An Identity-Based Signcryption Scheme for Multi-domain Ad Hoc Networks

Fagen Li[1,2], Yupu Hu[1], and Chuanrong Zhang[1,3]

[1] Key Laboratory of Computer Networks and Information Security,
Xidian University, Xi'an 710071, China
[2] School of Computer Science and Engineering,
University of Electronic Science and Technology of China, Chengdu 610054, China
[3] Telecommunication Engineering Institute,
Air Force Engineering University, Xi'an 710077, China
fagenli@mail.xidian.edu.cn

Abstract. As various applications of wireless ad hoc networks have been proposed, security has become one of the big research challenges and is receiving increasing attention. Recently, Several security schemes for wireless ad hoc networks have been proposed using identity-based signcryption schemes. However, almost all identity-based signcryption schemes that have been proposed until now are based on a single private key generator, which is not suitable for multi-domain ad hoc networks. In this paper, we propose a new identity-based signcryption scheme based on multiple private key generators, which is more suitable for multi-domain ad hoc networks. We prove its semantical security under the Decisional Bilinear Diffie-Hellman assumption in the random oracle model.

Keywords: Ad hoc networks, identity-based signcryption, bilinear pairings, provable security.

1 Introduction

An ad hoc network is a collection of autonomous nodes that communicate with each other by forming a multi-hop wireless network. The property of not relying on the support from any fixed infrastructure makes it useful for a wide range of applications, such as instant consultation between mobile users in the battlefields, emergency, and disaster situations, where geographical or terrestrial constraints demand totally distributed networks. While ad hoc network provides a great flexibility for establishing communications, it also brings a lot of research challenges. One of the important issues is the security due to all the characteristics of these networks, such as the vulnerability of the wireless links, the limited physical protection of each node and the dynamically changing topology. Recently, Several security schemes for ad hoc networks have been proposed using identity-based (ID-based) signcryption schemes, such as key management scheme [18], authenticated broadcasting scheme [5], and routing protocols

J. Katz and M. Yung (Eds.): ACNS 2007, LNCS 4521, pp. 373–384, 2007.

TIDS [11], ISSRP [23] and ISMANET [24]. The using of ID-based signcryption has the following advantages:

1. There is no need to authenticate a public key because of using the ID-based cryptography.
2. Confidentiality, integrity, non-repudiation and authentication are provided simultaneously because of using the signcryption technique.
3. Computational costs and communication overheads can be reduced.

However, almost all ID-based signcryption schemes that have been proposed until now are based on a single private key generator (PKG), which is not suitable for multi-domain ad hoc networks [15] formed by a consortium of different organizations. It is unrealistic to assume that different organizations use a single PKG. Therefore, it is necessary to find an ID-based signcryption scheme based on multiple PKGs.

1.1 Related Work

ID-based cryptography was introduced by Shamir in 1984 [26]. The distinguishing property of ID-based cryptography is that a user's public key can be any binary string, such as an email address that can identify the user. This removes the need for senders to look up the recipient's public key before sending out an encrypted message. Usually, private keys of users' are issued by a trusted authority called the PKG. ID-based cryptography is supposed to provide a more convenient alternative to conventional public key infrastructure. In 2001, Boneh and Franklin [6] proposed the first practical ID-based encryption scheme using pairings on elliptic curves. Since then, most researches on ID-based cryptography are based on this system.

Confidentiality, integrity, non-repudiation and authentication are the important requirements for many cryptographic applications. A traditional approach to achieve these requirements is to sign-then-encrypt the message. Signcryption, first proposed by Zheng in 1997 [28], is a cryptographic primitive that performs digital signature and public key encryption simultaneously, at lower computational costs and communication overheads than the signature-then-encryption approach. Several efficient signcryption schemes have been proposed since 1997 [3,29,12,25,22,14,27,21] and a first example of formal security proof in a formal security model was published in 2002 [2]. However, until 2002, none of these schemes were ID-based. Malone-Lee [20] proposed a first method to achieve an ID-based signcryption solution. Libert and Quisquater [19] pointed out that Malone-Lee's scheme [20] is not semantically secure because the signature of the message is visible in the signcrypted message. Chow et al. [10] designed an ID-based signcryption scheme that provides both public verifiability and forward security. Boyen [7] presented an ID-based signcryption scheme that provides not only public verifiability and forward security but also ciphertext unlinkability and anonymity. In [9], Chen and Malone-Lee improved Boyen's scheme [7] in efficiency. In [4], Barreto et al. constructed the most efficient ID-based signcryption scheme to date.

