A Practical Identity-based Signcryption Scheme

Huiyan Chen[1], Yong Li[2], and Jinping Ren[3]
(Corresponding author: Huiyan Chen)
Beijing Electronic Science and Technology Institute[1],
Beijing 100070, P.R. China (Email:chenhy2003@gmail.com)
School of Electronics and Information Engineering, Beijing Jiaotong University[2],
Beijing 100044, P.R. China
State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences[3],
Beijing 100049, P.R. China
(Received Feb. 25, 2006; revised Mar. 28, 2006, and accepted May 28, 2007)

Abstract

In this paper, we construct a new identity-based signcryption scheme from bilinear pairings, which can process arbitrary length plaintexts. The scheme produces shorter ciphertext than the Libert-Quisquater signcryption scheme for the same plaintext and adapts to the bandwidth-constrained scenario very well. It is proved secure against adaptive chosen ciphertext and identity attack based on a variant of the Bilinear Diffie-Hellman problem in the random oracle model.

Keywords: identity-based cryptography, pairings, Signcryption

1 Introduction

The two fundamental primitives of public key cryptography are encryption and digital signature. Encryption provides confidentiality, and digital signature, provides authentication and non-repudiation. Often when we use one of these two security services, we would like to use also the other. In 1997, Zheng [22] proposed a novel cryptographic primitive which he called *signcryption*. The idea of this kind of primitive is to simultaneously perform both the functions of digital signature and encryption in a logically single step, and with a cost significantly lower than that required by traditional "signature then encryption" method. Several efficient signcryption schemes [19, 20, 23] have been proposed since 1997. Malone-Lee extended the signcryption idea to identity-based cryptography and firstly presented an identity-based signcryption scheme [14]. Indeed, the concept of identity-based cryptography was proposed in 1984 by Shamir [18]. The idea behind identity-based cryptography is that the user's public key can be derived from arbitrary string (e.g. e-mail address, IP address combined to a user name, etc.) which identifiers him in a non ambiguous way. This greatly reduces the problems of key management in the traditional public key infrastructure. Several practical identity-based schemes [3, 10, 12, 21] have been devised since 1984.

To date, several identity-based signcryption schemes have been proposed [2, 5, 8, 9, 13, 15, 17]. Unfortunately, except for schemes [9, 13], most identity-based signcryption schemes only operate on the *short size* plaintexts.

The main contribution of this paper is to propose a new identity-based signcryption scheme which can process *arbitrary length* messages. Comparing with schemes [9, 13], the new scheme produces shorter ciphertext for the same plaintext and adapts to the bandwidth-constrained scenario very well.

The rest of this paper is organized as follows: In Section 2, we review some preliminaries used throughout this paper. In Section 3, we analyze Libert and Quisquater's scheme [13]. The new scheme and its security results are given in Section 4. We compare our scheme with other schemes in Section 5. Section 6 concludes the paper.

2 Preliminaries

2.1 Notations

The following notations will be used throughout this paper.

$|q|$: the length of q in bit. If $|q| = 0$, q is denoted as ϕ.

Z^+: the set of natural numbers.

$\{0,1\}^*$: the space of finite binary strings.

$[m]^l$: the most significant l bits of m.

$[m]_l$: the least significant l bits of m.

$a||b$: the concatenation of strings a and b.

$[x]= y$: if $y \leq x < y + 1$ and $y \in Z^+$.

$a \oplus b$: the bitwise XOR of bit strings a and b.

$x \in_R G$: x is an element randomly selected from G.

$y \leftarrow \mathcal{A}(x)$: y is the output by $\mathcal{A}$ when it is run on input x. If $\mathcal{A}$ is deterministic, then y is unique; if $\mathcal{A}$ is probabilistic, then y is a random variable.

$y \leftarrow S$: y is chosen from S uniformly at random, if S is a finite set.

F_q: finite field, q is a prime number.

F_q^*: the largest multiplication group of F_q.

