Computers and Electrical Engineering 35 (2009) 49–53

Contents lists available at ScienceDirect

Computers and Electrical Engineering

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

Identity-based strong designated verifier signature schemes: Attacks and new construction

Baoyuan Kang [a,b,*], Colin Boyd [b], Ed Dawson [b]

[a] School of Mathematical Sciences and Computing Technology, Central South University, Chang'sha, Hunan 410075, PR China
[b] Information Security Institute, Queensland University of Technology, GPO Box 2434, Brisbane, QLD 4001, Australia

ARTICLE INFO

Article history:
Received 7 December 2007
Accepted 29 May 2008
Available online 15 July 2008

Keywords:
Identity base cryptography
Designated verifier signature
Identity-based signature
Proxy signature
Bilinear parirings

ABSTRACT

A strong designated verifier signature scheme makes it possible for a signer to convince a designated verifier that she has signed a message in such a way that the designated verifier cannot transfer the signature to a third party, and no third party can even verify the validity of a designated verifier signature. We show that anyone who intercepts one signature can verify subsequent signatures in Zhang-Mao ID-based designated verifier signature scheme and Lal-Verma ID-based designated verifier proxy signature scheme. We propose a new and efficient ID-based designated verifier signature scheme that is strong and unforgeable. As a direct corollary, we also get a new efficient ID-based designated verifier proxy signature scheme.

1. Introduction

In an ordinary digital signature scheme, anyone can verify the validity of a signature using the signer's public key. However, in some scenarios, this public verification is not desired, if the signer does not want the recipient of a digital signature to show this signature to a third party at will. To address this problem above, Chaum and Van Antwerpen [1] introduced undeniable signature which allowed a signer to have complete control over his signature. In an undeniable signature scheme, the verification of a signature requires the participation of the signer, in order to avoid undesirable verifiers getting convinced of the validity of the signature. Motivated by the above problem, Jakobsson et al. [3] proposed the concept of designated verifier signature (DVS) schemes. A DVS scheme is special type of digital signature which provides message authentication without non-repudiation. These signatures have several applications such as in E-voting, call for tenders and software licensing. Suppose Alice has sent a DVS to Bob. Unlike the conventional digital signatures, Bob cannot prove to a third party that Alice has created the signature. This is accomplished by the Bob's capability of creating another signature designated to himself which is indistinguishable from Alice's signature.

In [3], Jakobsson et al. also introduced a stronger version of DVS. In this stronger scheme, no third party can even verify the validity of a designated verifier signature, since the designated verifier's private key is required in the verifying phase. After Saeednia et al. [5] formalized the notion of strong DVS in 2003, many strong designated verifier signature schemes have been proposed [2,4,6–8]. Recently, Zhang and Mao [7] proposed a novel ID-based strong designated verifier signature scheme (Zhang-Mao scheme) based on bilinear pairings by combining ID-based cryptosystem with the designated verifier signature. They also provided the security proofs of their scheme. In Zhang-Mao scheme, they claimed that their scheme was a strong designated verifier signature, in which no third party can verify the validity of a designated verifier signature.

* Corresponding author. Address: School of Mathematical Sciences and Computing Technology, Central South University, Chang'sha, Hunan 410075, China. Tel.: +86 7312655523.
E-mail addresses: baoyuankang@yahoo.com.cn (B. Kang), c.boyd@qut.edu.au (C. Boyd), e.dawson@qut.edu.au (E. Dawson).

0045-7906/$ - see front matter © 2008 Elsevier Ltd. All rights reserved.
doi:10.1016/j.compeleceng.2008.05.004

However, in this paper, we point out Zhang-Mao scheme can not satisfy this strong property, that is, anyone who intercepts one signature can get some information and verify subsequent signatures. Like Zhang-Mao scheme, there is same flaw in the ID-based designated verifier proxy signature scheme [8] proposed by Sunder Lal and Vandani Verma (Lal-Verma scheme). By pointing out the undesirable flaws in these designated verifier signature schemes, we also propose new and efficient ID-based designated verifier signature and proxy signature schemes.

The paper is organized as follows. In the next Section, we describe background concepts of bilinear pairings and related mathematical problems. We briefly review Zhang-Mao scheme and Lal-Verma scheme in Section 3. In Section 4, we show the weakness in their schemes. In Section 5, we propose new and efficient designated verifier signature and proxy signature schemes. Finally, Section 6 concludes the paper.

2. Background concepts

In this section, we briefly review the basic concepts of bilinear pairings and some related mathematical problems.

