A Secure Modified ID-based Undeniable Signature Scheme

Sherman S.M. Chow * Lucas C.K. Hui S.M. Yiu K.P. Chow
Department of Computer Science
University of Hong Kong
Hong Kong
email: {smchow, hui, smyiu, chow}@cs.hku.hk

Abstract

Han *et al.* proposed the first identity-based undeniable signature scheme at the fourth ACM conference on electronic commerce. Zhang *et al.* showed two attacks (the denial attack and the forge attack) against the scheme. In this paper, we modify the scheme to make it secure against these attacks. We also show how to modify our scheme to make it be an ID-based *convertible* undeniable signature scheme.
Keywords: undeniable signatures, identity-based signatures, convertible undeniable signature, bilinear pairings, e-commerce.

1 Introduction

Digital signature is an important cryptographic primitive. A digital signature binds a signer to an e-document. The validity of the digital signature can be verified by any person who received it without any help from the signer. This feature is undesirable in some applications. For example, Bob can show a signed love letter from Alice to a third party without the consent of Alice and Alice cannot deny to be the author of the letter. To overcome this deficiency of digital signature, D. Chaum *et al.* introduced the *undeniable signature* [2]. To verify an undeniable signature, the verifier must go through an interactive protocol with the signer.

Most of the digital (and undeniable) signature schemes are based on a public key infrastructure (PKI). As an alternative to PKI, A. Shamir introduced the concept of identity-based (ID-based) signature schemes [7] and the design of ID-based schemes have attracted a lot of attention recently [3, 6].

At the fourth ACM conference on electronic commerce (EC'03), Han *et al.* proposed the first ID-based undeniable signature scheme[1] [5], but their scheme was not secure against the denial attack and the forge attack [8]. In this paper, we modified Han *et al.*'s scheme to make it secure against Zhang *et al.*'s attacks.

We say an undeniable signature scheme is *convertible* if the alleged signature can be converted into an universally verifiable signature by the signer. We also show how to modify our scheme to make it be an ID-based *convertible* undeniable signature scheme.

The rest of the paper is organized as follows. Section 2 reviews Han *et al.*'s scheme and a minor flaw in their scheme is discussed. Section 3 reviews Zhang *et al.*'s attacks. Our new scheme based on Han *et al.*'s scheme is described in Section 4 together with a security analysis. We conclude the paper in Section 5.

2 Han *et al.*'s Scheme

We first review Han *et al.*'s ID-based undeniable scheme using their notations [5]. Then, we show that the changes they proposed to the scheme to prevent the signer from denying a valid signature do not work.

* corresponding author

[1] The authors claim that the scheme is a confirmer signature scheme, but it is actually an undeniable signature scheme (as this has also been pointed out by Zhang *et al.* in [8]).

Their Scheme: Let $\mathbb{G}_1$ be a cyclic additive group of prime order q, and $\mathbb{G}_2$ be a cyclic multiplicative group with the same order q. The bilinear pairing is given as $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. The modified Weil pairing [1] and the Tate pairing [4] are admissible pairing functions. Let H, H_0 be two cryptographic hash functions where $H : \{0,1\}^* \rightarrow \mathbb{Z}_q$ and $H_0 : \{0,1\}^* \rightarrow \mathbb{G}_1$. Let A be a larger number about 10^{20} and $[A] = \{1, 2, \cdots, A\}$.

