Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER Applied Mathematics and Computation 170 (2005) 1284–1289
APPLIED MATHEMATICS AND COMPUTATION
www.elsevier.com/locate/amc

Comments on ID-based multi-signature with distinguished signing authorities

Hung-Yu Chien

Department of Information Management, Chaoyang University of Technology, Wufeng, Taichung 413, Taiwan, ROC

Abstract

A multi-signature scheme with distinguished signing authorities is a multi-signature scheme where the signed document is divided into several parts and each signer signs only on the part which he is responsible for. This article shows the security weakness of Wu–Hsu's ID-based multi-signature scheme with distinguished signing authorities.

Keywords: Cryptography; Multi-signature; Forgery attack

1. Introduction

A multi-signature scheme allows a group of members to jointly sign a document such that a verifier can verify that all the members have signed on the document [1]. This type of multi-signature scheme is called a multi-signature scheme with undistinguished signing authorities, since all the members sign on the same document. In 1999, Harn [2] first proposed the multi-signature with distinguished signing authorities, where each signer signs a partial

E-mail address: redfish6@ms45.hinet.net

0096-3003/$ - see front matter
doi:10.1016/j.amc.2005.01.019

document that he is responsible for. Later, Li et al. [3] found the security weaknesses of Harn's scheme.

In 2002, Wu and Hsu [4] proposed two ID-based multi-signature schemes with distinguished signing authorities for sequential and broadcasting architectures. In an ID-based cryptosystem [5], each signer's identity is his/her public key and there is no extra public key certificate. The signers sign the documents based on a pre-defined sequential order in the sequential architecture; while, in the broadcasting architecture, the signers can independently sign the document. However, we find that both of Wu–Hsu's schemes are vulnerable to some insider forgery attacks. One is that an insider of a group can easily forge signatures on behalf of other members. The other is that an insider can easily replace a partial document/signature m_i/s_i with another partial document/signature m_i'/s_i' without being noticed. Since Wu–Hsu's two schemes are similar and our attacks applies on both of Wu–Hsu's sequential and broadcasting architecture, we only review and demonstrate the attack on the broadcasting version.

2. Review of Wu–Hsu's ID-based multi-signature scheme with distinguished signing authorities

In this section, we review the broadcasting version of Wu–Hsu's ID-based multi-signature scheme. Wu–Hsu's scheme is based the modified Maurer–Yacobi's scheme [6]. The scheme consists of three phases—the initialization phase, the multi-signature generation phase and the multi-signature verification phase. In the multi-signature generation phase, the issuer broadcasts the message to all the signers, the signers sign the partial document that he is responsible for, and the collector collects and combines the multi-signature. Let $U_1, U_2, \ldots, U_n$ be the participant signers, and U_I be the document issuer.

2.1. The initialization phase

The system performs the following set-up steps:

1. Choose two primes p and q of about 100 digits such that $p = \pm 1 \bmod 8$ and $q = \pm 3 \bmod 8$, and $(p-1)/2$ and $(q-1)/2$ are relatively prime. Compute $n = p \cdot q$ and select a public element g that is a primitive element in both Z_p^* and Z_q^*. Note that the Jacobi symbol $(2/n) = -1$ in this setting. Please notice that it is feasible to compute discrete logarithms modulo each prime but infeasible to factoring the product [6].
2. Choose e and d in Z_λ^* such that $e \cdot d = 1 \bmod \lambda$, where $\lambda = \mathrm{lcm}(p-1, q-1)$. The system publishes e as the system's public key and d as the private key. Note that the length of e should be chosen between 20 and 70 bits [6].