Available online at www.sciencedirect.com
SCIENCE DIRECT®
Computers and Electrical Engineering 31 (2005) 69–80
Computers and Electrical Engineering
www.elsevier.com/locate/compeleceng

New threshold-proxy threshold-signature schemes

Hwang Shin-Jia [a,*], Chen Chiu-Chin [b]

[a] Department of Computer Science and Information Engineering, TamKang University, Tamsui, Taipei Hsien 251, Taiwan, ROC
[b] Department of Information Management, Chaoyang University of Technology, Wufeng, Taichung Country 413, Taiwan, ROC

Received 3 June 2002; received in revised form 19 June 2004; accepted 3 November 2004
Available online 17 March 2005

Abstract

A new (t,n) threshold-proxy (c,m) threshold-signature scheme is proposed in this paper. In this scheme, only any t or more original signers of n original signers can authorize a proxy group of m proxy signers and then only c or more proxy signers can cooperatively generate threshold-proxy threshold-signatures. Our scheme provides the fair protection for the original and proxy groups. So original signers cannot forge the proxy signatures while the proxy signers cannot forge signatures on behalf of the original signers. Moreover, our scheme satisfies the seven conditions proposed by Mambo et al. Further, in our scheme, the verifier has to verify the correctness of the threshold proxy certificate before checking the correctness of the threshold-proxy threshold-signatures. To meet the practical situations, the proxy agreement is reached not only the original group but also the proxy group. To realize this new kind of agreement, the scheme provides two options for the generation of threshold-proxy certificates: threshold and total agreements. The total agreement option provides the flexible for the proxy group that the members cannot trust with each other. The best way to agree on the proxy authorization is the common view reached by all members.

Keywords: Proxy signatures; Threshold proxy signatures; Multi-proxy multi-signatures; Threshold-proxy threshold-signatures

* Corresponding author. Tel.: +886 2 26215656x2727; fax: +886 2 26209749.
E-mail addresses: sjhwang@mail.tku.edu.tw (S.-J. Hwang), s8914604@mail.cyut.edu.tw (C.-C. Chen).

0045-7906/$ - see front matter © 2005 Elsevier Ltd. All rights reserved.
doi:10.1016/j.compeleceng.2004.11.003

1. Introduction

In 1996, Mambo et al. fist proposed the proxy signature scheme [14,15]. In this scheme, there are two participators, one is the original signer, and the other is proxy signer. In the proxy signature scheme, the original signer is able to authorize the proxy signer as his proxy agent. For proxy signature schemes, Mambo et al. also gave seven important conditions [14,15]. There are unforgeability, verificability, proxy signer's deviation, distinguishability, identifiability, secret-key's dependence and undeniability conditions. Since then many different kinds of proxy schemes are proposed [3–12,17–24,26,27].

For group-oriented applications, Sun proposed an efficient nonrepudiable threshold proxy signature scheme with known signers [18] in 1999. In his (t,n) threshold proxy signature scheme, the proxy secret key generated by one original signer is shared out among all of n proxy singers in the proxy signer group. Any t or more proxy signers can cooperatively recover the proxy secret key to generate the proxy signature, but any $t-1$ or less proxy signers cannot. Sun's scheme also provides the nonrepudiable function to identify the signers who actually generated proxy signatures. However, in 2000, Hwang et al. shows Sun's scheme is insecure by collusion attack and also proposed their improvement [4]. Unfortunately, Hwang and Chen [10] pointed out both Sun's scheme and Hwang et al.'s schemes are insecure by their attacks. Recently, Hsu et al.'s proposed another nonrepudiable threshold proxy signature scheme with known signers [3]. Their scheme is more efficient than Sun's scheme. Moreover, their scheme can defense against the collusion attack [4].

However, these proxy schemes only consider the group-oriented case that the proxy agent is a group. Moreover, in some group-oriented applications, a group consisting of n original signers wants to authorize a proxy group consisting of m proxy signers. In our real life, there are many applications of (t,n) threshold-proxy (c,m) threshold-signature schemes. For example, the board of n directors of a company wants to depute a lawyer group. Only the agreement of any t or more directors can depute a lawyer group as their agents. Only the agreement reached by any c or more lawyers represents the agreement of the lawyer group. For example, the board of n directors may needs the help of m independent certified accountants to check and sign the financial statement of their company on behalf of them. This proxy authorization should be agreed with any t directors and all certified accountants since certified accountants are independent. Then the proxy signature is still generated by any c or more accountants. To respect the law/finance professional is why the board of directors has to authorize a lawyer/accountant proxy group.

In this paper, threshold-proxy threshold-signature schemes will be proposed. In a (t,n) threshold-proxy (c,m) threshold-signature scheme, only any t or more original signers of the n original signers can authorize the proxy signer group consist of m proxy signers. Only any c or more proxy signers can generate the proxy signature on behalf of the original signer group.

For the proxy authorization, it is better that this authorization should be also is agreed by the proxy group. In other word, not only the t original signers but also some proxy signers cooperatively generate the threshold proxy certificate. On the number of proxy signers, two cases are considered in our scheme. In the first case, the number of proxy signers is the threshold value c. So the proxy certificate is reached with threshold agreement of the proxy group. In another case, all proxy signers join the work to generate the proxy certificate. So the proxy certificate is reached with totally agreement of the proxy group. Consider the following condition to show why the totally agreement is necessary. Suppose that the signer group temporally consists of