Security Proof of the Original SOK-IBS Scheme

Xiao-Ming Lu and Deng-Guo Feng
(Corresponding author: Xiao-Ming Lu)

State Key Lab of Information Security, Institute of Software, Chinese Academy of Sciences
Beijing 100080, P. R. China (Email: luxiaoming@chinamobile.com)

(Received Nov. 21, 2005; revised and accepted Dec. 31, 2005 & Feb. 20, 2006)

Abstract

The identity-based signature (IBS) scheme proposed by Sakai, Ohgishi and Kasahara in 2000, which we refer to as the SOK-IBS scheme, is the first pairing-based IBS scheme. Though most other existing IBS schemes, especially two modified SOK-IBS schemes, have already been proved secure recently, the security of the original SOK-IBS scheme is still unclear. In this paper, we prove that the original SOK-IBS scheme is existentially unforgeable under chosen message attacks in the random oracle model. We also show that it is not strongly existentially unforgeable under chosen message attacks, though the two modified versions of it are.

Keywords: Identity-based cryptography, identity-based signature, random oracle model, security proof

1 Introduction

Identity-based cryptography (ID-PKC) has become a hot research area in recent years. The concept was first proposed by Shamir in 1984 [17] to simplify key management and to avoid certificates. Since its appearance, several identity-based signature (IBS) schemes have been proposed [7, 10]. In 2000, Sakai, Ohgishi and Kasahara proposed the first pairing-based IBS scheme [16] (we call it the SOK-IBS scheme below). Later, Boneh and Franklin proposed the first practical identity-based encryption (IBE) scheme [4] also based on the bilinear pairings. After that, a rapid development of ID-PKC has taken place and many identity-based primitives have been proposed. Interestingly, many existing identity-based cryptographic primitives based on pairings, such as [6, 11, 14], including the Boneh-Franklin IBE scheme [4], use the same key setup algorithm that was first used in the SOK-IBS scheme [16].

The SOK-IBS scheme has an efficiency comparable to other existing IBS schemes such as [5, 11], and can obtain a higher efficiency when pre-computation is used. Besides being used to sign messages, the SOK-IBS scheme can also be used in some other applications. For example, the certification algorithm of the certificate based encryption (CBE) scheme using subcovers in [8] and the key extraction algorithm of the hierarchical identity-based encryption (HIBE) scheme in [9] can both be regarded as applications of the SOK-IBS scheme.

When security is concerned, we note that the original SOK-IBS scheme has never been analyzed till now. However, most other existing IBS schemes, especially two modified SOK-IBS schemes have already been proved secure by previous works. At Eurocrypt'04, Bellare, Namprempre and Neven [2] provided proofs for a large family of IBS schemes including a modified SOK-IBS scheme (we call it the SOK-IBS-1 scheme below) using their general framework. Later, Libert and Quisquater [13] proved that another modified SOK-IBS scheme (we call it the SOK-IBS-2 scheme below), which is also obtained through the transformation in [2], has a sub-optimal reduction from the Computational Diffie-Hellman assumption. They further showed that the SOK-IBS-2 scheme is as secure as the one more Diffie-Hellman problem. The latter reduction is the first optimal security reduction for an IBS scheme.

We note that in some applications the two modified SOK-IBS schemes [2, 13] are unable to substitute the original one, though they are only slightly different from it, and have the same efficiency with it. For example, if the HIBE scheme [9] mentioned above uses the modified SOK-IBS schemes in its key extraction algorithm, the relying party will have to lookup the user's Q values before encrypting messages to him. Consequently, the advantage of the ID-PKC– needlessness of directory– will be lost. Therefore, we think that the security of the original SOK-IBS scheme still deserves analysis.