1.2 Our Contribution

In this paper, we present an ID-based signcryption scheme based on multiple PKGs. We prove its semantical security under the Decisional Bilinear Diffie-Hellman assumption in the random oracle model. We believe that our scheme is more suitable for multi-domain ad hoc networks than previously proposed schemes.

1.3 Organization

The rest of this paper is organized as follows. Some preliminary works are given in Section 2. The formal model of ID-based signcryption is described in Section 3. The proposed ID-based signcryption scheme is given in Section 4. We analyze the proposed scheme in Section 5. Finally, the conclusions are given in Section 6.

2 Preliminaries

In this section, we briefly describe the basic definition and properties of the bilinear pairings.

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 of the same order q. A bilinear pairing is a map $\hat{e} : G_1 \times G_1 \rightarrow G_2$ with the following properties:

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

The modified Weil pairing and the Tate pairing [6] are admissible maps of this kind. The security of our scheme described here relies on the hardness of the following problems.

Definition 1. *Given two groups G_1 and G_2 of the same prime order q, a bilinear map $\hat{e} : G_1 \times G_1 \rightarrow G_2$ and a generator P of G_1, the Decisional Bilinear Diffie-Hellman problem (DBDHP) in $(G_1, G_2, \hat{e})$ is to decide whether $h = \hat{e}(P, P)^{abc}$ given (P, aP, bP, cP) and an element $h \in G_2$. We define the advantage of a distinguisher against the DBDHP like this*

$$Adv(D) = |P_{a,b,c,\in_R Z_q, h\in_R G_2}[1 \leftarrow D(aP, bP, cP, h)] - P_{a,b,c,\in_R Z_q}[1 \leftarrow D(aP, bP, cP, \hat{e}(P, P)^{abc})]|.$$

Definition 2. *Given two groups G_1 and G_2 of the same prime order q, a bilinear map $\hat{e} : G_1 \times G_1 \rightarrow G_2$ and a generator P of G_1, the Computational Bilinear Diffie-Hellman problem (CBDHP) in $(G_1, G_2, \hat{e})$ is to compute $h = \hat{e}(P, P)^{abc}$ given (P, aP, bP, cP).*

The decisional problem is of course not harder than the computational one. However, no algorithm is known to be able to solve any of them so far.

3 Formal Model of ID-Based Signcryption

3.1 Generic Scheme

A generic ID-based signcryption scheme based on multiple PKGs consists of the following five algorithms. We suppose that there are two trusted authorities, say PKG_1 and PKG_2.

Setup1: Given a security parameter k, this algorithm generates the system's public parameters *params*.

Setup2: Given the system's public parameters *params*, the PKG_1 generates a master secret key s_1 and a corresponding public key P^1_{pub}. Similarly, The PKG_2 generates a master secret key s_2 and a corresponding public key P^2_{pub}.

Extract: Given an identity ID in $\mathrm{PKG}_l (l = 1, 2)$, the PKG_l computes the corresponding private key S_{ID} and transmits it to its owner in a secure way.

Signcrypt: To send a message m to Bob, Alice obtains the ciphertext σ by computing $\mathbf{Signcrypt}(m, S_{ID_A}, ID_B)$.

Unsigncrypt: When Bob receives σ, he computes $\mathbf{Unsigncrypt}(\sigma, ID_A, S_{ID_B})$ and obtains the plaintext m or the symbol $\perp$ if σ is an invalid ciphertext between identities ID_A and ID_B.

