Attack on Han *et al.*'s ID-based Confirmer (Undeniable) Signature at ACM-EC'03

Fangguo Zhang, Reihaneh Safavi-Naini and Willy Susilo

School of Information Technology and Computer Science
University of Wollongong, NSW 2522 Australia
{fangguo, rei, wsusilo}@uow.edu.au

Abstract. At the fourth ACM conference on electronic commerce (EC'03), S. Han, K.Y. Yeung and J. Wang proposed an ID-based confirmer signature scheme using pairings (actually, this is an ID-based undeniable signature scheme). However, in this paper, we will show that this signature scheme is not secure. The signer can deny any signature, even this signature is his 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.

Key words Confirmer signature, Undeniable signature, Attack, Bilinear pairings, ID-based cryptography.

1 Introduction

Undeniable signatures, introduced by Chaum and Van Antwerpen [1], are public key digital signatures which cannot be verified without 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. In recent years, the bilinear pairings have been found various applications in cryptography and have allowed us to construct some new cryptographic primitives. More precisely, they are basic tools for construction of ID-based cryptographic schemes. At the fourth ACM conference on electronic commerce (EC'03), S. Han, K.Y. Yeung and J. Wang proposed an ID-based confirmer signature scheme using pairings, actually, this is an ID-based undeniable signature scheme, and they declared that their scheme had soundness property. However, in this paper, we will show that this signature scheme is not secure. We propose two attacks on it: The signer can misuse the verifying operation to prove a valid signature to be invalid and any one can forge a signature for arbitrary message and prove this invalid signature to be valid.

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 $P_{pub} = sP$, and keeps s as the *master-key*, which is known only by itself.
- **Extraction:** A signer submits his identity information $ID \in \{0,1\}^*$ to KGC. KGC computes the signer's public key as $Q_{ID} = H_0(ID)$, and returns $D_{ID} = sQ_{ID}$ and $L_{ID} = s^{-1}Q_{ID}$ 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 $S = k^{-1}D_{ID} + H(m)L_{ID}$. 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 $X = e(r + P_{pub}, P - L_{ID})$ and $R = e(C_1, L_{ID})$, and sends them to the verifier.
  - The verifier checks whether

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

$$R^{y^{-1}} X^x e(P, Q_{ID})^x = e(r + P_{pub}, P)^x.$$

    If the above equalities hold, then the verifier accepts the signature as valid. Otherwise, the validity of the signature is undetermined.
- **Denial:** To deny an invalid signature,
  - The verifier sets $C_1 = xyr, C_2 = xyP$ and sends them to Signer.
  - The signer computes $B = \frac{e(C_1, S)}{e(C_2, D_{ID})e(C_1, L_{ID})^{H(m)}}$ and sends it to the verifier.
  - The verifier sends $C = B^{y^{-1}}$ to the signer.
  - The signer computes x' from C, and sends x' to the verifier. At last, the verifier will be verifying whether $x' = x$. If it holds, the verifier accepts the signature as invalid. Otherwise, the invalidity is undetermined.

About the completeness and the security analysis of this scheme, the readers can refer to [3] for detail.

3 Attack

Now, we give two attacks on Han *et al.*'s ID-based confirmer signature scheme. First, the signer can deny any signature, even this signature is his valid signature (we call this **Denial attack**). Second, suppose that there is an attacker $\mathcal{A}$. Then we show that $\mathcal{A}$ can imitate the signer with identity ID to forge a signature for any message m, and then prove to the verifier that this forged signature is valid signature of the signer with identity ID (we call this **Forge attack**).

Denial attack: Suppose that $\{r, S\}$ is a valid signature of the signer, but the signer wants to deny it.

- The verifier sets $C_1 = xyr, C_2 = xyP$ and sends them to the signer.
- The signer picks $\alpha \in Z_q^*$ and computes $B = e(C_2, \alpha P)$ and sends it to the verifier.
- The verifier sends $C = B^{y^{-1}}$ to the signer.
- The signer computes x' from C, and sends x' to the verifier.

Since $C = B^{y^{-1}} = e(P, \alpha P)^x$, the signer can test x' from $[A]$ for C and find such x'. The verifier can check $x' = x$ is really true and then believes that $\{r, S\}$ is not Signer's.

Forge attack:

- **Sign:** To forge a signature for message $m \in \{0,1\}^*$, $\mathcal{A}$ first picks $k, \beta \in Z_q^*$ randomly, sets $r = kP_{pub}$ and $S = k^{-1}(Q_{ID} + \beta H(m)P)$. Then the signature on m is $\{r, S\}$.
- **Confirmation:** To confirm a signature $\{r, S\}$ for a message m,
  - The verifier chooses $x \in [A], y \in Z_q^*$ uniformly and randomly, sets $C_1 = xyr, C_2 = xyP$ and sends them to $\mathcal{A}$.
  - $\mathcal{A}$ computes $X = e(r + P_{pub}, P)e(P, Q_{ID})^{-1}e(P_{pub}, \beta P)^{-1}$ and $R = e(\beta P_{pub}, C_2)$, and sends them to the verifier.
  - The verifier checks whether

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

$$R^{y^{-1}} X^x e(P, Q_{ID})^x = e(r + P_{pub}, P)^x.$$

Because

$$\begin{aligned}
&e(r, S)^x \\
&= e(kP_{pub}, k^{-1}(Q_{ID} + \beta H(m)P))^x \\
&= e(P_{pub}, Q_{ID})^x e(P_{pub}, \beta H(m)P)^x \\
&= e(P_{pub}, Q_{ID})^x e(\beta P_{pub}, xyP)^{H(m)y^{-1}} \\
&= e(P_{pub}, Q_{ID})^x R^{H(m)y^{-1}}
\end{aligned}$$

$$\begin{aligned}
&R^{y^{-1}} X^x e(P, Q_{ID})^x \\
&= e(\beta P_{pub}, C_2)^{y^{-1}} (e(r + P_{pub}, P)e(P, Q_{ID})^{-1}e(P_{pub}, \beta P)^{-1})^x e(P, Q_{ID})^x \\
&= e(r + P_{pub}, P)^x
\end{aligned}$$

The verifier will believe that the signature $\{r, S\}$ for a message m is valid signature of the signer with identity ID and accept it.

4 Conclusion

In this paper, we propose two attacks on Han *et al.*'s ID-based confirmer (undeniable) signature scheme from pairings: Signer can deny any signature, even this signature is his 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.

References

1. D. Chaum and H. van Antwerpen, *Undeniable signatures*, CRYPTO '89, LNCS 435, pp. 212-216, Springer-Verlag, 1990.
2. D. Chaum, *Designated confirmer signatures*, EUROCRYPT 94, LNCS 950, pp. 86-91, Springer-Verlag, 1995.
3. S. Han, K.Y. Yeung and J. Wang, *Identity-based confirmer signatures from pairings over elliptic curves*, Proceedings of ACM conference on Electronic commerce citation 2003, San Diego, CA, USA, June 09 - 12, 2003. pp.262-263.