2.2 Bilinear Map and Complexity Assumptions

Let G_1 be a cyclic additive group generated by P, whose order is a prime q, and G_2 be a cyclic multiplicative group with the same order q. The bilinear map is given as $\widehat{e}: G_1 \times G_1 \rightarrow G_2$, which satisfies the following properties:

1) Bilinearity: $\widehat{e}(aP, bQ) = \widehat{e}(P, Q)^{ab}$ for all $P, Q \in G_1$, $a, b \in Z_q$. Here, $Z_q = \{0, 1, \ldots, q-1\}$, and $Z_q^* = Z_q \backslash \{0\}$.
2) Non-degeneracy: There exists $P, Q \in G_1$ such that $\widehat{e}(P, Q) \neq 1$.
3) Computability: There is an efficient algorithm to compute $\widehat{e}(P, Q)$ for all $P, Q \in G_1$.

We note that the Weil and Tate pairings associated with supersingular elliptic curves can be modified to create such bilinear maps.

Definition 1. *Let l be a security parameter. Given two groups G_1 and G_2 of the same prime order q ($|q|=l$), a bilinear map $\widehat{e}: G_1 \times G_1 \rightarrow G_2$ and a generator P of G_1, the Decisional Bilinear Diffie-Hellman Problem (DBDHP) in $(G_1, G_2, \widehat{e})$ is, given (P, aP, bP, cP, h) for unknown $a, b, c \in Z_q$, to decide whether $h = \widehat{e}(P, P)^{abc}$. The Modified Decisional Bilinear Diffie-Hellman Problem (MDBDHP) in $(G_1, G_2, \widehat{e})$ is, given $(P, aP, bP, cP, c^{-1}P, h)$ for unknown $a, b, c \in Z_q$, to decide whether $h = \widehat{e}(P, P)^{abc^{-1}}$.*

The advantage of a distinguisher $\mathcal{D}$ against MDBDHP is defined as $Adv_{\mathcal{D}}^{MDBDHP(G_1,G_2,P)}(l) = |Pr_{a,b,c \in_R Z_q}[1 \leftarrow \mathcal{D}(aP, bP, cP, c^{-1}P, \widehat{e}(P, P)^{abc^{-1}})] - Pr_{a,b,c \in_R Z_q, h \in_R G_2}[1 \leftarrow \mathcal{D}(aP, bP, cP, c^{-1}P, h)]|$.

Obviously, DBDHP is harder than MDBDHP. However, no known existing efficient algorithm can solve MDBDHP, to the best of our knowledge.

2.3 Framework of Identity-based Signcryption Scheme

Signcryption schemes are made of five algorithms: *Setup*, *Keygen*, *Signcrypt*, *Unsigncrypt* and *TPVerify* (if public verifiability is satisfied).

- *Setup*: Given a security parameter l, the private key generator (PKG) generates the system's public parameters *params*.
- *Keygen*: Given an identity ID, the PKG computes the corresponding private keys s_{ID}, d_{ID} and transmits them to their owner in a secure way.
- *Signcrypt*: To send m to Bob, Alice computes *Signcrypt*(m, s_{ID_A}, ID_B) to obtain the ciphertext σ.
- *Unsigncrypt*: When Bob receives σ, he computes *Unsigncrypt*(σ, ID_A, d_{ID_B}) and outputs the plaintext m and ephemeral data *temp* for public verifiability, or the symbol $\perp$ if σ was an invalid ciphertext between identities ID_A and ID_B.
- *TPVerify*: On input $(\sigma, ID_A, m, temp)$, it outputs $\top$ for true or $\perp$ for false, depending on whether σ is a valid ciphertext of message m signcrypted by ID_A or not.

For consistency, it requires that if σ=*Signcrypt*(m, s_{ID_A}, ID_B), then $(m, temp)$ = *Unsigncrypt*(σ, ID_A, d_{ID_B}) and $\top$=*TPverify*(σ, ID_A, m, *temp*).

2.4 Security Notions

Malone-Lee [14] extended notions of sematic security for public key encryption to identity-based signcryption schemes (IBSC). Sherman et al. slightly modified the definitions of these notions [9]. These modified notions are indistinguishable against adaptive chosen ciphertext and identity attacks (IND-IBSC-CCIA) and existential unforgery of identity based signcryption under adaptive chosen message and identity attacks (EUF-IBSC-ACMIA). Now we recall the following definitions.

