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:

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

Finally, the resulting signature is (U_1, U_2, V) to the designated verifier Bob.

4. *Verify*: Given a designated verifier signature (U_1, U_2, V), the designated verifier first computes $H = H_2(M, U_1, U_2)$, and accepts this signature if and only if the following equation holds:

$$e(U_1, V) = e(U_2, H)e(S_{\mathrm{ID_B}}, Q_{\mathrm{ID_A}})$$

5. *Transcript simulation: To simulate the transcript, the designated verifier Bob randomly chooses two numbers $r'_1, r'_2 \in Z_q^*$ and computes*

$$U'_1 = r'_1 Q_{\mathrm{ID_A}}$$
$$U'_2 = r'_1 r'_2 Q_{\mathrm{ID_A}}$$
$$H' = H_2(M, U'_1, U'_2)$$
$$V' = r'_2 H' + r'^{-1}_1 S_{\mathrm{ID_B}}$$

the signature (U'_1, U'_2, V') on the message M also satisfies the verifying equation in the Verify phase.

3.2. Lal-Verma scheme

Lai-Verma's designated verifier proxy signature scheme has five phases: Setup phase, Key generation phase, Proxy key generation phase, proxy signature generation phase, Proxy signature verification, and Setup phase and Key generation are as same as that of Zhang-Mao scheme except $H_2 : \{0,1\}^* \times G_2 \to G_1$ in Lal-Verma scheme. So, we only list the following three phases:

- *Proxy key generation:* The original signer Alice computes the signature on message M as follow: Alice chooses three random numbers $r_1, r_2, r_3 \in Z_q^*$ and a warrant W and computes $U_1 = r_1 Q_{\mathrm{IDB}}$, $U_2 = r_2 Q_{\mathrm{IDA}}$, $U_3 = r_3 U_1$ and $V = r_3 H + r_1^{-1} S_{\mathrm{IDA}}$, here $H = H_2(M, W, e(r_2 Q_{\mathrm{IDB}}, S_{\mathrm{IDA}})$. Alice sends $\sigma = (M, W, U_1, U_2, U_3, V)$ to the proxy signer Bob. On receiving σ Bob computes $H = H_2(M, W, e(U_2, S_{\mathrm{IDB}})$. Bob accepts the signature if only if $e(U_1, V) = e(U_3, H)e(S_{\mathrm{IDB}}, Q_{\mathrm{IDA}})$. Then, Bob computes the proxy secret key $S_{\mathrm{IDP}} = V + S_{\mathrm{IDB}}$.
- *Proxy signature generation:* To generate the proxy signature on message M, the proxy signer Bob chooses three random numbers $t_1, t_2, t_3 \in Z_q^*$ and computes $X_1 = t_1 Q_{\mathrm{IDC}}$, $X_2 = t_2 S_{\mathrm{IDP}}$, $X_3 = t_3 X_1$ and $X = t_3 H^1 + t_1^{-1} S_{\mathrm{IDP}}$. Here $H^1 = H_2(M, W, e(t_2 Q_{\mathrm{IDC}}, S_{\mathrm{IDP}})$, and Q_{IDC} is the public key of the designated verifier Cindy. Bob sends $(M, W, X_1, X_2, X_3, X, V)$ to Cindy.
- *Proxy signature verification:* On receiving $(M, W, X_1, X_2, X_3, X, V)$ the designated verifier Cindy performs as follows:
  1. Checks whether the message M confirms to the warrant W. if not, stops. Otherwise, continues.
  2. Checks whether Alice and Bob are specified as the original signer and the proxy signer in the warrant W, respectively.
  3. If all validation passes, Cindy computes $H^1 = H_2(M, W, e(X_2, Q_{\mathrm{IDC}}))$. Cindy accepts the signature if only if

$$e(X_1, X) = e(X_3, H^1)e(S_{\mathrm{IDC}}, Q_{\mathrm{IDB}})e(Q_{\mathrm{IDC}}, V).$$

Here S_{IDC} is the secret key of the designated verifier Cindy.

4. Attacks on the two schemes

In Zhang-Mao scheme, they claimed their scheme is a strong designated verifier signature, and no third party can even verify the validity of a designated verifier signature, since the designated verifier's private key is required in the verification equation. However, we find Zhang-Mao scheme can not satisfy this property.