However, the methods to prove securities of the two modified SOK-IBS schemes in [2, 13] are not suitable for the original scheme. As shown in [2], the general framework defined there cannot be applied to prove security of the original SOK-IBS scheme. The proof technique to prove the security of the SOK-IBS-2 scheme in [13] can also hardly be applied directly to prove the security of the original scheme because of the difference between the two schemes. We will discuss it in detail in Section 3. Moreover, it seems that we cannot use the forking lemma technique proposed in [15] to prove the security of the original SOK-IBS scheme, since this scheme cannot be viewed as

the result of performing the Fiat-Shamir transformation [7] on some underlying identification scheme. Though the securities of the HIBE scheme [9] and the CBE scheme [8] may imply the security of the original SOK-IBS scheme, no explicit security proof for it is given there. What is more, the securities of the HIBE scheme [9] and the CBE scheme [8] are both based on the Bilinear Diffie-Hellman assumption. We wonder if we can prove the security of the original SOK-IBS scheme based on a weaker assumption, such as the Computational Diffie-Hellman assumption, as done in [13] for the SOK-IBS-2 scheme. We also want to find whether the original SOK-IBS scheme possesses the same security property as the two modified schemes [2, 13].

In this paper, we prove that the original SOK-IBS is secure against existential forgery under chosen message attack based on the Computational Diffie-Hellman assumption. Our reduction is tighter than those exhibited in [5, 11, 12], though it is slightly looser than that in [13]. We also show that the original SOK-IBS scheme is not strongly existentially unforgeable under chosen message attacks, while the two modified schemes of it in [2, 13] are. Thus, we can see that the modifications made on the original SOK-IBS scheme in [2] improve its security and do not lower its efficiency.

The rest of the paper is organized as follows. The background definitions are given in Section 2. The original SOK-IBS scheme is presented in Section 3. We analyze the security of the original SOK-IBS scheme in Section 4. Section 5 concludes this paper.

2 Preliminaries

2.1 Bilinear Maps

Let G_1 and G_2 be two groups of order q for some large prime q. We call a map $\hat{e} : G_1 \times G_1 \rightarrow G_2$ an *admissible bilinear map*, if it satisfies the following properties:

1) Bilinear: We say that a map $\hat{e} : G_1 \times G_1 \rightarrow G_2$ is bilinear if $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ for all $P, Q \in G_1$ and all $a, b \in Z_q^*$.

2) Non-degenerate: The map does not send all pairs in $G_1 \times G_1$ to the identity in G_2.

3) Computable: There is an efficient algorithm to compute $\hat{e}(P, Q)$ for any $P, Q \in G_1$.

As shown in [4], such admissible maps can be obtained from the Weil or the Tate pairings over supersingular elliptic curves or abelian varieties.

2.2 Computational Diffie-Hellman Problem (CDHP)

Definition 1. *Let G be a cyclic group of prime order q, let P be an arbitrary generator of G, the CDH problem is, given $\langle G, P, aP, bP\rangle$ for unknown $a, b \in Z_q$, compute $abP \in G$.*

Definition 2. ***(Computational Diffie-Hellman Assumption)*** *Let $\mathcal{G}$ be a CDH parameter generator, which taking security parameter 1^k as input generates a cyclic group G of prime order q, and a generator $P \in G^*$. We define the advantage of an algorithm $\mathcal{A}$ in solving the CDH problem for $\mathcal{G}$ as*

$$Adv_{\mathcal{G},\mathcal{A}}^{CDH}(k) = Pr[\mathcal{A}(G, P, aP, bP) = abP|$$

$$\langle G, P\rangle \leftarrow \mathcal{G}(1^k),\ a, b \stackrel{R}{\leftarrow} Z_q^*]$$

We say $\mathcal{G}$ satisfies the CDH assumption if for any probabilistic polynomial time (in k) algorithm $\mathcal{A}$ the advantage $Adv_{\mathcal{G},\mathcal{A}}^{CDH}(k)$ is negligible.