Definition 2. *An identity-based signcryption scheme has the IND-IBSC-CCIA property if no adversary has a non-negligible advantage in the following game.*

1) *The challenger runs the* Setup *algorithm and sends the system parameters to the adversary.*
2) *The adversary $\mathcal{A}$ performs a polynomially bounded number of queries:*
   - Signcrypt *query: $\mathcal{A}$ produces two identities ID_A, ID_B and a plaintext m. The challenger computes* (s_{ID_A}, d_{ID_A}) = Keygen(ID_A) *and then* Signcrypt(m, s_{ID_A}, ID_B) *and sends the result to $\mathcal{A}$.*
   - Unsigncrypt *query: $\mathcal{A}$ produces two identities ID_A and ID_B, a ciphertext σ. The challenger generates the private key* (s_{ID_B}, d_{ID_B}) = Keygen(ID_B) *and sends the result of* Unsigncrypt(σ, d_{ID_B}, ID_A) *to $\mathcal{A}$ (this result can be the $\perp$ symbol if σ is an invalid ciphertext).*

- Keygen *query:* $\mathcal{A}$ *produces an identity* ID *and receives the extracted private key* (s_{ID}, d_{ID}) = Keygen(ID).
  $\mathcal{A}$ *can present its queries adaptively: every query may depend on the answer to the previous ones.*

3) $\mathcal{A}$ *chooses two plaintexts* $m_0, m_1(|m_0| = |m_1|)$ *and two identities* ID_A *and* ID_B *on which he wishes to be challenged. He cannot have asked the private key corresponding to* ID_B *in the first stage.*

4) The challenger randomly takes a bit $d \in \{0,1\}$ *and computes* σ=Signcrypt(m_d, s_{ID_A}, ID_B) *which is sent to* $\mathcal{A}$.

5) $\mathcal{A}$ *asks again a polynomially bounded number of queries just like in the first stage. This time, he cannot make a* Keygen *query on* ID_B *and he cannot ask the plaintext corresponding to* σ.

6) Finally, $\mathcal{A}$ *produces a bit* d' *and wins the game if* $d' = d$. *The adversary* $\mathcal{A}$*'s advantage is defined as* $Adv(\mathcal{A}) := |2Pr[d' = d] - 1|$.

Definition 3. *An identity-based signcryption scheme is said to have the EUF-IBSC-ACMIA property if no adversary has a non-negligeable advantage in the following game.*

1) The challenger runs the setup algorithm and gives the system parameters to the adversary $\mathcal{A}$.

2) The adversary $\mathcal{A}$ *performs a polynomially bounded number of queries just like in the previous Definition 2.*

3) Finally, $\mathcal{A}$ *produces a new triple* (σ^*, ID_A, ID_B) *(i.e. a triple that was not produced by the signcryption oracle), where the private key of* ID_A *was not asked in the first stage and wins the game if the result of* Unsigncrypt(σ, ID_A, d_{ID_B}) *is not the* $\perp$ *symbol.*

The adversary's advantage is its probability of winning the above game.

In this definition, to obtain the non-repudiation property and to prevent a dishonest recipient to send a ciphertext to himself on Alice's behalf and to try to convince a third party that Alice was the sender, it is necessary for the adversary to be allowed to make a *Keygen* query on the forged message's recipient ID_B.

3 Review of Libert-Quisquater Signcryption Scheme

The Libert-Quisquater signcryption scheme [13] is described as follows.

–*Setup*: Given security parameters l and n , the PKG chooses groups G_1 and G_2 of the same prime order q, a bilinear map $\widehat{e} : G_1 \times G_1 \to G_2$, a generator P of G_1, a secure symmetric cipher $(\mathcal{E}, \mathcal{D})$ and hash functions $H_1 : \{0,1\}^* \to G_1$, $H_2 : G_2 \to \{0,1\}^n$, $H_3 : \{0,1\}^* \times G_2 \to F_q$. It also choose a master-key $s \in F_q^*$ and computes P_{pub}=sP. The system's public parameters are

$$\mathcal{P} = (G_1, G_2, n, \widehat{e}, P, P_{pub}, H_1, H_2, H_3).$$

–*Keygen*: Given an identity ID, the PKG computes $Q_{ID} = H_1(ID)$ and the private key $d_{ID} = sQ_{ID}$.