In fact, assume (U_1, U_2, V) is the signature of message M. Anyone who intercepts (U_1, U_2, V) can compute $e(S_{\mathrm{ID_B}}, Q_{\mathrm{ID_A}})$ according to the verification equation

$$e(U_1, V) = e(U_2, H)e(S_{\mathrm{ID_B}}, Q_{\mathrm{ID_A}}).$$

He first computes $H = H_2(M, U_1, U_2)$, then he can easily get $e(S_{\mathrm{ID_B}}, Q_{\mathrm{ID_A}})$ from the following equation

$$e(S_{\mathrm{ID_B}}, Q_{\mathrm{ID_A}}) = \frac{e(U_1, V)}{e(U_2, H)}$$

After that, when the attacker intercepts new signature (U_1^*, U_2^*, V^*) of message M^*, now he first computes $H^* = H_2(M^*, U_1^*, U_2^*)$, and then check the validity of signature (U_1^*, U_2^*, V^*) by following equation

$$e(U_1^*, V^*) = e(U_2^*, H^*)e(S_{\mathrm{ID_B}}, Q_{\mathrm{ID_A}})$$

Since he has got $e(S_{\mathrm{ID_B}}, Q_{\mathrm{ID_A}})$ before. So, it is easy for the attacker to verify the validity of the designated verifier signature without the private key of the designated verifier.

Similar attack is effective to Lai-Verma designated verifier proxy signature scheme. Because it is easy to get $e(S_{IDC}, Q_{IDB})$ from the following equation:

$$e(S_{IDC}, Q_{IDB}) = \frac{e(X_1, X)}{e(X_3, H^1)e(Q_{IDC}, V)}$$

when someone intercepts the proxy signature $(M, W, X_1, X_2, X_3, X, V)$. Then, anyone who get $e(S_{IDC}, Q_{IDB})$ can easily verify the validity of subsequent proxy signature$(M^*, W^*, X_1^*, X_2^*, X_3^*, X^*, V^*)$ by following equation

$$e(X_1^*, X^*) = e(X_3^*, H^{1*})e(S_{IDC}, Q_{IDB})e(Q_{IDC}, V^*)$$

without the designated verifier's private key is required. This violate the main property of designated verifier.

5. New ID-based designated verifier signature and proxy signature schemes

In this section, we propose a new and efficient ID-based designated verifier signature, and as a direct corollary we get a new ID-based designated verifier proxy signature.

5.1. ID-based designated verifier signature scheme

Our ID-based designated verifier signature scheme has five phases: Setup phase, Key generation phase, Signature generation phase, Signature verification phase, Signature simulation phase. The Setup phase and Key generation are as same as that of Zhang-Mao scheme except $H_2 : \{0,1\}^* \times G_2 \to G_1$ in our scheme. So, we only describe the last three phases.

- *Signature generation:* To generate signature on the message M which can be verified by the user Cindy, the signer Alice chooses one random number $r \in Z_q^*$ and computes

  $$U = rQ_{IDA}$$
  $$\sigma = H_2(M, e(rQ_{IDC}, S_{IDA})$$

  Alice sends (σ, U) to the designated verifier Cindy.
- *Signature verification:* On receiving (σ, U) the designated verifier Cindy accepts the signature if and only if

  $$\sigma = H_2(M, e(U, S_{IDC}))$$

- *Signature simulation:* Cindy chooses one random number $r' \in Z_q^*$ and computes

  $$U' = r'Q_{IDA}$$
  $$\sigma = H_2(M, e(U', S_{IDC}))$$

  Obviously, (σ, U') satisfies the verification.

5.1.1. Security analysis

Now we analyze the security of the proposed designated verifier signature scheme.

Correctness The following equations gives the correctness of the verification:

$$\sigma = H_2(M, e(rQ_{IDC}, S_{IDA})) = H_2(M, e(rQ_{IDC}, sQ_{IDA})) = H_2(M, e(sQ_{IDC}, rQ_{IDA})) = H_2(M, e(S_{IDC}, U))$$

Strongness: The designated verifier has to use his secret key S_{IDC} during the verification. Moreover, unlike Zhang-Mao scheme and Lal-Verma scheme, nobody can get any useful information to signature verification from intercepted signatures. Thus, our scheme is a strong designated verifier scheme.

Unforgeability: It is not possible to construct the term σ without the knowledge of either the signer secret key S_{IDA} or the verifier secret key S_{IDC}. Thus, the signature is unforgeable.

Like Kumar et al.'s scheme [4], Our scheme also have properties of non-transferability privacy, source hiding and non-delegatability. People interesting to these properties may refer to paper [4].

5.1.2. Efficiency analysis

Among the existed ID-based designated verifier signature schemes, Kumar et al.'s scheme (K-scheme) [4] and Susilo et al.'s scheme (S-scheme) [6] are more secure and efficient. Now we give a performance comparison of our scheme with these two schemes, based on the length of the signature and the required computational cost. Let C_p be pairing operation, C_* be multiplication in G_1 and C_e be exponentiation in G_2. C_h be hash operation and C_i be inverse operation. Add operation in G_1 are be neglected. We assume that the bit length of element in G_1 is $|G_1|$(assume that $|G_1| = |G_2|$). From the Table 1, we know that on the whole, our proposed scheme is more efficient, and the size of signature is only $2|G_1|$ in our proposed scheme.

