Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER Applied Mathematics and Computation 170 (2005) 1166–1169
APPLIED MATHEMATICS AND COMPUTATION
www.elsevier.com/locate/amc

Attack on Han et al.'s ID-based confirmer (undeniable) signature at ACM-EC'03

Fangguo Zhang [a,*], Reihaneh Safavi-Naini [b], Willy Susilo [b]

[a] *Department of Electronics and Communication Engineering, School of Information Science and Technology, Sun Yat-Sen University, Guangzhou 510275, P.R. China*
[b] *School of Information Technology and Computer Science, University of Wollongong, NSW 2522, Australia*

Abstract

In ACM conference on electronic commerce (EC'03), Han et al. [Identity-based confirmer signatures from pairings over elliptic curves, in: Proceedings of ACM Conference on Electronic Commerce Citation 2003, San Diego, CA, USA, June 09–12, 2003, pp. 262–263] proposed an ID-based confirmer signature scheme using pairings (the scheme is in fact an ID-based undeniable signature scheme). In this paper, we show that this signature scheme is not secure and the signer can deny any signature, even if it is a valid signature, and any one can forge a valid confirmer signature of a signer with identity ID on an arbitrary message and confirm this signature to the verifier.

Keywords: Confirmer signature; Undeniable signature; Attack; Bilinear pairings; ID-based cryptography

* Corresponding author.
E-mail addresses: isdzhfg@zsu.edu.cn (F. Zhang), rei@uow.edu.au (R. Safavi-Naini), wsusilo@uow.edu.au (W. Susilo).

0096-3003/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.amc.2005.01.015

1. Introduction

Undeniable signatures, introduced by Chaum and van Antwerpen [1], are digital signatures that can only be verified by interacting with the signer. Confirmer signatures [2] are undeniable signatures where signatures may also be verified by interacting with an entity called the confirmer who has been designated by the signer. At the fourth ACM conference on electronic commerce (EC'03), Han et al. proposed an ID-based confirmer signature scheme using pairings and showed the soundness of the scheme [3]. In this paper, we will show that this scheme is not secure and propose two attacks. In the first attack the signer can subvert the verification operation to prove a valid signature to be invalid, and in the second attack, anyone can forge a signature for an arbitrary message and prove that it is a valid signature.

2. Han et al.'s ID-based confirmer signature scheme

First, we review Han et al.'s ID-based confirmer signature scheme from pairings in brief using the same notation as [3].

The system parameters are $\{\mathbb{G}_1, \mathbb{G}_2, e, q, P, H_0, H\}$, here $\mathbb{G}_1$ is a cyclic additive group generated by P, whose order is a prime q, and $\mathbb{G}_2$ is a cyclic multiplicative group with the same order q. e: $\mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_2$ is a bilinear pairing. H, H_0 are two cryptographic hash functions, H:$\{0,1\}^* \to Z_q$ and H_0 : $\{0,1\}^* \to \mathbb{G}_1$. Let A be a large number about 10^{20} and $[A] = \{1, 2, \ldots, A\}$ known to verifiers and signers.

- *Setup:* The Key Generation Center (KGC) chooses a random number $s \in Z_q^*$ and sets $P_{\text{pub}} = sP$, and keeps s as the *master-key*, which is known only by itself.
- *Extraction:* A signer submits his identity information $\text{ID} \in \{0,1\}^*$ to KGC. KGC computes the signer's public key as $Q_{\text{ID}} = H_0(\text{ID})$, and returns $D_{\text{ID}} = sQ_{\text{ID}}$ and $L_{\text{ID}} = s^{-1}Q_{\text{ID}}$ to the signer as his private keys.
- *Sign:* To sign a message $m \in \{0,1\}^*$, the signer first picks $k \in Z_q^*$ randomly, sets $r = kP$ and computes $S = k^{-1}D_{\text{ID}} + H(m)L_{\text{ID}}$. Then the signature on m is $\{r, S\}$.
- *Confirmation:* To confirm a signature $\{r, S\}$ for a message m,
  - Verifier chooses $x \in [A], y \in Z_q^*$ uniformly and randomly, sets $C_1 = xyr, C_2 = xyP$ and sends them to the signer.
  - The signer computes $X = e(r + P_{\text{pub}}, P - L_{\text{ID}})$ and $R = e(C_1, L_{\text{ID}})$, and sends them to the verifier.
  - The verifier checks whether

$$e(r, S)^x = e(P_{\text{pub}}, Q_{\text{ID}})^x R^{H(m)y^{-1}},$$