–*Signcrypt*: To send a message m to Bob, Alice follows the steps below:

1) Compute Q_{ID_B}=$H_1(ID_B) \in G_1$.
2) Randomly choose $x \in F_q^*$, and compute $k_1 = \widehat{e}(P, P_{pub})^x$, k_2=$H_2(\widehat{e}(P_{pub}, Q_{ID_B})^x)$.
3) Compute $c = \mathcal{E}_{k_2}(m)$, $r = H_3(c, k_1)$, $S = xP_{pub} - rd_{ID_A} \in G_1$.

The ciphertext is $\sigma = (c, r, S)$.

–*Unsigncrypt*: When receiving $\sigma = (c, r, S)$, Bob performs the following tasks:

1) Compute Q_{ID_A}=$H_1(ID_A) \in G_1$.
2) Compute $k_1 = \widehat{e}(P, S)\widehat{e}(P_{pub}, Q_{ID_A})^r$.
3) Compute $\tau = \widehat{e}(S, Q_{ID_B})\widehat{e}(Q_{ID_A}, d_{ID_B})^r$, $k_2 = H_2(\tau)$.
4) Recover $m = \mathcal{D}_{k_2}(c)$ and accept σ if and only if $r = H_3(c, k_1)$.

Apparently, Libert-Quisquater signcryption scheme doesn't provide any forward security functionality. If the sender or the receiver's private key are compromised, the attacker can recover each of the issued messages by using the equality $\widehat{e}(Q_{ID_A}, d_{ID_B})$=$\widehat{e}(Q_{ID_B}, d_{ID_A})$.

Furthermore, if we replace σ with σ'=(xP, c, r, S) and also verify whether or not $\widehat{e}(xP, P_{pub})$=$\widehat{e}(P, S)$ $\widehat{e}(P_{pub}, Q_{ID_A})^r$ in *Unsigncrypt* algorithm, the Libert-Quisquater signcryption scheme above becomes an "encryption-then-sign"scheme and is the result of a combination of the simplified version of Boneh and Franklin's identity-based encryption scheme [18] with the following signature scheme:

–*Setup* and *Keygen* are the same as above.

–*Sign*: To sign a message m,

1) Choose $x \in F_q^*$, and compute $k_1 = \widehat{e}(P, P_{pub})^x$, and $r = H_3(m, k_1)$.
2) Compute $S = xP_{pub} - rd_{ID_A}$.

The signature on m is σ=(r, S).

–*Verify*: When receiving the signature $\sigma = (r, S)$ on m, Bob performs the following tasks:

1) Compute $k_1 = \widehat{e}(P,S)\widehat{e}(P_{pub}, Q_{ID_A})^r$.
2) Accept the signature σ if and only if $r = H_3(m, k_1)$.

This signature may be viewed as a variant of Hess's identity-based signature [12]. The ciphertext produced by the Libert-Quisquater signcryption scheme is only reduced by xP in comparison with the "encryption-then-sign"approach. In the next section, we will describe an identity-based signcryption scheme which produces shorter ciphertext than the Libert-Quisquater signcryption scheme for the same plaintext.

4 New Identity-based Signcryption Scheme

4.1 Description of the Scheme

Our identity-based signcryption scheme is based on the identity-based signature scheme [7]. It works as follows:

