An Attack on Libert et al.'s ID-Based Undeniable Signature Scheme

Zichen Li[2], C. F. Chong[1], Lucas Chi-Kwong Hui[1], Siu-Ming Yiu[1], K. P. Chow[1], Wai-Wan Tsang[1], H. W. Chan[1], and Kelvin K. H. Pun[1]
(Corresponding author: S. M. Yiu)

Department of Computer Science, The University of Hong Kong[1]
Pokfulam, Hong Kong (Email: smyiu@cs.hku.hk)
Department of Computer Science & Technology, Henan Polytechnic University, Jiaozuo 454003, PRC[2]

(Received Dec. 1, 2005; revised and accepted Apr. 7, 2006)

Abstract

In 2004, Libert and Quisquater proposed an identity based undeniable signature scheme using pairings over elliptic curves. In this article, we show that the scheme is not secure. In particular, if a valid message-signature pair has been revealed, an adversary can forge the signer's signature for any arbitrary message for which the signer has no way to deny it. More importantly, through this example, we illustrate that the bilinear property of pairings, although is useful for the design of cryptographic schemes, is also a source for security flaws.

Keywords: Attack, bilinear pairings, ID-based cryptography, undeniable signature

1 Introduction

Undeniable signature was introduced by Chaum and van Antwerpen in 1990 [2] in which only designated verifiers can validate the signature with a proof token (specific to the verifier) generated by the signer. And the signer has no way to generate a fake token to deny a valid signature. On the other hand, to simplify key management, the paradigm of identity based (ID-based) cryptography was proposed by Shamir [5]. And bilinear pairing over elliptic curves is found to be useful for designing ID-based schemes (e.g. [1]). It is natural to combine the two concepts to construct ID-based undeniable signatures. In 2004, Libert and Quisquater proposed one of an identity based undeniable signature based on bilinear pairing [4].

In this paper, we show that this undeniable signature scheme is not secure. In particular, if a valid message-signature pair has been revealed, an adversary can forge the signer's signature for any arbitrary message for which the signer has no way to deny it. More importantly, through this example, we want to highlight that while the bilinear property of pairing is helpful for designing cryptographic protocols, it is also a source for security flaws.

The rest of the paper is organized as follows. The properties of a bilinear pairing will be presented in Section 2. Section 3 reviews Libert et al.s identity based undeniable signature scheme. The attack will be given in Section 4. Section 5 concludes the paper.

2 Bilinear Pairings

Let G_1 be an additive group of prime order q and G_2 be a multiplicative group of the same order. A cryptographic bilinear pairing is a mapping $\hat{e} : G_1 \times G_1 \rightarrow G_2$ that satisfies the following properties:

- Bilinearity: $\forall P, Q \in G_1$, $\forall a, b \in Z_q^*$, we have $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$.
- Non-degeneracy: $\forall P \in G_1$, if $P \neq 0$, then $\hat{e}(P, P) \neq 1$.
- Computability: The mapping $\hat{e}$ can be efficiently computed.

3 Review of Libert et al.'s Identity Based Undeniable Signature Scheme

In this section, we review Libert et al.'s identity based undeniable signature scheme. The scheme consists of five algorithms: Setup, Keygen, Sign, Confirm, Deny. The exact procedures of the algorithms are given in the following.

- Setup:
  Given security parameters k and ℓ, the PKG (Private Key Generator) chooses groups G_1 and G_2 of prime order $q > 2^k$, a generator P for G_1, a bilinear map $\hat{e} : G_1 \times G_1 \rightarrow G_2$ and hash functions $H_1 : \{0, 1\}^\star \rightarrow G_1$,

$H_2 : \{0,1\}^\star \times \{0,1\}^\ell \times \{0,1\}^\star \to G_1$, $H_3 : G_2^3 \to Z_q$ and $H_4 : G_2^4 \to Z_q$. It randomly chooses a master key $s \in Z_q$ and computes the corresponding public key $P_{pub} = sP \in G_1$. The system's parameters are

$$params := \{q, G_1, G_2, \hat{e}, P, P_{pub}, H_1, H_2, H_3, H_4\}$$

- Keygen:
  Given a user (signer or verifier) with an identity ID, the PKG computes $Q_{ID} = H_1(ID) \in G_1$ and the associated private key $d_{ID} = sQ_{ID} \in G_1$ which will be transmitted to the user.

- Sign:
  To sign a message $M \in \{0,1\}^*$,the signer Alice with identity ID_A and private key d_{ID_A} computes $\gamma = \hat{e}(H_2(M, r, ID_A), d_{ID_A}) \in G_2$, where $r \in \{0,1\}^\ell$ is a random string picked by Alice. Then, the pair (r, γ) is the signature on M.