2.3 Existential Unforgeability Under Chosen Message Attacks (UF-CMA)

Definition 3. *An identity-based signature scheme is said to be existentially unforgeable under chosen message attacks if no probabilistic polynomial time (PPT) adversary has a non-negligible advantage in the following game:*

1) *The challenger runs the setup algorithm to generate the system's parameters and sends them to the adversary.*

2) *The adversary $\mathcal{A}$ performs a series of queries:*

   - *Key extraction queries: $\mathcal{A}$ produces an identity ID and receives the private key d_{ID} corresponding to ID.*
   - *Signature queries: $\mathcal{A}$ produces an identity ID and a message M and receives a signature on M that is generated by the signature oracle using the private key corresponding to the identity ID.*

3) *After a polynomial number of queries, $\mathcal{A}$ produces a tuple (ID^*, M^*, σ^*) such that ID^* and (ID^*, M^*) have not been asked to the key extraction oracle and the signature oracle respectively. $\mathcal{A}$ wins the game if σ^* is a valid signature on M^* for ID^*.*

The adversary's advantage is defined to be its probability of producing a forged signature taken over the coin-flipping of the challenger and $\mathcal{A}$.

2.4 Strong Existential Unforgeability Under Chosen Message Attacks (sUF-CMA)

Definition 4. *An identity-based signature scheme is said to be strongly existentially unforgeable under chosen message attacks if no probabilistic polynomial time (PPT) adversary has a non-negligible advantage in the following game:*

1) *The challenger runs the setup algorithm to generate the system's parameters and sends them to the adversary.*

2) The adversary $\mathcal{A}$ performs a series of queries:

- *Key extraction queries: $\mathcal{A}$ produces an identity ID and receives the private key d_{ID} corresponding to ID.*
- *Signature queries: $\mathcal{A}$ produces an identity ID and a message M and receives a signature on M that is generated by the signature oracle using the private key corresponding to the identity ID.*

3) After a polynomial number of queries, $\mathcal{A}$ produces a tuple (ID^*, M^*, σ^*) such that ID^* has never been asked to the key extraction oracle and σ^* has never been returned by the signature oracle on the input (ID^*, M^*). $\mathcal{A}$ wins the game if σ^* is a valid signature on M^* for ID^*.

The adversary's advantage is defined to be its probability of producing a forged signature taken over the coin-flipping of the challenger and $\mathcal{A}$.

The notion of sUF-CMA was first proposed by An et al. in [1] and was considered in several other works [3, 13, 18]. It is slightly stronger than UF-CMA in that the adversary is required to be unable to even forge a new signature on a previously signed message.

3 The Original SOK-IBS Scheme

In this section, we recall the original SOK-IBS scheme proposed by Sakai, Ohgishi and Kasahara in [16]. The scheme consists of four algorithms:

Setup: Given a security parameter k, the PKG chooses groups G_1 and G_2 of prime order $q > 2^k$, a bilinear map $\hat{e} : G_1 \times G_1 \rightarrow G_2$, a generator P of G_1, a randomly chosen master key $s \in Z_q^*$ and the associated public key $P_{Pub} = sP$. It also picks cryptographic hash functions $H_1, H_2 : \{0,1\}^* \rightarrow G_1^*$. The system's public parameter are

$$params = (G_1, G_2, \hat{e}, P, P_{Pub}, H_1, H_2).$$

Keygen: Given a user's identity ID, the PKG computes $Q_{ID} = H_1(ID) \in G_1$ and the associated private key $d_{ID} = sQ_{ID} \in G_1$ that is transmitted to the user.

Sign: In order to sign a message M,

1) Pick $r \in_R Z_q^*$ and compute $U = rP \in G_1$ and $H = H_2(M) \in G_1$.
2) Compute $V = d_{ID} + rH \in G_1$.

The signature on M is the pair $\sigma = \langle U, V \rangle \in G_1 \times G_1$.

Verify: To verify a signature $\sigma = \langle U, V \rangle \in G_1 \times G_1$ on message M for an identity ID, the verifier first takes $Q_{ID} = H_1(ID) \in G_1$ and $H = H_2(M) \in G_1$. The verifier accepts the signature if $\hat{e}(V, P) = \hat{e}(Q_{ID}, P_{Pub})\,\hat{e}(H, U)$ and rejects it otherwise.

The difference among the original SOK-IBS scheme and the two modified schemes in [2, 13] is the definition of H. The SOK-IBS-1 scheme defines H to be $H_2(M, U)$ [2], while the SOK-IBS-2 scheme defines H to be $H_2(ID, M, U)$ [13]. We will show in the next section that the slight difference causes the security of the original scheme to differ from those of the two modified schemes.