– *Setup*: Given security parameters l, $n \in Z^+$, PKG chooses two groups G_1 and G_2 (here G_2 is the subgroup of $F^*_{p^2}$, $F_{p^2}=\{t_1\xi + t_2 | t_1, t_2 \in Z_p$, p is a prime$\}$, $\xi(\neq 1)$ is a solution of $x^3 - 1 = 0$ in F_{p^2}) of prime order q (here, $l=|q|=l_1+l_2$, $l_1=[\frac{l+1}{2}]$, $l_2=[\frac{l}{2}]$), a bilinear map $\widehat{e} : G_1 \times G_1 \rightarrow G_2$, a generator P of G_1, a secure symmetric cipher $(\mathcal{E}, \mathcal{D})$ and cryptographic hash functions $H_1 : \{0,1\}^* \rightarrow G_1$, $H_2 : \{0,1\}^* \rightarrow Z^*_q$, $H_3 : G_2 \rightarrow \{0,1\}^n$, $F_1 : \{0,1\}^* \rightarrow \{0,1\}^{l_1}$, $F_2 : \{0,1\}^{l_1} \rightarrow \{0,1\}^{l_2}$. It also chooses a master-key $s \in Z^*_q (= Z_q \setminus \{0\})$, computes $P_{pub} = sP$ and $g = \widehat{e}(P, P_{pub})$. The system's public parameters are

$$\mathcal{P}=\{p, q, n, G_1, G_2, \widehat{e}, \mathcal{E}, \mathcal{D}, P, P_{pub}, g, H_1, H_2, H_3, F_1, F_2\}.$$

Remark 1. For any $t_1\xi + t_2 \in F_{q^2}$, let $(t_1\xi + t_2)_X = t_1$ and $(t_1\xi + t_2)_Y = t_2$.

– *Keygen*: Given identity ID, the PKG computes $Q_{ID} = H_1(ID)$ as the user's public key and sends $s_{ID} = sQ_{ID}$, $d_{ID} = s^{-1}Q_{ID}$ to the user as his/her private key.

– *Signcrypt*: To send a message m to Bob, Alice follows the steps below:

1) Compute $Q_{ID_B} = H_1(ID_B) \in G_1$.
2) Randomly choose $x \in Z^*_q$, compute $r_1 = (g^x)_X \ mod \ q$.
3) Compute $k = H_3(\widehat{e}(P, Q_{ID_B})^x)$.
4) Compute $c = c_1 || c_2 = \mathcal{E}_k(m)$, (here if $|c| = l_2$, $c_1 = \phi$, $c_2 = c$; if $|c| > l_2$, $c_1 = [c]^{|c|-l_2}$, $c_2 = [c]_{l_2}$).
5) Compute $f = F_1(c) || (F_2(F_1(c)) \oplus c_2)$.
6) Compute $r = r_1 \oplus f$ and $r_0 = H_2(r || c_1)$.
7) Compute $S = xP_{pub} - r_0 s_{ID_A}$.
8) The ciphertext is $\sigma = (c_1, r, S)$.

– *Unsigncrypt*: When receiving $\sigma = (c_1, r, S)$, Bob executes the following steps.

1) Compute $Q_{ID_A} = H_1(ID_A) \in G_1, r_0 = H_2(r || c_1)$.
2) Compute $r_1 = (\widehat{e}(P,S)\widehat{e}(P_{pub}, Q_{ID_A})^{r_0})_X \bmod q$.
3) Compute $\tau = \widehat{e}(S, d_{ID_B})\widehat{e}(Q_{ID_A}, Q_{ID_B})^{r_0}, k = H_3(\tau)$.
4) Compute $f = r_1 \oplus r$.
5) Compute $c_2 = [f]_{l_2} \oplus F_2([f]^{l_1})$, $m = \mathcal{D}_k(c_1 || c_2)$.
6) Accept σ if and only if $[f]^{l_1} = F_1(c_1 || c_2)$.

Remark 2. If $|\mathcal{E}_{(\cdot)}(m)| < l_2$, we need some redundancy to signcrypt message m. For example, we choose a cryptographic hash function $H : \{0,1\}^* \rightarrow \{0,1\}^{l_2}$ and set $c' = \mathcal{E}_{(\cdot)}(m) || H(\mathcal{E}_{(\cdot)}(m))$, then we sign message c'. Throughout this paper, we assume $|\mathcal{E}_{(\cdot)}(m)| \geq l_2$ if message m need to be signcrypted. If $|r_1| < l$, we pad $l - |r_1|$ zeros at the left of r_1.