For consistency, we of course require that if $\sigma = \mathbf{Signcrypt}(m, S_{ID_A}, ID_B)$, then we have $m = \mathbf{Unsigncrypt}(\sigma, ID_A, S_{ID_B})$.

3.2 Security Notions

Malone-Lee [20] defines the security notions for ID-based signcryption schemes. These notions are indistinguishability against adaptive chosen ciphertext attacks and unforgeability against adaptive chosen messages attacks. We modify his definitions slightly to adapt for our ID-based signcryption scheme based on multiple PKGs.

Definition 3 (Confidentiality). *An ID-based signcryption scheme based on multiple PKGs (IDSCMP) is said to have the indistinguishability against adaptive chosen ciphertext attacks property (IND-IDSCMP-CCA2) if no polynomially bounded adversary has a non-negligible advantage in the following game.*

1. *The challenger $\mathcal{C}$ runs the* **Setup1** *and* **Setup2** *algorithms with a security parameter k and sends the system parameters to the adversary $\mathcal{A}$.*
2. *$\mathcal{A}$ performs a polynomially bounded number of queries (these queries may be made adaptively, i.e. each query may depend on the answer to the previous queries).*
   - *Key extraction queries: $\mathcal{A}$ chooses an identity ID in $PKG_l (l = 1, 2)$. $\mathcal{C}$ computes $S_{ID} = \mathbf{Extract}(ID)$ and sends S_{ID} to $\mathcal{A}$.*
   - *Signcryption queries: $\mathcal{A}$ produces two identities ID_i, ID_j and a plaintext m. $\mathcal{C}$ computes $S_{ID_i} = \mathbf{Extract}(ID_i)$ and $\sigma = \mathbf{Signcrypt}(m, S_{ID_i}, ID_j)$ and sends σ to $\mathcal{A}$.*

- *Unsigncryption queries:* $\mathcal{A}$ *produces two identities* ID_i *and* ID_j*, and a ciphertext* σ*.* $\mathcal{C}$ *generates the private key* $S_{ID_j} = \mathbf{Extract}(ID_j)$ *and sends the result of* $\mathbf{Unsigncrypt}(\sigma, ID_i, S_{ID_j})$ *to* $\mathcal{A}$ *(this result can be the* $\perp$ *symbol if* σ *is an invalid ciphertext).*

3. $\mathcal{A}$ *generates two equal length plaintexts* m_0, m_1 *and two identities* ID_A *and* ID_B *on which he wants to be challenged. He cannot have asked the private key corresponding to* ID_B *in the first stage.*
4. $\mathcal{C}$ *takes a bit* $b \in_R \{0,1\}$ *and computes* $\sigma = \mathbf{Signcrypt}(m_b, S_{ID_A}, ID_B)$ *which is sent to* $\mathcal{A}$*.*
5. $\mathcal{A}$ *can ask a polynomially bounded number of queries adaptively again as in the first stage. This time, he cannot make a key extraction query on* ID_B *and cannot make an unsigncryption query on* σ *to obtain the corresponding plaintext.*
6. *Finally,* $\mathcal{A}$ *produces a bit* b' *and wins the game if* $b' = b$*.*

The advantage of $\mathcal{A}$ *is defined as* $Adv(\mathcal{A}) = |2P[b' = b] - 1|$*, where* $P[b' = b]$ *denotes the probability that* $b' = b$*.*

Notice that the adversary is allowed to make a key extraction query on identity ID_A in the above definition. This condition corresponds to the stringent requirement of insider security for confidentiality of signcryption [1]. On the other hand, it ensures the forward security of the scheme, i.e. confidentiality is preserved in case the sender's private key becomes compromised.

