Information Sciences 227 (2013) 102–115

Contents lists available at SciVerse ScienceDirect

Information Sciences

journal homepage: www.elsevier.com/locate/ins

A new proxy signature scheme for a specified group of verifiers ☆

Min-Shiang Hwang [a], Cheng-Chi Lee [b,c,*], Shiang-Feng Tzeng [d]

[a] Department of Computer Science and Information Engineering, Asia University, No. 500, Lioufeng Road, Wufeng Shiang, Taichung, Taiwan, ROC
[b] Department of Library and Information Science, Fu Jen Catholic University, 510 Jhongjheng Road, Sinjhuang City, Taipei County 24205, Taiwan, ROC
[c] Department of Photonics and Communication Engineering, Asia University, No. 500, Lioufeng Road, Wufeng Shiang, Taichung, Taiwan, ROC
[d] Department of Information Management, Chaoyang University of Technology, 168 Gifeng E. Road, Wufeng, Taichung County 413, Taiwan, ROC

ARTICLE INFO

Article history:
Received 24 June 2008
Received in revised form 11 April 2011
Accepted 10 November 2012
Available online 7 December 2012

Keywords:
Data security
Digital signature
Proxy signature
Threshold proxy signature

ABSTRACT

In this article, we shall propose a $((t_1, n_1), (t_2, n_2))$ proxy signature scheme with (t_3, n_3) shared verification based on the RSA problem. In this scheme, any t_1 original signers can delegate the signing capability to the proxy group. After that, any t_2 proxy signers can sign a message on behalf of the original group for a specified verifier group. Only any t_3 verifiers together can check the validity of the proxy signature from the proxy group. The proposed scheme satisfies all proxy requirements of proxy signatures. Furthermore, the actual original signers and proxy signers can be individually identified in our scheme.

1. Introduction

Digital signature is developed to enable a signer to generate the signature for a message by using her/his private key [2,13,32,34,37,40,52,54]. To check the validity of the signature, the corresponding public key of the signer should be employed. Generally speaking, a digital signature scheme should provide such important cryptographic function as authentication, integrity and non-repudiation. However, ordinary digital signature schemes [7,8,10,20,29,41] are not quite enough to satisfy some practical needs. Let us consider a typical example of the proxy situation in a business organization. Suppose a manager in a computer company needs to go on a business trip. In other words, she/he is not at her/his company and thus is not able to do the routine of signing a number of documents. So, she/he indeed needs a capable and trustworthy secretary to do it instead. Now, the secretary becomes a proxy signer on behalf of the manager. This is a typical case of what happens in our lives every day. Mambo et al. [35,36] first considered this interesting problem in 1996. It is referred to as the "proxy signature". The "proxy signature" provides a solution to the problem with the delegation of signing capability. The designated proxy signer generates a signature on behalf of the original signer. So far, many proxy signature schemes have been proposed and discussed [11,14,15,18,22,23,25–28,45,47,48,51,59].

However, all of the proxy signature schemes proposed so far allow any outsider to play the role of a verifier. Only one verifier can verify the validity of the proxy signature [5,33,44,55,57]. In fact, in real-life applications, a signature usually has to go through some specified verifiers. For example, suppose two network companies have a contract between them

☆ This work was supported in part by National Science Council under the Grant NSC 101-2221-E-030-018.
* Corresponding author at: Department of Library and Information Science, Fu Jen Catholic University, 510 Jhongjheng Road, Sinjhuang City, Taipei County 24205, Taiwan, ROC.
E-mail addresses: mshwang@asia.edu.tw (M.-S. Hwang), cclee@mail.fju.edu.tw (C.-C. Lee).

0020-0255/$ - see front matter
http://dx.doi.org/10.1016/j.ins.2012.11.004

to sign for commercial collaboration. The contract needs to be signed and verified between the two companies. Assume several directors, called original signers, represent a directorate to delegate their signing capability to some of the designated managers, called proxy signers. Then, several of the designated managers can represent their company to sign this contract with the representative(s) of the other company through a computer network. However, it should never be necessary to check the legitimacy of the signature on occasions when fewer than t_3 of the specified verifiers are present. Only a specified group of verifiers can verify the validity of the contract.