4.2 Security Result

Theorem 1. *In the random oracle model, if there is an IND-IBSC-CCIA adversary $\mathcal{A}$ that succeeds with an advantage ϵ when running in a time t and asking at most q_{H_1} H_1 queries, at most q_E Keygen queries, at most q_R H_3 queries, q_R Signcrypt queries and q_U Unsigncrypt queries, then there is a distinguisher $\mathcal{B}$ that can solve the MDBDH problem in $t_1 = O(t + (4q_R^2 + 4q_U)T_{\widehat{e}} + (2q_R^2 + 2q_U)T_{ex})$ time with an advantage*

$$Adv_{\mathcal{B}}^{MDBDHP(G_1,G_2,P)}(l) > \frac{\epsilon(2^{[l/2]} - q_U) - q_U}{(q_{H_1})^2 2^{[l/2]+1}},$$

where $T_{\widehat{e}}$ denotes the computation time of the bilinear pairing, T_{ex} denotes the computation time of exponentiation in G_2.

Proof. See the appendix.

The existential unforgeability against adaptive chosen messages and identity attacks derives from the security of Chen et al.'s identity-based signature scheme [7]. By arguments similar to those in [11], one can show that an attacker that is able to forge a signcrypted message must be able to forge a signature for Chen et al.'s identity-based signature scheme.

5 Comparisons

Among these schemes [2, 5, 8, 9, 13, 14, 15, 17], only schemes [9, 13] use the more general symmetric cipher and seem to process messages of arbitrary length. So, in Table 1, we compare our scheme with schemes [9, 13] in

Table 1: Comparison of schemes

Schemes	Ciphertext Size		Efficiency					
	$\|c\|^*=l_2$	$\|c\|^*>l_2$	Signcrypt			Unsigncrypt		
		$(c_1 = [c]^{\|c\|-l_2})$	mls	exps	pcs	mls	exps	pcs
Libert-Quisquater[10]♣	$\|c\| + \|q\| + \|G_1\|$	$\|c\| + \|q\| + \|G_1\|$	1	2	$2^{\ddagger}$		2	$4^{\ddagger}$
Chow-Yiu-Hui-Chow[15]	$\|c\| + \|q\| + \|G_1\|$	$\|c\| + \|q\| + \|G_1\|$	1	2	$2^{\ddagger}$		2	$4^{\ddagger}$
Our scheme	$\|q\| + \|G_1\|$	$\|c_1\| + \|q\| + \|G_1\|$	1	2	$1^{\dagger}$		2	$4^{\ddagger}$

(∗) c is produced by encrypting plaintext m with symmetric cipher.
(†) One pairing is precomputable
(‡) Two pairings are precomputable
(♣) This scheme has no forward-secure property

terms of the length of the ciphertext which they produce and the number of the dominant operations required by them. In Table 1, we use mls, exps, and pcs as abbreviations for point multiplications in G_1, exponentiations in G_2 and pairing computations respectively. We denote all the ciphertexts, which are produced by encrypting the plaintext m with symmetric cipher in different and equal length keys and which are of equal length, as c for convenience, since we only consider the ciphertext length instead of the content of the ciphertext.

6 Conclusion

We proposed a new practical identity-based signcryption scheme. The scheme produces shorter ciphertext than schemes [9, 13] for the same plaintext. It has the IND-IBSC-CCIA property based on MDBDHP in the random oracle model.

References

[1] M. Abe and T. Okamoto, "A signature scheme with message recovery as secure as discrete logarithm," *Proceedings of Asiacrypt 1999,* LNCS 1716, pp. 378-389, Springer-Verlag, 1999.

[2] P. S. L. M. Barreto, B. Libert, N. McCullagh, and J.-J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," *Proceedings of Asiacrypt 2005,* LNCS 3788, pp. 515-532, Springer-Verlag, 2005.

[3] D. Boneh and M. Franklin, "Identity-based encryption from the Weil Pairing," *Proceedings of Crypto'01,* LNCS 2139, pp. 213-229, Springer-Verlag, 2001.

[4] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil Pairing," *Proceedings of Asiacrypt 2001,* LNCS 2248, pp. 514-532, Springer-Verlag, 2001.

[5] X. Boyen, "Multipurpose identity-based Signcryption: A swiss army knife for identity-based cryptography," *Proceedings of Crypto'2003,* LNCS 2729, pp. 383-399, Springer-Verlag, 2003.

