Aggregate Proxy Signature and Verifiably Encrypted Proxy Signature

Jin Li[1,⋆], Kwangjo Kim[1], Fangguo Zhang[2], and Xiaofeng Chen[3]

[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] Department of Electronics and Communication Engineering
Sun Yat-Sen University, Guangzhou, 510275, P.R. China
[3] Department of Computer Science
Sun Yat-Sen University, Guangzhou, 510275, P.R. China

Abstract. An aggregate signature is a single short string that convinces any verifier that, for all $1 \leq i \leq n$, signer i signed message m_i, where the n signers and n messages are distinct. The main motivation of aggregate signatures is compactness. In this paper, the concept of aggregate proxy signature (APS) is first proposed to compact the proxy signatures. Furthermore, a concrete APS scheme is constructed, which can be proved to be secure under the security model of APS. Additionally, as an application of APS, the concept of verifiably encrypted proxy signature (VEPS) is also first proposed in this paper, which can be used in contract signing. The VEPS allows the original signer to delegate another to sign the contract on its behalf. Finally, a VEPS construction is derived from the APS, which can be easily proved to be secure from the security of APS.

Keywords: Proxy signature, Aggregate signature, Random oracle, Bilinear pairings.

1 Introduction

A proxy signature protocol allows an original signer to delegate its signing power to another entity, called proxy signer, to sign messages on its behalf. The delegated proxy signer can compute a proxy signature that can be verified by anyone with access to the original signer's public key. Proxy signatures have many practical applications such as in distributed system etc. [10] and are one of important cryptographic protocols. The concept of proxy signature was first introduced by Mambo, Usuda, and Okamoto [8] in 1996. After Mambo et al.'s first scheme was published, many various types of proxy signature schemes have been proposed such as short proxy signature scheme [5,7], one-time proxy signatures [16]. Also, there are a lot of proxy signature schemes were found flaws such as [11].

⋆ 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. 208–217, 2007.

The main reason is the lack of formal security model. Until 2003, the formal security model was proposed in [1]. In this security model, a public key infrastructure setting (PKI) is also assumed, where each entity holds a public and secret key pair.

The notion of aggregate signature schemes was introduced in 2003 by Boneh, Gentry, Lynn and Shacham [3]. Basically, aggregating signatures means compressing n signatures on n distinct messages from n distinct users into a unique (shorter) signature. This is useful in many real-world applications. For example, certificate chains in a hierarchical PKI of depth n consist of n signatures by n different CAs on n different public keys. By using an aggregate signature scheme, this chain can be compressed down to a single aggregate certificate. After the concept of aggregate signatures was proposed, many types of aggregate signatures have been presented such as identity-based aggregate signatures [4], sequential aggregate signatures [13].

In this paper, the concept of aggregate proxy signature (APS) is first proposed. Consider the following situations: n proxy signers have generated n proxy signatures on n different messages on behalf of the same original signer. To verify these proxy signatures, the ordinary method is to verify them one by one, which costs large storage and computation. Reducing the amount of memory required to store these proxy signatures and the computational time required to verify their validity is the motivation for the concept of APS. An APS is obtained from n different initial proxy signatures, ideally in such a way that: (1) the length of the aggregate proxy signature is smaller than the sum of the length of the n initial proxy signatures; (2) verifying the correctness of the aggregate proxy signature costs less than verifying the n initial proxy signatures one by one. If an aggregate proxy signature is verified as valid, then the receiver is convinced that the n initial signatures are valid. On the other hand, if the aggregate signature is invalid, the receiver is convinced that some initial proxy signature is not valid.

Next, we show an application of APS to verifiably encrypted proxy signature (VEPS). It is known that verifiably encrypted signatures can be used in applications such as online contract signing [8]. Suppose Alice wants to show Bob that she has signed a message, but does not want Bob to possess her signature of that message. Alice can achieve this by encrypting her signature using the public key of a trusted third party, and sending this to Bob along with a proof that she has given him a valid encryption of her signature. Bob can verify that Alice has signed the message, but cannot deduce any information from her signature. Later, in the protocol, if Alice is unwilling or unable to reveal her signature, Bob can ask the third party to reveal Alice's signature.

However, consider the following situation: If either Alice or Bob is busy, they can delegate their signing power to the other party, which is called as proxy signer, to sign the contract on behalf of him or her. So, the concept of VEPS is first presented in this paper to solve this problem. In this case, the proxy signer of Alice, for example, wants to show Bob that it has signed a message on behalf of Alice, but does not want Bob to possess its proxy signature on that message. The proxy signer can achieve this by encrypting its proxy signature using the