Definition 4 (Unforgeability). *An ID-based signcryption scheme based on multiple PKGs (IDSCMP) is said to have the existential unforgeability against adaptive chosen messages attacks (EUF-IDSCMP-CMA) if no polynomially bounded adversary has a non-negligible advantage in the following game.*

1. *The challenger* $\mathcal{C}$ *runs the* **Setup1** *and* **Setup2** *algorithms with a security parameter* k *and sends the system parameters to* $\mathcal{A}$*.*
2. $\mathcal{A}$ *performs a polynomially bounded number of queries just like in the Definition 3.*
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 second stage.* $\mathcal{A}$ *wins the game if the result of* $\mathbf{Unsigncrypt}(\sigma, ID_A, S_{ID_B})$ *is not the* $\perp$ *symbol.*

The advantage of $\mathcal{A}$ *is defined as the probability that it wins.*

Note that the adversary is allowed to make a key extraction query on the identity ID_B in the above definition. Again, this condition corresponds to the stringent requirement of insider security for signcryption [1].

4 An ID-Based Signcryption Scheme for Multiple PKGs

In this section, we look at signcryption between members of separate domains. This idea was first suggested in an authenticated key agreement protocol [8].

We present an ID-based signcryption scheme for multiple PKGs, which is more suitable for multi-domain ad hoc networks than previously proposed schemes. The following shows the details of our scheme.

Setup1: Define G_1, G_2 and $\hat{e}$ as in previous section. Let H_1, H_2 and H_3 be three cryptographic hash functions where $H_1 : \{0,1\}^* \rightarrow G_1$, $H_2 : G_2 \rightarrow \{0,1\}^n$ and $H_3 : \{0,1\}^* \rightarrow Z_q^*$. Let P be a generator of G_1. Note that the system's public parameters $\{G_1, G_2, n, \hat{e}, P, H_1, H_2, H_3\}$ are globally agreed, e.g., recommended by an international standards body.

Setup2: The PKG_1 chooses a master secret key $s_1 \in_R Z_q^*$ and computes $P_{pub}^1 = s_1 P$. The PKG_1 publishes P_{pub}^1 and keeps the master secret key s_1 secret. Similarly, the PKG_2 chooses a master secret key $s_2 \in_R Z_q^*$ and computes $P_{pub}^2 = s_2 P$. The PKG_2 publishes P_{pub}^2 and keeps the master secret key s_2 secret.

Extract: Suppose that Alice registers with PKG_1 and gets her private key $S_{ID_A} = s_1 Q_{ID_A}$, where $Q_{ID_A} = H_1(ID_A)$, and Bob registers with PKG_2 and gets his private key $S_{ID_B} = s_2 Q_{ID_B}$, where $Q_{ID_B} = H_1(ID_B)$.

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

1. Choose $x \in_R Z_q^*$ and compute $U = xP$.
2. Compute $\tau = \hat{e}(P_{pub}^2, Q_{ID_B})^x$.
3. Compute $k = H_2(\tau)$.
4. Compute $c = m \oplus k$.
5. Compute $r = H_3(m, U, k)$.
6. Compute $V = xP_{pub}^1 + rS_{ID_A}$.

The ciphertext is $\sigma = (c, U, V)$.

Unsigncrypt: When receiving $\sigma = (c, U, V)$, Bob follows the steps below.

1. Compute $\tau = \hat{e}(U, S_{ID_B})$.
2. Compute $k = H_2(\tau)$.
3. Recover $m = c \oplus k$.
4. Compute $r = H_3(m, U, k)$.
5. Accept the message if and only if the following equation holds:

$$\hat{e}(P, V) = \hat{e}(U, P_{pub}^1)\hat{e}(P_{pub}^1, Q_{ID_A})^r.$$

Note that we accept the assumption in [8] that the two PKGs share common system parameters and differ in the master secret key. Of course, our scheme can use different system parameters by using the method in [16,17].