We also note that the proof technique in [13] to prove the SOK-IBS-2 scheme cannot be used directly to prove the security of the original scheme owing to the slight difference between the two schemes. In the proofs of [13], to answer the signature query, $\mathcal{B}$ first sets the signature to be a randomly chosen pair $\langle U, V \rangle \in G_1 \times G_1$, and then calculates the value of $H = H_2(ID, M, U)$ from U and V. The probability that $\mathcal{A}$ can guess U correctly and query $H = H_2(ID, M, U)$ before querying the signature on M is slight. However, if we use this technique to prove the security of the original scheme, $\mathcal{A}$ can query $H = H_2(M)$ on each message M before querying signature on it and need not guess the value of U in advance. Consequently, $\mathcal{B}$ will always fail to answer signature queries.

4 Security Analysis

4.1 The Original SOK-IBS Scheme is UF-CMA Secure

Theorem 1. *In the random oracle model, if a PPT adversary $\mathcal{A}$ against the original SOK-IBS scheme has an advantage ϵ in forging a signature in an attack modelled by the game of Definition 3, when running in a time t and asking q_{H_i} queries to random oracle H_i $(i = 1, 2)$, q_E queries to the key extraction oracle and q_S queries to the signature oracle. Then we can construct an algorithm $\mathcal{B}$ to solve the CDH problem with the advantage ϵ' within a time t', where*

$$\begin{aligned} \epsilon' &\geq \frac{\epsilon - 1/2^k}{e^2 \cdot (1 + q_E)(1 + q_S)} \\ t' &< (1 + q_{H_1} + q_{H_2} + q_E + 2q_S)t_m + (1 + q_S)t_{mm}, \end{aligned}$$

where k denotes the security parameter of the scheme, e denotes the base of the natural logarithm, t_m denotes the time to perform a scalar multiplication in G_1 and t_{mm} denotes the time to perform a multi-exponentiation in G_1.

Proof. We show how can we use a forger $\mathcal{A}$ to construct a PPT algorithm $\mathcal{B}$ to solve the CDH problem. Let $\langle X = xP, Y = yP \rangle$ be a random instance of the CDH problem taken as input by $\mathcal{B}$. The latter initializes $\mathcal{A}$ with $P_{Pub} = X$ as system overall public key. $\mathcal{A}$ then performs queries as described by Definition 3, $\mathcal{B}$ answers the queries as follows:

- Queries on H_1 oracle: To answer the H_1 query, $\mathcal{B}$ maintains a list L^1, which is initially empty. When an identity ID is submitted to H_1 oracle, $\mathcal{B}$ first scans L^1 to check whether H_1 was already defined for that input. If it was, $\mathcal{B}$ returns the previously defined

value. Otherwise, $\mathcal{B}$ flips a coin $T_1 \in \{0,1\}$ that $Pr[T_1 = 0] = \delta_1$ and $Pr[T_1 = 1] = 1 - \delta_1$. $\mathcal{B}$ picks a random value $u \in Z_q^*$. If $T_1 = 0$, $H_1(ID)$ is defined to be uP. If $T_1 = 1$, $H_1(ID)$ is defined to be uY. Then $\mathcal{B}$ inserts a tuple (ID, T_1, u) in L^1 and returns $H_1(ID)$ to $\mathcal{A}$.

- Queries on H_2 oracle: To answer the H_2 query, $\mathcal{B}$ maintains a list L^2 which is initially empty. On input message M, $\mathcal{B}$ first scans L^2 to check whether H_2 was already defined for that input. If it was, $\mathcal{B}$ returns the previously defined value. Otherwise, $\mathcal{B}$ flips a coin $T_2 \in \{0,1\}$, with the probability $Pr[T_2 = 0] = \delta_2$ and $Pr[T_2 = 1] = 1 - \delta_2$. $\mathcal{B}$ picks a random value $r \in Z_q^*$ and stores the tuple (M, T_2, r) in L^2. If $T_2 = 0$, $\mathcal{B}$ returns $H_2(M) = rP$ to $\mathcal{A}$, otherwise, $\mathcal{B}$ returns $H_2(M) = rX$ to $\mathcal{A}$.