- **Setup:** Let P be the generator of $\mathbb{G}_1$, the Key Generation Center (KGC) chooses $s \in \mathbb{Z}_q^*$ randomly. It sets $P_{pub} = sP$. The master-key is s, which is kept secret and known only by itself. The system parameters are $\{\mathbb{G}_1, \mathbb{G}_2, q, P, e, H, H_0, A\}$.
- **Extraction:** Signer with identity $ID \in \{0,1\}^*$ submits ID to KGC. KGC sets the signer's public key Q_{ID} to be $H_0(ID) \in \mathbb{G}_1$, computes the signer's private key (D_{ID}, L_{ID}) by $D_{ID} = sQ_{ID}$ and $L_{ID} = s^{-1}Q_{ID}$. Then KGC sends the private key to the signer.
- **Signing:** To sign a message $m \in \{0,1\}^*$, signer chooses a random $k \in \mathbb{Z}_q^*$, and sets the alleged signature to be $\{r, S\} = \{kP, k^{-1}D_{ID} + H(m)L_{ID}\}$.
- **Confirmation:**
  1. Verifier randomly chooses $x \in [A]$, $y \in \mathbb{Z}_q^*$, and sends $C_1 = xyr$, $C_2 = xyP$ to signer.
  2. Signer computes $X = e(r + P_{pub}, P - L_{ID})$ and $R = e(C_1, L_{ID})$, then sends them to verifier.
  3. Verifier checks whether $e(r, S)^x = e(P_{pub}, Q_{ID})^x R^{H(m)y^{-1}}$ and $R^{y^{-1}} X^x e(P, Q_{ID})^x = e(r + P_{pub}, P)^x$. If all of the equalities hold, then the verifier accepts the signature as valid. Otherwise, the validity of the signature remains undetermined.
- **Denial:**
  1. Verifier randomly chooses $x \in [A]$, $y \in \mathbb{Z}_q^*$, and sends $C_1 = xyr$, $C_2 = xyP$ to signer.
  2. Signer computes $B = \frac{e(C_1,S)}{e(C_2,D_{ID})e(C_1,L_{ID})^{H(m)}}$ and sends it to verifier.
  3. Verifier calculates the inverse of y and sends $C = B^{y^{-1}}$ to signer.
  4. Signer computes x' from C by computing $\frac{e(r,S)}{e(P_{pub},Q_{ID})e(r,L_{ID})^{H(m)}}$ and sends x' to verifier.
  5. Verifier checks whether $x' = x$. If the equality holds, verifier accepts the signature as invalid. Otherwise, the invalidity of the signature remains undetermined.

A Minor Flaw: The scheme described in the previously cannot prevent a signer from denying a valid signature. The reason behind is that verifier has no way to verify the values of D_{ID} and L_{ID} used in B are valid based only on the value of B. So, the authors proposed some changes to the denial protocol to handle this problem. We find that the proposed changes will make the scheme fail in handling an invalid signature.

Their Proposed Changes: In Step 2 of the denial protocol, in addition to B, the signer also sends $G = e(C_2, D_{ID})$ and $R = e(C_1, L_{ID})$ to the verifier. The verifier can check whether $e(r, S)^x = G^{y^{-1}} R^{H(m)y^{-1}}$. If this equality does not hold, the verifier aborts the protocol and concludes that the signer is lying.

The Flaw of Proposed Changes: If the signature $\{r, S\}$ is valid, the changes work. However, if $\{r, S\}$ is an invalid signature, the equality does not hold even if both G and R are valid. In other words, the signer cannot deny an invalid signature based on the changes proposed even if the signer complies legally with the protocol.

3 Zhang *et al.*'s Attacks

In this section, we review the two attacks given by Zhang *et al.* [8]. These attacks are based on the Han *et al.*'s scheme without the changes described in Section 2.

The Denial Attack: Denial attack is an attack launched by the signer to deny a valid signature. The proposed attack is given as follows. After the verifier sends C_1 and C_2 to the signer, the signer picks $\alpha \in \mathbb{Z}_q^*$, computes $B = e(C_2, \alpha P)$ and sends it to the verifier.

Then the verifier sends $C = B^{y^{-1}}$ to the signer according to the denial protocol. As $C = e(P, \alpha P)^x$, the signer can find x' from $[A]$ such that $C = e(P, \alpha P)^{x'}$, the verifier is convinced that the alleged signature $\{r, S\}$ is not created by the signer.