5 Analysis of the Scheme

5.1 Correctness

The correctness can be easily verified by the following equations.

$$\hat{e}(U, S_{ID_B}) = \hat{e}(xP, s_2 Q_{ID_B}) = \hat{e}(xs_2 P, Q_{ID_B}) = \hat{e}(P_{pub}^2, Q_{ID_B})^x$$

and

$$\begin{aligned}\hat{e}(P,V) &= \hat{e}(P, xP^1_{pub} + rS_{ID_A}) = \hat{e}(P, xP^1_{pub})\hat{e}(P, rs_1 Q_{ID_A}) \\ &= \hat{e}(xP, P^1_{pub})\hat{e}(s_1 P, Q_{ID_A})^r \\ &= \hat{e}(U, P^1_{pub})\hat{e}(P^1_{pub}, Q_{ID_A})^r\end{aligned}$$

5.2 Security

Theorem 1 (Confidentiality). *In the random oracle model, we assume we have an IND-IDSCMP-CCA2 adversary called $\mathcal{A}$ that is able to distinguish ciphertext during the game of Definition 3 with an advantage ϵ when running in a time t and asking at most q_{H_1} identity hashing queries, at most q_{H_2} H_2 queries, at most q_{H_3} H_3 queries, at most q_K key extraction queries, q_S signcryption queries and q_U unsigncryption queries. Then, there exists a distinguisher $\mathcal{C}$ that can solve the Decisional Bilinear Diffie-Hellman problem in a time $O(t + (q_{H_3} q_S + q_S^2 + 4q_U)T_{\hat{e}})$ with an advantage*

$$Adv(\mathcal{C})^{DBDH(G_1,P)} > \frac{\epsilon(2^k - q_U) - q_U}{q_{H_1} 2^{k+1}},$$

where $T_{\hat{e}}$ denotes the computation time of the bilinear map.

Proof. We assume the distinguisher $\mathcal{C}$ receives a random instance (P, aP, bP, cP, h) of the Decisional Bilinear Diffie-Hellman problem. His goal is to decide whether $h = \hat{e}(P,P)^{abc}$ or not. $\mathcal{C}$ will run $\mathcal{A}$ as a subroutine and act as $\mathcal{A}$'s challenger in the IND-IDSCMP-CCA2 game. During the game, $\mathcal{A}$ will consult $\mathcal{C}$ for answers to the random oracles H_1, H_2 and H_3. Roughly speaking, these answers are randomly generated, but to maintain the consistency and to avoid collision, $\mathcal{C}$ keeps three lists L_1, L_2, L_3 respectively to store the answers. The following assumptions are made.

1. $\mathcal{A}$ will ask for $H_1(ID)$ before ID is used in any key extraction query, signcryption query and unsigncryption query.
2. Ciphertext returned from a signcryption query will not be used by $\mathcal{A}$ in an unsigncryption query.

At the beginning of the game, $\mathcal{C}$ gives $\mathcal{A}$ the system parameters with $P^2_{pub} = cP$ and $P^1_{pub} = dP$, where $d \in_R Z_q^*$. Note that c and d are unknown to $\mathcal{C}$. This value simulates the master secret key value for the PKG_2 and PKG_1 in the game. Then, $\mathcal{C}$ chooses a random number $j \in \{1, 2, \ldots, q_{H_1}\}$. $\mathcal{A}$ asks a polynomially bounded number of H_1 queries on identities of his choice. At the j-th H_1 query, $\mathcal{C}$ answers by $H_1(ID_j) = bP$ (We suppose that the identity ID_j belongs to PKG_2, otherwise we exchange P^2_{pub} for P^1_{pub}). For queries $H_1(ID_e)$ with $e \neq j$, $\mathcal{C}$ chooses $b_e \in_R Z_q^*$, puts the pair (ID_e, b_e) in list L_1 and answers $H_1(ID_e) = b_e P$.

We now explain how the other kinds of queries are treated by $\mathcal{C}$.