- Confirm:
  To verify the signature, the designated verifier with identity ID_B will run a confirmation protocol with the signer Alice to produce a proof (U, v, h, S), where $S = R + (h + v)d_{ID_A}$, $h = H_3(c, g_1, g_2)$, $U \in G_1, R \in G_1$ and $v \in Z_q$ are randomly selected by the signer, and $c = \hat{e}(P, U)\hat{e}(P_{pub}, Q_{ID_B})$, $g_1 = \hat{e}(P, R) \in G_2$ and $g_2 = \hat{e}(H_2(M, r, ID_A), R) \in G_2$.

  To check the validity of the signature, based on the proof (U, v, h, S) for the signature (r, γ) on the message M from the signer, the verifier will first compute $c' = \hat{e}(P, U)\hat{e}(P_{pub}, Q_{ID_B})$, $g'_1 = \hat{e}(P, S)\hat{e}(P_{pub}, Q_{ID_A})^{h+v}$ and $g'_2 = \hat{e}(H_2(M, r, ID_A), S)\gamma^{h+v}$ and accepts if and only if $h' = H_3(c', g'_1, g'_2)$.

- Deny:
  To convince a designated verifier with identity ID_B that a given signature (r, γ) is not a valid signature, the signer Alice will run the denying protocol, and produce a proof (C, U, v, h, S, s), where $C = (\frac{\hat{e}(H_2(M,r,ID_A),\ d_{ID_A})}{\gamma})^\omega$, $S = V + (h+v)R \in G_1$, $s = v + (h + v)\alpha$, $h = H_4(C, c, \rho_1, \rho_2)$, $U \in G_1, V \in G_1$, $v \in Z_q, \omega \in Z_q$, are randomly selected by the signer, and $c = \hat{e}(P, U)\hat{e}(P_{pub}, Q_{ID_B})^v$, $\rho_1 = \hat{e}(H_2(M, r, ID_A), V)\gamma^{-v} \in G_2$ and $\rho_2 = \hat{e}(P, V)y^{-v} \in G_2$, $y = \hat{e}(P_{pub}, Q_{ID_A})$, $\alpha = \omega$, $R = \omega d_{ID_A}$.

  Based on this proof (C, U, v, h, S, s) for the signature (r, γ) on the message M from the signer, if $C = 1$, the designated verifier will reject the proof immediately. Otherwise, the verifier will compute $c' = \hat{e}(P, U)\hat{e}(P_{pub}, Q_{ID_B})^v$, $\rho'_1 = \hat{e}(H_2(M, r, ID_A), S)\gamma^{-s}C^{-(h+v)}$ and $\rho'_2 = \hat{e}(P, S)y^{-s} \in G_2$, $y = \hat{e}(P_{pub}, Q_{ID_A})$, and accepts the proof if and only if $h' = H_4(C, c', g'_1, g'_2)$.

4 The Attack

Now, we present an attack on Libert et al.'s identity based undeniable signature scheme. Suppose that an attacker has the information that (r, γ) is a valid signature, signed by the signer Alice with identity ID_A, for the message M, then the attacker is able to forge a signature for Alice on any message M^* as follows.

1) He picks a random string $r^* \in \{0, l\}^\ell$;

2) Computes $H_2(M^*, r^*, ID_A) \in G_1$;

3) Then, computes

$$\begin{aligned} k &= \frac{H_2(M^*, r^*,\ ID_A)}{H_2(M, r, ID_A)}\ mod\ q \\ &= H_2(M^*, r^*, ID_A)H_2(M, r, ID_A)^{-1}\ mod\ q. \end{aligned}$$

4) Finally, computes $\gamma^* = \gamma^k\ modq$.

The pair $(r^*,\ \gamma^*)$ is a forged signature on the message M^*. The following lemma shows that the forged signature is a *valid* signature on M^* if r^* is the random string selected by the signer in Sign algorithm.