According to the above statement, Tzeng et al. [51] proposed a novel variation of proxy signature scheme called threshold multi-proxy multi-signature scheme with shared verification. Its scheme is based on discrete logarithms problems [10,19]. In this article, we shall propose a new proxy signature scheme based on RSA problem [6,21,41]. To be specific, the authorized message can be delegated, signed and verified by predefined threshold values and under the predefined proxy warrant, respectively.

In the next section, we shall briefly review some related works. In Section 3, we shall propose our new proxy signature scheme with shared verification ($(t_1, n_1), (t_2, n_2), (t_3, n_3)$ proxy signature). In Section 4, the security analysis and performance evaluation of the proposed scheme will be discussed. Finally, the conclusion will be given in the last section.

2. Related works

So far, five types of proxy delegation have been developed. In 1996, Mambo et al. [35,36] proposed three types of delegation: the full delegation, the partial delegation and the delegation with warrant. Each of them has its own level of delegation and security assumption. After that, Kim et al. [28] presented two types of delegation: the partial delegation with warrant and threshold delegation. Partial delegation and delegation by warrant are the most secure, and full delegation is the least secure. The advantage of partial delegation is its fast processing speed. In addition, delegation by warrant is appropriate for the restricted period to be signing. Moreover, the warrant can also be used to prevent a proxy signer from transferring a proxy delegation to another person who is not the designated proxy signer. Partial delegation with warrant combines the benefits of partial delegation and delegation by warrant. Therefore, among these types of delegation, partial delegation with warrant seems to be the best choice. In this article, we shall focus on the proxy signature authorized by using partial delegation with warrant.

In general, a secure proxy signature scheme should satisfy the following security requirements:

- *Strong unforgeability*: A designated proxy signer can generate a valid proxy signature on behalf of the original signer, but the original signer or any third party who is not the designated proxy signer cannot generate a valid proxy signature.
- *Verifiability*: By checking the proxy signature, the verifier can make sure of the original signer's guarantee on the signed message.
- *Proxy signer's deviation*: A proxy signer cannot generate a valid proxy signature not detected as her/his signature. Furthermore, she/he cannot generate a valid signature of the original signer, either.
- *Distinguishability*: Valid proxy signatures are distinguishable from valid self-signing signatures for anyone in polynomial time or size computation. Here, a self-signing signature means a signature generated by the original signer.
- *Strong identifiability*: The original signer and any third party can determine the identity of the actual proxy signer by checking the proxy signature.
- *Secret-keys' dependence*: A new proxy signature key is computed from the private key of an original signer. Furthermore, the original signer cannot calculate another one.
- *Strong undeniability*: Once a proxy signer generated a valid signature on behalf of the original signer, she/he cannot repudiate signature creation against the original signer.

So far, many threshold proxy signature schemes have been widely studied [15,22,24,28,48]. In a (t, n) threshold proxy signature scheme, which is a variant of the proxy signature scheme, the proxy signature key is shared among a group of n proxy signers delegated by the original signer. Any t or more proxy signers can cooperatively sign messages on behalf of the original signer.

Based on Kim's scheme [28], Sun [48] proposed an efficient non-repudiable threshold proxy signature scheme with known signers. Sun's scheme is more efficient than the other threshold proxy signature schemes. The main advantage of Sun's scheme is that the verifier is able to identify the actual signers in the proxy group. However, the weakness of Sun's scheme is that it is vulnerable to the conspiracy attack [15,22]. Hsu et al. [15] proposed a new non-repudiable proxy signature scheme with known signers that can withstand the conspiracy attack and is more efficient than Sun's scheme. Technically, the security of the above two non-repudiable threshold proxy signature schemes is based on the discrete logarithm problem [10].

In 2000, Wang et al. [53] proposed a new (t, n) threshold signature scheme with (k, l) threshold-shared verification. According to the security level of a document, not only the document can be signed by some specified signers in a group, but it can also be verified by some specified verifiers in another group. Later, quite some literatures were released [17,50]. Lee et al. [30] proposed an untraceable (t, n) threshold signature scheme based on the Ohta–Okamoto signature scheme [39]. For the sake of privacy and safety, the identity of the signers should be anonymous in a democratic society.