- H_2 queries: On a $H_2(\tau_e)$ query, $\mathcal{C}$ searches a pair (τ_e, k_e) in the list L_2. If such a pair is found, $\mathcal{C}$ answers k_e, otherwise he answers $\mathcal{A}$ by a random binary sequence $k \in_R \{0,1\}^n$ such that no entry $(\cdot, k)$ exists in L_2 (in order to avoid collisions on H_2) and puts the pair (τ_e, k) into L_2.
- H_3 queries: On a $H_3(m_e, U_e, k_e)$ query, $\mathcal{C}$ checks if there exists (m_e, U_e, k_e, r_e) in L_3. If such a tuple is found, $\mathcal{C}$ answers r_e, otherwise he chooses $r \in_R Z_q^*$, gives it as an answer to the query and puts the tuple (m_e, U_e, k_e, r) into L_3.
- Key extraction queries: When $\mathcal{A}$ asks a question $\mathbf{Extract}(ID_e)$, if $ID_e = ID_j$, then $\mathcal{C}$ fails and stops. If $ID_e \neq ID_j$, then the list L_1 must contain a pair (ID_e, b_e) for some b_e (this indicates $\mathcal{C}$ previously answered $H_1(ID_e) = b_e P$ on a H_1 query on ID_e). The private key corresponding to ID_e is then $b_e P_{pub}^2 = c b_e P$ or $b_e P_{pub}^1 = d b_e P$. It is computed by $\mathcal{C}$ and returned to $\mathcal{A}$.
- Signcryption queries: At any time, $\mathcal{A}$ can perform a signcryption query for a plaintext m and identities ID_A and ID_B. We have the following three cases to consider.
  - Case 1: $ID_A \neq ID_j$. $\mathcal{C}$ computes the private key S_{ID_A} corresponding to ID_A by running the key extraction query algorithm. Then $\mathcal{C}$ answers the query by a call to $\mathbf{Signcrypt}(m, S_{ID_A}, Q_{ID_B})$.
  - Case 2: $ID_A = ID_j$ and $ID_B \neq ID_j$. $\mathcal{C}$ chooses $x, r \in_R Z_q^*$ and computes $U = xP - rQ_{ID_A}$, $V = xP_{pub}^1$, and $\tau = \hat{e}(U, S_{ID_B})$($\mathcal{C}$ could obtain S_{ID_B} from the key extraction algorithm because $ID_B \neq ID_j$). $\mathcal{C}$ runs the H_2 simulation algorithm to find $k = H_2(\tau)$ and computes $c = m \oplus k$. $\mathcal{C}$ then checks if L_3 already contains a tuple (m, U, k, r') with $r' \neq r$. In this case, $\mathcal{C}$ repeats the process with another random pair (x, r) until finding a tuple (m, U, k, r) whose first three elements do not appear in a tuple of the list L_3. This process repeats at most $q_{H_3} + q_S$ times as L_3 contains at most $q_{H_3} + q_S$ entries ($\mathcal{A}$ can issue q_{H_3} H_3 queries and q_S signcryption queries, while each signcryption query contains a single H_3 query). When an appropriate pair (x, r) is found, the ciphertext (c, U, V) appears to be valid from $\mathcal{A}$'s viewpoint. $\mathcal{C}$ has to compute one pairing operation for each iteration of the process.
  - Case 3: $ID_A = ID_j$ and $ID_B = ID_j$. $\mathcal{C}$ chooses $x^*, r^* \in_R Z_q^*$, computes $U^* = x^* P - r^* Q_{ID_A}$, $V^* = x^* P_{pub}^1$, and chooses $\tau^* \in_R G_2$ and $k^* \in_R \{0,1\}^n$ such that no entry $(\cdot, k^*)$ is in L_2 and computes $c^* = m \oplus k^*$. $\mathcal{C}$ then checks if L_3 already contains a tuple (m, U^*, k^*, r') with $r' \neq r^*$. If not, $\mathcal{C}$ puts the tuple (m, U^*, k^*, r^*) into L_3 and (τ^*, k^*) into L_2. Otherwise, $\mathcal{C}$ chooses another random pair (x^*, r^*) and repeats the process as above until he finds a tuple (m, U^*, k^*, r^*) whose first three elements do not appear in an entry of L_3. Once an appropriate pair (x^*, r^*) is found, $\mathcal{C}$ gives the ciphertext $\sigma^* = (c^*, U^*, V^*)$ to $\mathcal{A}$. As $\mathcal{A}$ will not ask for the unsigncryption of σ^*, he will never see that σ^* is not a valid ciphertext of the plaintext m for identities ID_A and ID_B.