Lemma 1. *Let $r^* \in 0, 1^\ell$ be the random string selected by the signer in the procedure Sign algorithm of Libert et al.'s scheme and (r^*, γ') be the corresponding signature computed by the procedure. Then, $\gamma^* = \gamma'$.*

Proof. Based on the procedure Sign algorithm of Libert et al.'s scheme, $\gamma' = \hat{e}(H_2(M^*, r^*, ID_A), d_{ID_A})$. From the revealed message-signature pair, $\gamma = \hat{e}(H_2(M, r, ID_A), d_{ID_A})$ and since $\gamma^* = \gamma^k\ mod\ q$, based on the bilinear property of $\hat{e}$, we have the following.

$$\begin{aligned} \gamma^* &= \hat{e}(H_2(M, r, ID_A), d_{ID_A})^k \\ &= \hat{e}(kH_2(M, r, ID_A), d_{ID_A}). \end{aligned}$$

Note that $k = H_2(M^*, r^*, ID_A)H_2(M, r, ID_A)^{-1}\ mod\ q$, we have the following.

$$\begin{aligned} \gamma^* &= \hat{e}(kH_2(M, r, ID_A), d_{ID_A}) \\ &= \hat{e}(H_2(M^*, r^*, ID_A), d_{ID_A}) \\ &= \gamma'. \end{aligned}$$

Thus, Lemma 1 is established. □

Lemma 2. *Let $(r^*,\ \gamma^*)$ be the forged signature generated by the attacker. Going through the procedure Confirm algorithm, the signer will produce a proof showing that the signature is valid. On the other hand, the signer cannot deny this forged signature with the denying protocol.*

Proof. Based on Lemma 1, if r^* is selected by the signer in the procedure Sign algorithm, then the signature produced will be exactly the same as (r^*, γ^*). So, a correct proof will be produced by the signer by executing the confirmation protocol. Similarly, the signer is not able to convince the verifier that the signature is invalid using the denying protocol. □

Combining Lemmas 1 and 2, we show that the attacker is able to forge the signer's signature for any message once a valid message-signature pair has been revealed.

5 Conclusion

In this paper, we have shown that the identity based undeniable signature scheme proposed by Libert and Quisquater is not secure. In particular, once a valid message-signature pair has been revealed, the attacker is able to forge signatures of the signer for any message. Interestingly, while the design of the signature scheme relies on the property of bilinear mapping, the attack is also based on the same property of the bilinear mapping. As a remark, we have published a secure version of an identity based undeniable signature scheme in [3].

References

[1] D. Boneh and M. Franklin, "Identity-based encryption from the Weipairing," *Advances in Cryptology, Crypto'2001*, LNCS 2139, pp. 213-229, Springer-Verlag, 2001.

[2] D. Chaum and H. Van Antwerpen, "Undeniable signatures," *Advances in Cryptology, CRYPTO'89*, LNCS 435, pp. 212-216, Springer-Verlag, 1990.

[3] S. S. M. Chow, L. C. K. Hui, S. M. Yiu, and K. P. Chow, "A secure modified Id-based undeniable signature scheme," *Cryptology ePrint Archive*, Report 2003/262, 2003, http://eprint.iacr.org/.

[4] B. Libert and J. J. Quisquater, "Identity based undeniable signatures," *Topics in Cryptology, CT-RSA'2004*, LNCS 2964, pp. 112-125, Springer-Verlag, 2004.

[5] A. Shamir, "Identity based cryptosystems and signature schemes," *Advances in Cryptology, CRYPTO'84*, LNCS 196, pp. 47-53, Springer-Verlag, 1984.

Li Zichen received his Ph.D degree in EE, M.S. and B.S. degree in applied mathematics in 1999, 1985 and 1986, respectively. He is currently a professor in the School of Computer Science and Technology, Henan Polytechnic University, China. His research interests include coding theory, communications theory, modern cryptography, and signal processing.

C.F. Chong is a Lecturer in Department of Computer Science of the University of Hong Kong. His research interests are Cryptanalysis, Digital Signature Schemes, Elliptic Curve Cryptosystems.

Lucas C.K. Hui is the founder and Honorary Director of the Center for Information Security & Cryptography, and concurrently an associate professor in the Department of Computer Science in the University of Hong Kong. His research interests include Information Security, Computer Crime, Cryptographic Systems, and Electronic Commerce Security.

S.M. Yiu obtained his PhD in Computer Science from the University of Hong Kong and is currently a Research Assistant Professor in the Department of Computer Science of the same university. His research interests include information security, cryptography, and bioinformatics.

K. P. Chow is an Associate Professor in the Department of Computer Science and he is also the Associate Programme Director for the MSc in E-Commerce and Internet Computing Programme in University of Hong Kong. His research interests are cryptography and software engineering,

W. W. Tsang is an Associate Professor in Department of Computer Science of the University of Hong Kong. His research interests are Statistical Computing, Random Number Generation.

H. W. Chan is an Assistant Professor in Department of Computer Science of the University of Hong Kong. His research interests include network security, mobile computing and communication.