable that the length of signature is enlarged by more than or equal to the length of random salt per signer; namely, the signature size in each scheme is optimal.

Second, we apply Coron's technique (using "reduction") to the multisignature schemes and estimate the optimal length of a random salt utilized in the schemes. We first show an optimal proof (general result) which derives the lower bound for the length of a random salt with which we ensure the security of multisignature scheme. Then, we prove the security of the schemes and derive the optimal length of a random salt. It is of theoretical interest that the optimal length of a random salt utilized in the multisignature schemes is equal to the optimal length of a random salt utilized in PSS (estimated in [4]).

1.3 Related Work – Sequential Aggregate Signatures

In 2003, Boneh et al. [3] proposed an aggregate signature scheme which is recognized as one of the generalizations of the multisignature scheme. The aggregate signature scheme is a signature scheme which can unify several signatures generated by plural signers on different messages. The original aggregate signature

[1] Sequential aggregate signatures are essentially the same as message flexible multisignature schemes. See the section 1.3 for detail.