– Unsigncryption queries: For a unsigncryption query on a ciphertext $\sigma' = (c', U', V')$ for identities ID_A and ID_B. We have the following two cases to consider.
  - Case 1: $ID_B = ID_j$. $\mathcal{C}$ always answers $\mathcal{A}$ that σ' is invalid.
  - Case 2: $ID_B \neq ID_j$. $\mathcal{C}$ computes $\tau' = \hat{e}(U', S_{ID_B})$ ($\mathcal{C}$ could obtain S_{ID_B} from the key extraction algorithm because $ID_B \neq ID_j$). $\mathcal{C}$ then runs the H_2 simulation algorithm to obtain $k' = H_2(\tau')$ and computes $m' = c' \oplus k'$. Finally, $\mathcal{C}$ runs the H_3 simulation algorithm to obtain $r' = H_3(m', U', k')$ and checks if $\hat{e}(P, V') = \hat{e}(U', P^1_{pub})\hat{e}(P^1_{pub}, Q_{ID_A})^{r'}$ holds. If the above equation does not hold, $\mathcal{C}$ rejects the ciphertext. Otherwise $\mathcal{C}$ returns m'.

  It is easy to see that, for all queries, the probability to reject a valid ciphertext does not exceed $q_U/2^k$.

After the first stage, $\mathcal{A}$ picks a pair of identities on which he wishes to be challenged. Note that $\mathcal{C}$ fails if $\mathcal{A}$ has asked a key extraction query on ID_j during the first stage. We know that the probability for $\mathcal{C}$ not to fail in this stage is $\frac{q_{H_1}-q_K}{q_{H_1}}$. Further, with a probability exactly$\frac{1}{q_{H_1}-q_K}$, $\mathcal{A}$ chooses to be challenged on the pair (ID_i, ID_j) with $i \neq j$. Hence the probability that $\mathcal{A}$'s response is helpful to $\mathcal{C}$ is $\frac{1}{q_{H_1}}$. Note that if $\mathcal{A}$ has submitted a key extraction query on ID_j, then $\mathcal{C}$ fails because he is unable to answer the question. On the other hand, if $\mathcal{A}$ does not choose (ID_i, ID_j) as target identities, $\mathcal{C}$ fails too.

Then $\mathcal{A}$ outputs two plaintexts m_0 and m_1. $\mathcal{C}$ chooses $b \in_R \{0, 1\}$ and signcrypts m_b. To do so, he sets $U^* = aP$, obtains $k^* = H_2(h)$(where h is $\mathcal{C}$ candidate for the DBDH problem) from the H_2 simulation algorithm, and computes $c_b = m \oplus k^*$. Then $\mathcal{C}$ chooses $V^* \in_R G_1$ and sends the ciphertext $\sigma^* = (c_b, U^*, V^*)$ to $\mathcal{A}$.

$\mathcal{A}$ then performs a second series of queries which is treated in the same way as the first one. At the end of the simulation, he produces a bit b' for which he believes the relation $\sigma^* = \mathbf{Signcrypt}(m_{b'}, S_{ID_i}, ID_j)$ holds. At this moment, if $b = b'$, $\mathcal{C}$ outputs $h = \hat{e}(U^*, S_{ID_j}) = \hat{e}(aP, cbP) = \hat{e}(P, P)^{abc}$ as a solution of the DBDH problem, otherwise $\mathcal{C}$ stops and outputs "failure".