Table 1
Comparison between our scheme with Kumar et al. scheme and Susilo et al.'s scheme

Scheme	Length	Signing cost	Verifying cost
K-scheme	$4\|G_1\|$	$1C_p$+$5C_*$+$1C_h$+$1C_i$	$4C_p$+$1C_h$
S-scheme	$2\|G_1\| + \|H\|$	$1C_p$+$2C_*$+ $1C_e$+$1C_h$+$1C_i$	$2C_p$+$1C_*$+ $2C_e$+$1C_h$
Our-scheme	$2\|G_1\|$	$1C_p$+$1C_*$+$1C_h$	$1C_p$+$1C_h$

5.2. ID-based designated verifier proxy signature scheme

As a direct corollary of our ID-based designated verifier signature scheme, we give a new ID-based designated verifier proxy signature scheme. Our proxy signature scheme has five phases: Setup phase, Key generation phase, Proxy key generation, Proxy signature generation phase, Proxy signature verification phase. The Setup phase and Key generation are as same as that of Zhang-Mao scheme except $H_2 : \{0,1\}^* \times G_2 \to G_1$ in our scheme. So, we only describe the last three phases.

- *Proxy key generation:* The original signer Alice chooses one random number $r \in Z_q^*$ and computes

  $$U = rQ_{\mathrm{IDA}}$$
  $$\sigma = H_2(W, e(rQ_{\mathrm{IDB}}, S_{\mathrm{IDA}}).$$

  Here W is the warrant which records the identities of the original signer and the proxy signer, and the valid period, etc., Q_{IDB} is the public key of the proxy signer Bob. Alice sends (σ, W, U) to Bob. Bob accepts (σ, W, U) if and only if $\sigma = H_2(W, e(U, S_{\mathrm{IDB}}))$.
- *Proxy signature generation:* The proxy signer Bob computes the proxy signature on message M as follows: Bob chooses one random number $t \in Z_q^*$ and computes

  $$X = tQ_{\mathrm{IDB}}$$
  $$S_{IDP} = t^{-1}\sigma + S_{\mathrm{IDB}}$$
  $$V = H_2(M, W, e(tQ_{\mathrm{IDC}}, S_{\mathrm{IDP}}).$$

  Bob sends (M, W, σ, X, V) to the designated proxy verifier Cindy.
- *Proxy signature verification:* On receiving (M, W, σ, X, V) the designated verifier Cindy performs as follows:
  1. Checks whether the message M confirms to the warrant W. if not, stops. Otherwise, continues.
  2. Checks whether Alice and Bob are specified as the original signer and the proxy signer in the warrant W, respectively.
  3. If all validation passes, Cindy accepts the signature if and only if $V = H_2(M, W, e(Q_{\mathrm{IDC}}, \sigma)e(S_{\mathrm{IDC}}, X))$.

6. Conclusion

In this paper. we show that Zhang-Mao ID-based designated verifier signature scheme and Lal-Verma ID-based designated verifier proxy signature scheme do not satisfy the strong property of the designated verifier signature. In their schemes anyone who intercepts one signature can verify subsequent signatures. We also propose new and efficient ID-based designated verifier signature scheme and proxy signature scheme.

References

[1] Chaum, Van Antwerpen H. Undeniable signature. In: Advance in Crypto'89. LNCS, 435. Springer-Verlag; 1990. p. 212–6.
[2] Huang X, Susilo W, Mu Y, Zhang F. Short designated verifier signature scheme and its identity-based variant. Int J Network Security 2003;6(1):82–93.
[3] Jakobsson, Sako K, Impagliazzo R. Designated verifier proofs and their applications. In: Advances in Eurocrypt'96. LNCS, 1070. Springer-Verlag; 1996. p. 143–54.
[4] Kumar K, Shailaja G, Saxena A. Identity based strong designated verifier signature scheme. Cryptography eprint Archive Report 2006/134. Available at http://eprint.iacr.org/complete/2006/134.pdf.
[5] Saeednia S, Kramer S, Markovitch O. An efficient strong designated verifier signature scheme. In: ICISC 2003, Berlin: Springer-Verlag; 2003, p. 40–54.
[6] Susilo W, Zhang F, Mu Y. Identity-based strong designated verifier signature schemes. In: ACISP 2004. LNCS 3108; 2004, p. 313–24.
[7] Zhang J, Mao J. A novel ID-based designated verifier signature scheme. Inf Sci 2008;178:733–66.
[8] Sunder Lal, Vandani Verma, Identity base strong designated verifier proxy signature schemes. Cryptography eprint Archive Report 2006/394. Available at http://eprint.iacr.org/complete/2006/394.pdf.