Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER Applied Mathematics and Computation 166 (2005) 58–63
APPLIED MATHEMATICS AND COMPUTATION
www.elsevier.com/locate/amc

Security of a multisignature scheme for specified group of verifiers

Jiqiang Lv [a,*], Xinmei Wang [a], Kwangjo Kim [b]

[a] National Key Lab of ISN, Xidian University, Xi'an City, Shaanxi Province, 710071, China
[b] International Research Center for Information Security, Information and Communications University, 58-4 Hwaam-dong, Yusong-ku, Taejon, Daejeon 305732, South Korea

Received 24 February 2004; accepted 29 April 2004

Abstract

A multisignature scheme for specified group of verifiers needs a group of signers' cooperation to sign a message to a specified group of verifiers that must cooperate to check the signature's validity later. Recently, Zhang et al. proposed a new multisignature scheme for specified group of verifiers. However, we find that Zhang et al.'s scheme cannot prevent a dishonest clerk of signing group from changing the signing message to another message of his choice while he is cooperating with the signers to produce a multisignature. Therefore, their scheme is insecure.

Keywords: Public key cryptography; Digital signature; Multisignature scheme

1. Introduction

A digital signature provides the functions of integration, authentication and nonrepudiation for a signing message. Under some ordinary situations, one

* Corresponding author.
E-mail address: lvjiqiang@hotmail.com (J. Lv).

0096-3003/$ - see front matter
doi:10.1016/j.amc.2004.04.108

signer is sufficient to generate a signature on some message. But under other situations, it may need a group of signers' participation to produce a signature on a message. Due to the existence of the above situations, Itakura and Nakamura [1] proposed a new concept of digital signature scheme, called multisignature scheme, during which a group of signers must cooperate to produce a signature on a message and any verifier can check the multisignature's validity by using the signing group's public key. Later, Laih and Yen [2] proposed a new type of multisignature scheme that is used for a specified group of verifiers. It is different from a multisignature scheme in that only under the group of verifiers' cooperation could a multisignature be verified. Unfortunately, He [3] pointed out that Laih et al.'s scheme has the weakness that the clerk of verifying group can verify a multisignature by himself if he once receives a signature from the same signing group. Recently, Zhang et al. [4] proposed a new multisignature scheme for specified group of verifiers, and claimed that forging signatures in the proposed scheme is equivalent to forging Harn's signatures [5].

In this paper, we show that Zhang et al.'s scheme has the following weakness: a dishonest clerk of signing group can change the signing message to an arbitrary one while he is cooperating with the signers to produce a multisignature.

In Section 2, we briefly review Zhang et al.'s multisignature scheme for specified group of verifiers. In Section 3, we show the weakness in Zhang et al.'s scheme. Concluding remarks are made in Section 4.

2. Review of Zhang et al.'s multisignature scheme for specified group of verifiers [4]

Zhang et al.'s multisignature scheme consists of three phases: key generation, multisignature generation, and multisignature verification.

2.1. Key generation phase

Let $G_S = \{U_{S1}, U_{S2}, \ldots, U_{Sn}\}$ be the group of n signers and $G_V = \{U_{V1}, U_{V2}, \ldots, U_{Vm}\}$ be the group of m verifiers. In each group, there is a specified user, called clerk. The clerk U_{Sc} of the signer's group is responsible for verifying all partial signatures signed by signers in G_S and combining them into a multisignature. The clerk U_{Vc} of the verifier's group is responsible for assisting all verifiers in G_V to verify the multisignature. The trusted center selects two large primes p and q such that $q|p-1$, a generator g with order q in Z_p and a public one-way hash function $H(\cdot)$. Each $U_{Si} \in G_S$ selects his private key $s_i \in Z_q$ and computes his public key $Y_{Si} = g^{s_i} \bmod p$. Each $U_{Vi} \in G_V$ selects his private key $v_i \in Z_q$ and computes his public key $Y_{Vi} = g^{v_i} \bmod p$. Then G_S and G_V