The Forge Attack: Forge attack is an attack launched by an entity to forge a signature with an arbitrary identity ID on any message m. The steps are given as follows. To forge a signature for message $m \in \{0,1\}^*$, the attacker $\mathcal{A}$ picks $\beta \in \mathbb{Z}_q^*$ randomly in addition to the k as in the original signing step. Without the knowledge of D_{ID} and L_{ID}, $\mathcal{A}$ forms the alleged signature $\{r, S\}$ by computing $r = kP_{pub}$ and $S = k^{-1}(Q_{ID} + \beta H(m)P)$.

In the confirmation protocol, after the verifier sends C_1 and C_2 to $\mathcal{A}$, $\mathcal{A}$ computes X and R by the equations $X = e(r + P_{pub}, P)e(P, Q_{ID})^{-1}e(P_{pub}, \beta P)^{-1}$ and $R = e(\beta P_{pub}, C_2)$, then $\mathcal{A}$ sends them to the verifier. It can be shown that both equalities $e(r, S)^x = e(P_{pub}, Q_{ID})^x R^{H(M)y^{-1}}$ and $R^{y^{-1}} X^x e(P, Q_{ID})^x = e(r + P_{pub}, P)^x$ hold. In other words, the verifier will be convinced that the signature $\{r, S\}$ for a message m is a valid signature of the signer with identity ID.

4 The Modified Scheme

- **Setup:** Same as Han *et al.*'s scheme. In addition, KGC sets $P_{inv} = s^{-1}P$ and publishes it. i.e. The system parameters are $\{\mathbb{G}_1, \mathbb{G}_2, q, P, P_{inv}, e, H, H_0, A\}$.
- **Extraction** and **Signing** : Same as Han *et al.*'s scheme.
- **Confirmation & Denial:** To confirm or deny a signature $\{r, S\}$ for a message m,
  1. Verifier chooses $x \in [A], y \in \mathbb{Z}_q^*$ uniformly and randomly, and sends $C_1 = xyr = xykP$, $C_2 = xyP$ to signer.
  2. Signer chooses $z \in \mathbb{Z}_q^*$ uniformly and randomly, sets $X = e(r + P_{pub}, P - L_{ID})$, $T = z^{-1}C_1$, $U = z^{-1}C_2$, $V = zL_{ID}$, $W = zP$ and sends them to verifier.
  3. Verifier checks the validity of T and W by checking whether $e(T, W) = e(z^{-1}C_1, zP) = e(C_1, P)$.
  4. Verifier checks the validity of U and V by checking whether $e(U, V) = e(z^{-1}C_2, zs^{-1}Q_{ID}) = e(xyP_{inv}, Q_{ID})$ by using the knowledge of x and y.
  5. Verifier checks whether z in the expression $U = z^{-1}C_2$ and z in the expression $W = zP$ are the same by checking whether $e(U, W) = e(z^{-1}C_2, zP) = e(C_2, P)$.
  6. If not all of the equalities hold, then verifier will consider signer is lying and the verification procedures will be aborted; otherwise, verifier computes $R = e(T, V) = e(C_1, L_{ID})$.
  7. To confirm a valid signature, the signer computes $X = e(r + P_{pub}, P - L_{ID})$, verifier checks the validity of signature by checking whether $e(r, S)^x = e(P_{pub}, Q_{ID})^x R^{H(m)y^{-1}}$ and $R^{y^{-1}} X^x e(P, Q_{ID})^x = e(r + P_{pub}, P)^x$. If all of the equalities hold, then verifier accepts the signature as valid. Otherwise, the validity of the signature is undetermined.
  8. To deny an invalid signature,
     (a) Verifier computes $B = \frac{e(C_1, S)}{e(xyP_{pub}, Q_{ID})R^{H(m)}}$ and sends $C = B^{y^{-1}}$ to signer.
     (b) Signer computes x' from C by computing $\frac{e(r,S)}{e(P_{pub}, Q_{ID})e(r, L_{ID})^{H(m)}}$ and sends x' to verifier.
     (c) If $x' = x$, verifier accepts the signature as invalid. Otherwise, the invalidity is undetermined.