[6] J. C. Cha and J. H. Cheon, "An identity-based signature from Gap Diffie-Hellman groups," *Proceedings of PKC'03,* LNCS 2567, pp. 18-30, Springer-Verlag, 2003.

[7] H. Chen, S. Lü and Z. Liu, "Identity-based signature scheme with partial message recovery," *Chinese Journal of Computers,* Vol. 29, no. 9, pp. 1622-1627, 2006.

[8] L. Chen and J. Malone-Lee, "*Improved Identity-Based Signcryption,"* Cryptology ePrint Archive, Report 2004/114, 2004.

[9] S. S.M. Chow, S.M. Yiu, L. C.K. Hui, and K.P. Chow, "Efficient forward and provably secure ID-based signcryption scheme with public verifiability and public ciphertext authenticity," *Proceedings of ICISC 2003,* LNCS 2971, pp. 352-369. Springer-Verlag, 2004.

[10] A. Fiat and A. Shamir, "How to Prove Yourself: Practical solutions to identification and signature problems," *Proceedings of Crypto'86,* LNCS 0263, pp. 186-194, Springer-Verlag, 1986.

[11] G. Gamage, J. Leiwo, and Y. Zheng, "Encrypted message authentication by firewalls," *Proceedings of PKC'99,* LNCS 1560, pp. 69-81, Springer-Verlag, 1999.

[12] F. Hess, "Efficient identity-based signature schemes based on pairings," *Proceedings of SAC 2002,* LNCS 2595, pp. 310-324, Springer-Verlag, 2002.

[13] B. Libert and J.-J. Quisquater, "New identity-based signcryption schemes based on pairings," *IEEE Information Theory Workshop,* Paris, France, 2003.

[14] J. Malone-Lee, "*Identity-Based Signcryption,"* Cryptology ePrint Archive, Report 2002/098, 2002.

[15] D. Nalla and K. C. Reddy, "*Signcryption Scheme For Identity-based Cryptosystems,*" Cryptology ePrint Archive, Report 2003/066, 2003.

[16] K. Ohta and T. Okamoto, "On the concrete security treatment of signatures derived from identification," *Proceedings of Crypto'98,* LNCS 1462, pp. 354-370, Springer-Verlag, 1998.

[17] R. Sakai and M. Kasahara, "Id-based cryptosystems with pairing on elliptic curve," *Proceedings of Symposium on Cryptography and Information Security (SCIS'2003)*, 2003.

[18] A. Shamir, "Identity-based cryptosystems and signature schemes," *Proceedings of Crypto'84,* LNCS 0196, pp. 47-53, Springer-Verlag, 1984.
[19] R. Steinfeld and Y. Zheng, "A signcryption scheme based on integer factorization" *Proceedings of ISW'00,* pp. 308-322, 2000.
[20] B.H. Yum and P.J. Lee, "New signcryption schemes based on KCDSA" *Proceedings of ICISC'01,* LNCS 2288, pp. 305-317, Springer-Verlag, 2001.
[21] F. Zhang, S. Liu, and K. Kim, "*ID-Based One Round Authenticated Tripartite Key Agreement Protocol,"* Cryptology ePrint Archive, Report 2002/122, 2002.
[22] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption)$\ll$ cost (signature)+ cost (encryption)," *Proceedings of Crypto'97,* LNCS 1294, pp.165-179, Springer-Verlag, 1997.
[23] Y. Zheng, "Signcryption and its applications in efficient public key solutions," *Proceedings of ISW'97,* pp. 291-312, 1998.

Huiyan Chen received his M.S. degree in Mathematics from Sichuan University in 1995, and the PhD degree from State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences in 2007. His research interests include cryptography, information security, and Ad Hoc Network.

Yong Li received his M.S. degree in Computer Science from Wuhan University in 2003, and the PhD degree from State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences in 2007. His research interests include cryptographic protocols and information security.

Jinping Ren received her PhD degree from State Key Laboratory of Information Security, Graduate University of Chinese Academy of Sciences in 2007. Her research interests include cryptography and information security.