- Queries on key extraction oracle: On input identity ID, $\mathcal{B}$ first runs the algorithm to respond the H_1 query to obtain the tuple (ID, T_1, u). If $T_1 = 0$, the private key corresponding to ID is set to be $d_{ID} = uX$. If $T_1 = 1$, $\mathcal{B}$ reports failure and aborts.

- Queries on signature oracle: On input identity ID and message M, $\mathcal{B}$ first runs the algorithm to respond the H_1 query and the algorithm to respond the H_2 query to obtain the tuple (ID, T_1, u) and the tuple (M, T_2, r) respectively.

  1) If $T_1 = 0$, $\mathcal{B}$ sets the private key d_{ID} to be uX, and uses the private key to generate the signature.
  2) If $T_1 = 1$ and $T_2 = 1$, $\mathcal{B}$ picks a random value $v \in_R Z_q^*$, sets V to be vX, U to be $r^{-1}(vP - Q_{ID})$ and the signature σ is $\langle U, V \rangle$.
  3) If $T_1 = 1$ and $T_2 = 0$, $\mathcal{B}$ reports failure and aborts.

- Challenge: $\mathcal{A}$ outputs an identity ID^*, a message M^* and a signature $\sigma^* = \langle U^*, V^* \rangle$. $\mathcal{B}$ runs the algorithm to respond H_1 query and the algorithm to respond H_2 query to obtain the tuple (ID^*, T_1^*, u^*) and the tuple (M^*, T_2^*, r^*) respectively. If $T_1^* = 0$ or $T_2^* = 1$, $\mathcal{B}$ reports failure and aborts. Otherwise, $\mathcal{B}$ knows that

$$\hat{e}(V^*, P) = \hat{e}(Q_{ID}^*, P_{Pub})\hat{e}(H^*, U^*)$$

  with $Q_{ID}^* = u^*Y$ and $H^* = H_2^*(M) = r^*P$. Then it also knows that $\hat{e}(V^* - rU^*, P) = \hat{e}(Y, X)^{u^*}$ and that ${u^*}^{-1}(V^* - rU^*)$ is the solution to the CDH instance $(X, Y) \in G_1 \times G_1$.

Now we assess the advantage of $\mathcal{B}$. The probability of $\mathcal{B}$ not to fail in the key extraction queries is at least $\delta_1^{q_E}$. The probability not to fail in the signature queries is at least $(1 - (1 - \delta_1)\delta_2)^{q_S}$. The probability not to fail in the challenge stage is $(1 - \delta_1)\delta_2$. The probability that $\mathcal{A}$ outputs a valid signature without asking the corresponding $H_2(M^*)$ is at most $1/2^k$. Therefore, the advantage of $\mathcal{B}$ is as least

$$\begin{aligned} &(\epsilon - 1/2^k) \cdot \delta_1^{q_E} \cdot (1 - (1 - \delta_1)\delta_2)^{q_S} \cdot (1 - \delta_1)\delta_2 \\ &= (\epsilon - 1/2^k) \cdot \delta_1^{q_E} \cdot (1 - \delta_1) \cdot (1 - (1 - \delta_1)\delta_2)^{q_S} \cdot \delta_2 \\ &\geq (\epsilon - 1/2^k) \cdot \delta_1^{q_E} \cdot (1 - \delta_1) \cdot (1 - \delta_2)^{q_S} \cdot \delta_2. \end{aligned}$$

Clearly, the value $\delta_1^{q_E} \cdot (1 - \delta_1)$ is maximized at the point where its derivative equals zero, i.e., $(\delta_1^{q_E} \cdot (1 - \delta_1))' = q_E\delta_1^{q_E - 1} - (q_E + 1)\delta_1^{q_E} = 0$. Therefore, the value $\delta_1^{q_E} \cdot (1 - \delta_1)$ is maximized at $\delta_1^{opt} = \frac{q_E}{1+q_E}$, and the maximal value equals $\frac{1}{(1+\frac{1}{q_E})^{q_E}} \cdot \frac{1}{1+q_E} \geq \frac{1}{e(1+q_E)}$.