Security Analysis: The denial attack given in [8] is prevented since R is calculated by verifier instead of by signer. Although R is calculated based on the information (T, U, V and W) provided by signer, signer does not know y and hence cannot cheat by providing "invalid" T, U, V and W that can pass the validity check of verifier. Similarly, the forge attack given in [8] is prevented since the attack is made possible by setting $R = e(\beta P_{pub}, C_2)$ where β is chosen by the attacker. Moreover, the private key of signer will not be compromised since verifier does not know z.

Furthermore, our scheme is *convertible* if signer chooses k in a way that is recoverable by the signer only for each message to be signed instead of a random one (e.g. setting $k = H(M||D_{ID}||L_{ID})$). Releasing k turns the alleged signatures into ordinary digital signatures since verifier can prove the validity of the alleged signature by showing that $e(r, S) = e(P_{pub}, Q_{ID})e(kP_{inv}, H(M)Q_{ID})$.

5 Conclusion

We proposed an identity-based convertible undeniable signature scheme from pairings based on Han *et al.*'s defective scheme. Our proposed scheme is secure against Zhang *et al.*'s attacks.

References

[1] Dan Boneh and Matt Franklin. Identity-Based Encryption from the Weil Pairing. In Joe Kilian, editor, *Advances in Cryptology - CRYPTO 2001, 21st Annual International Cryptology Conference, Santa Barbara, California, USA, August 19-23, 2001, Proceedings*, volume 2139 of *Lecture Notes in Computer Science*, pages 213–229. Springer-Verlag Heidelberg, 2001.

[2] David Chaum and Hans Van Antwerpen. Undeniable Signatures. In Gilles Brassard, editor, *Advances in Cryptology - CRYPTO '89, 9th Annual International Cryptology Conference, Santa Barbara, California, USA, August 20-24, 1989, Proceedings*, volume 435 of *Lecture Notes in Computer Science*, pages 212–216. Springer, 1990.

[3] Sherman S.M. Chow, S.M. Yiu, Lucas C.K. Hui, and K.P. Chow. Efficient Forward and Provably Secure ID-Based Signcryption Scheme with Public Verifiability and Public Ciphertext Authenticity. In Jong In Lim and Dong Hoon Lee, editors, *Information Security and Cryptology - ICISC 2003, 6th International Conference Seoul, Korea, November 27-28, 2003, Revised Papers*, volume 2971 of *Lecture Notes in Computer Science*, pages 352–369. Springer, 2003.

[4] Steven D. Galbraith, Keith Harrison, and David Soldera. Implementing the Tate Pairing. In Claus Fieker and David R. Kohel, editors, *Algorithmic Number Theory, 5th International Symposium, ANTS-V, Sydney, Australia, July 7-12, 2002, Proceedings*, volume 2369 of *Lecture Notes in Computer Science*, pages 324–337. Springer, 2002.

[5] Song Han, Winson K.Y. Yeung, and Jie Wang. Identity-based Confirmer Signatures from Pairings over Elliptic Curves. In *Proceedings of the 4th ACM conference on Electronic commerce*, pages 262–263. ACM Press, 2003.

[6] Florian Hess. Efficient Identity Based Signature Schemes based on Pairings. In Kaisa Nyberg and Howard M. Heys, editors, *Selected Areas in Cryptography, 9th Annual International Workshop, SAC 2002, St. John's, Newfoundland, Canada, August 15-16, 2002. Revised Papers*, volume 2595 of *Lecture Notes in Computer Science*, pages 310–324. Springer, 2003.

[7] Adi Shamir. Identity-Based Cryptosystems and Signature Schemes. In G. R. Blakley and David Chaum, editors, *Advances in Cryptology, Proceedings of CRYPTO 1984, Santa Barbara, California, USA, August 19-22, 1984, Proceedings*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer-Verlag, 19–22 August 1985.

[8] Fangguo Zhang, Reihaneh Safavi-Naini, and Willy Susilo. Attack on Han *et al.*'s ID-based Confirmer (Undeniable) Signature at ACM-EC'03. Cryptology ePrint Archive, Report 2003/129, 2003. Available at http://eprint.iacr.org.