- *Bilinear pairings* Let G_1 be an additive cyclic group with prime order q, G_2 be a multiplicative cyclic group of same order and P be a generator of G_1. Let $e : G_1 \times G_1 \to G_2$ be a bilinear mapping with the following properties:
  1. *Bilinearity*: $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in G_1, a, b \in Z_q^*$.
  2. *Non-degeneracy*: There exists $P \in G_1$, $Q \in G_1$ such that $e(P, Q) \neq 1$.
  3. *Computability*: There exists an efficient algorithm to compute $e(P, Q)$ for all $P, Q \in G_1$.

  A bilinear Diffie-Hellman (BDH) parameter generator is defined as a probabilistic polynomial time algorithm that takes as input a security parameter k and returns a uniformly random tuple (q, G_1, G_2, e, P) of bilinear parameters, including a prime number q of size k, a cyclic additive group G_1 of order q, a multiplicative group G_2 of order q, a bilinear map $e : G_1 \times G_1 \to G_2$ and a generator P of G_1.
- *Discrete logarithm problem (DLP):* Given two elements $P, Q \in G_1$, find an integer $a \in Z_q^*$, such that $Q = aP$ whenever such an integer exists.
- *Computational Diffie-Hellman problem (CDHP):* For any $a, b \in Z_q^*$, given P, aP, bP, compute abP.
- *Decisional Diffie-Hellman problem (DDHP):* For any $a, b, c \in Z_q^*$, given P, aP, bP, cP, decide whether $c = ab \bmod q$.
- *Bilinear Diffie-Hellman Problem (BDHP):* Given randomly chosen $P \in G_1$, as well as aP, bP and cP (for unknown randomly chosen $a, b, c \in Z_q$), compute $e(P, P)^{abc}$.
- *Gap Diffie-Hellman Problem (GDHP):* A class of problems, where DDHP can be solved in polynomial time but no probabilistic polynomial time algorithm exists which can solve CDHP.
- *Bilinear Diffie-Hellman (BDH) Assumption:* If $\mathcal{G}$ is a BDH parameter generator, the advantage $Adv_{\mathcal{G}}(\mathcal{A})$ that an algorithm $\mathcal{A}$ has in solving the BDH problem is defined to be the probability that the algorithm $\mathcal{A}$ outputs $e(P, P)^{abc}$ on inputs $G_1, G_2, e, P, aP, bP, cP$, where G_1, G_2, e is the output of $\mathcal{G}$ for sufficiently large security parameter k, P is a random generator of G_1 and a, b, c are random elements of Z_q. The BDH assumption is that $Adv_{\mathcal{G}}(\mathcal{A})$ is negligible for all efficient algorithms $\mathcal{A}$.

3. Review of two ID-based designated verifier signature schemes

3.1. Zhang-Mao scheme

Zhang-Mao's designated verifier signature scheme consists of the following five phases:

1. *Setup*: In this phase, the PKG (private key generation center) chooses a gap Diffie-Hellman group G_1 of prime order q and a multiplicative group G_2 of the same order and a bilinear map $e : G_1 \times G_1 \to G_2$, together with an arbitrary generator $P \in G_1$. Then it chooses a random value $s \in Z_q^*$ as the master secret key and computes the corresponding public key $P_{\text{pub}} = sP$. $H_1(\cdot)$ and $H_2(\cdot)$ are two cryptographic hash functions, with $H_1 : \{0,1\}^* \to G_1$ and $H_2 : \{0,1\}^* \times G_1 \times G_1 \to G_1$. The system parameters are $(G_1, G_2, P, P_{pub}, H_1, H_2, e, q)$ and the master secret key is s.
2. *KeyExtract*: Given an identity ID, PKG computes $S_{\text{ID}} = sH_1(\text{ID})$ and sends it to the user with identity ID. We remark $Q_{\text{ID}} = H_1(\text{ID})$ as the public key of the user with identity ID.
3. *Sign*: Given a secret key S_{ID_A} of the signer Alice, the public key Q_{ID_A}, Q_{ID_B} of the signer Alice and designated verifier Bob, respectively and the signed message M, the signer randomly chooses two numbers $r_1, r_2 \in Z_q^*$ and computes as follows:

$$U_1 = r_1 Q_{\text{ID}_B}$$
$$U_2 = r_1 r_2 Q_{\text{ID}_B}$$
$$H = H_2(M, U_1, U_2)$$
$$V = r_2 H + r_1^{-1} S_{\text{ID}_A}$$