In the same way, we can get that $(1 - \delta_2)^{q_S} \cdot \delta_2$ is maximized at $\delta_2^{opt} = \frac{1}{1+q_S}$ and the maximal value equals $\frac{1}{(1+\frac{1}{q_S})^{q_S}} \cdot \frac{1}{1+q_S} \geq \frac{1}{e(1+q_S)}$.

Since δ_1 and δ_2 are independent, we know that when using δ_1^{opt} and δ_2^{opt}, $\mathcal{B}'s$ advantage is at least

$$\begin{aligned} &\frac{\epsilon - 1/2^k}{(1 + \frac{1}{q_E})^{q_E}(1 + \frac{1}{q_S})^{q_S}(1 + q_E)(1 + q_S)} \\ \geq\ &\frac{\epsilon - 1/2^k}{e^2 \cdot (1 + q_E)(1 + q_S)}. \end{aligned}$$

□

4.2 The Original SOK-IBS Scheme is not sUF-CMA Secure

Libert and Quisquater proved that the SOK-IBS-2 scheme is sUF-CMA secure in the random oracle model [13]. We note that we can apply their proof technique to prove that the SOK-IBS-1 scheme is also sUF-CMA secure. We omit the detail proof here. However, we show that the original SOK-IBS scheme is not sUF-CMA secure.

Theorem 2. *The original SOK-IBS scheme is not sUF-CMA secure.*

Proof. On receiving a signature σ on message M for an identity ID, we can easily forge a distinct signature σ' on (M, ID) without obtaining the private key corresponding to ID.

Let $\sigma = \langle U, V \rangle$ be a signature on (M, ID), with $U = rP$, $V = d_{ID} + rH$ for some unknown $r \in Z_q^*$ and $H = H_2(M)$. We can pick a random value $r' \in_R Z_q^*$ and compute $U' = U + r'P$ and $V' = V + r'H$. It is easy to verify that $\sigma' = \langle U', V' \rangle$ is a valid signature, since

$$\begin{aligned} \hat{e}(V', P) &= \hat{e}(V, P)\hat{e}(r'H, P) \\ &= \hat{e}(Q_{ID}, P_{Pub})\hat{e}(H, U)\hat{e}(r'H, P) \\ &= \hat{e}(Q_{ID}, P_{Pub})\hat{e}(H, U'). \end{aligned}$$

□

5 Conclusion

The original SOK-IBS scheme is an interesting scheme. Unlike most other existing IBS schemes such as [5, 7, 11,

17] and the two modified SOK-IBS schemes in [2, 13], the original SOK-IBS scheme cannot be viewed as the result of performing the Fiat-Shamir transformation [7] on a certain underlying identification scheme. Due to this, the general framework in [2] and the forking lemma technique in [15] can both hardly be applied to prove the security of the original SOK-IBS scheme. Till now, its security has never been analyzed. In this paper, we proved that the original SOK-IBS scheme is UF-CMA secure. Our security reduction is slightly looser than that in [13], but is tighter than those in [5, 11, 12]. We also show that the original SOK-IBS scheme is not sUF-CMA secure, though the two modified versions of it in [2, 13] are. From this point, we can see that the modifications made on the original SOK-IBS scheme in [2] improve its security and do not lower its efficiency.

Acknowledgement

We thank professor Chuan-Kun Wu, associate professor Zhen-Feng Zhang and associate professor Jing Xu for their help and valuable suggestions. We also thank the support of the National Natural Science Foundation of China(No. 60273027, No. 60373039 and No. 60503014).

References

[1] J. H. An, Y. Dodis, and T. Rabin, "On the security of joint signature and encryption", in *EUROCRYPT'02*, LNCS 2332, pp. 83-107, Springer-Verlag, Apr. 2002.

[2] M. Bellare, C. Namprempre, and G. Neven, "Security proofs for identity-based identification and signature schemes", in *EUROCRYPT'04*, LNCS 3027, pp. 268-286, Springer-Verlag, May 2004.

[3] D. Boneh and X. Boyen, "Short signatures without random oracles", in *EUROCRYPT'04*, LNCS 3027, pp. 56-73, Springer-Verlag, May. 2004.

[4] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing", in *CRYPTO'01*, LNCS 2139, pp. 213-219, Springer-Verlag, Aug. 2001.

[5] J. C. Cha and J. H. Cheon, "An identity-based signature from gap diffie-hellman groups", in *Practice and Theory in Public Key Cryptography (PKC'03)*, LNCS 2567, pp. 18-30, Springer-Verlag, Jan. 2003.

[6] L. Q. Chen and C. Kudla, "Identity based authenticated key agreement protocols from pairings", in *The 16th IEEE Computer Security Foundations Workshop (CSFW2003)*, Pacific Grove, USA, pp. 219-233, June 2003.

[7] A. Fiat and A. Shamir, "How to prove yourself: Practical solutions to identification and signature problems", in *Crypto'86*, LNCS 0263, pp. 186-194, Springer-Verlag, May. 1986.

[8] C. Gentry, "Certificate-based encryption and the certificate revocation problem", in *EUROCRYPT'03*, LNCS 2656, pp. 272-293, Springer-Verlag, May. 2003.

[9] C. Gentry and A. Silverberg, "Hierarchical id-based cryptography", in *ASIACRYPT'02*, LNCS 2501, pp. 548-566, Springer-Verlag, Dec. 2002.

[10] L. C. Guillou and J. J. Quisquater, "A 'paradoxical' indentity-based signature scheme resulting from zero-knowledge", in *Crypto'88*, LNCS 0403, pp. 216-231, Springer-Verlag, Aug. 1988.

[11] F. Hess, "Efficient identity based signature schemes based on pairings", in *Selected Areas in Cryptography (SAC'02)*, LNCS 2595, pp. 310-324, Springer-Verlag, Aug. 2002.

[12] K. Kurosawa and S. H. Heng, "From digital signature to id-based identification/signature", in *Practice and Theory in Public Key Cryptography (PKC'04)*, LNCS 2947, pp. 248-261, Springer-Verlag, Mar. 2004.

[13] B. Libert and J. J. Quisquater, "The extract security of an identity based signature and its applications", Cryptology ePrint Archive, Report 2004/102.

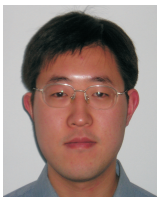
[14] N. McCullagh and P. S. Barreto, "Efficient and forward-secure identity-based signcryption", Cryptology ePrint Archive, Report 2004/117.

[15] D. Pointcheval and J. Stern, "Security arguments for digital signatures and blind signatures", *Journal of Cryptology*, vol. 13, no.3, pp. 361-396, 2000.

[16] R. Sakai, K. Ohgishi, and M. Kasahara, "Cryptosystems based on pairing", in *2000 Symposium on Cryptography and Information Security (SCIS'00)*, Okinawa, Japan, pp. 26-28, Jan. 2000.

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

[18] R. Zhang, J. Furukawa, and H. Imai, "Short signature and universal designated verifier signature without random oracles", in *Applied Cryptography and Network Security (ACNS'05)*, LNCS 3531, pp. 483-498, Springer-Verlag, June 2005.



XiaoMing Lu is currently a PhD candidate of the State Key Lab of Information Security, Institute of Software, Chinese Academy of Sciences. He received his B.S degree in Computer Science from Shandong University in 2000. His current research interests include public key cryptography and network security.

DengGuo Feng is now a professor and PhD supervisor in the Institute Of Software, Chinese Academy of Science. He is also the director of State Key Lab of Information Security, and the director of National Computer Network Intrusion Protection Center (NCNIPC). He received his PhD degree in 1995, with his degree paper as one of National Outstanding Degree Papers. He has already published

twenty influential books and more than two hundred scientific papers. He was elected into the CAS Hundred Talents Project in 1997. His current research interests include the theory and technology of information and network security, the theoretical and applied cryptography, and the cryptographic protocols analysis.