Taking into account all the probabilities that $\mathcal{C}$ will not fail its simulation, the probability that $\mathcal{A}$ chooses to be challenged on the pair (ID_i, ID_j), and also the probability that $\mathcal{A}$ wins the IND-IDSCMP-CCA2 game, the value of $Adv(\mathcal{C})$ is calculated as follows.

$$\begin{aligned} Adv(\mathcal{C}) &= (\frac{(\epsilon+1)}{2}(1-\frac{q_U}{2^k}) - \frac{1}{2})(\frac{1}{q_{H_1}}) \\ &= \frac{\epsilon(2^k - q_U) - q_U}{q_{H_1} 2^{k+1}} \end{aligned}$$

The bound on $\mathcal{C}$'s computation time derives from the fact that every signcryption query requires at most $q_{H_3} + q_S$ pairing operations and every unsigncryption query requires at most 4 pairing operations. □

Theorem 2 (Unforgeability). *The proposed scheme is secure in the sense of unforgeability.*

Proof. The unforgeability against adaptive chosen messages attacks derives from the security of Hess's ID-based signature scheme [13] under the Computational Diffie-Hellman assumption. One can show that an attacker that is able to forge a signcrypted message must be able to forge a signature for the following scheme which is a variant of Hess's signature.

Setup and **Extract** are the same as above. The others are described as follows.

Sign: To sign a message m, the signer follows the steps below.

1. Choose $x \in_R Z_q^*$ and compute $U = xP$.
2. Compute $r = H_3(m, U)$.
3. Compute $V = xP_{pub}^1 + rS_{ID_A}$.

The signature on message m is $\sigma = (U, V)$.

Verify: When receiving $\sigma = (U, V)$, the verifier follows the steps below.

1. Compute $r = H_3(m, U)$.
2. Accept the signature if and only if the following equation holds:

$$\hat{e}(P, V) = \hat{e}(U, P_{pub}^1)\hat{e}(P_{pub}^1, Q_{ID_A})^r.$$

□

Theorem 3 (Public verifiability). *The proposed scheme provides the public verifiability.*

Proof. When necessary, Bob may forward (m, U, V) to others, who can be convinced that it came originally from Alice by computing $r = H_3(m, U)$ and verifying

$$\hat{e}(P, V) = \hat{e}(U, P_{pub}^1)\hat{e}(P_{pub}^1, Q_{ID_A})^r.$$

Therefor, our scheme provides the public verifiability. □

6 Conclusions

We have proposed an ID-based signcryption scheme based on the bilinear pairings. Our scheme can work in multiple PKGs environment. We proved that our scheme satisfies the confidentiality, the unforgeability, and the public verifiability. As compared with previously proposed schemes based on a single PKG, our scheme is more suitable for multi-domain ad hoc networks.

Acknowledgements

We would like to thank the anonymous reviewers for their valuable comments and suggestions. This work is supported by the National Natural Science Foundation of China under contract no. 60473029.

References

1. J.H. An, Y. Dodis, and T. Rabin. On the security of joint signature and encryption. In *Advances in Cryptology-EUROCRYPT 2002*, LNCS 2332, pp. 83–107, Springer-Verlag, 2002.
2. J. Baek, R. Steinfeld, and Y. Zheng. Formal proofs for the security of signcryption. In *Public Key Cryptography-PKC 2002*, LNCS 2274, pp. 80–98, Springer-Verlag, 2002.
3. F. Bao and R.H. Deng. A signcryption scheme with signature directly verifiable by public key. In *Public Key Cryptography-PKC'98*, LNCS 1431, pp. 55–59, Springer-Verlag, 1998.
4. 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. In *Advances in Cryptology-ASIACRYPT 2005*, LNCS 3788, pp. 515–532, Springer-Verlag, 2005.
5. M. Bohio and A. Miri. An authenticated broadcasting scheme for wireless ad hoc network. In *2nd Annual Conference on Communication Networks and Services Research-CNSR'04*, pp. 69–74, Fredericton, Canada, 2004.
6. D. Boneh and M. Franklin. Identity-based encryption from the weil pairing. In *Advances in Cryptology-CRYPTO 2001*, LNCS 2139, pp. 213–229, Springer-Verlag, 2001.
7. X. Boyen. Multipurpose identity-based signcryption: a swiss army knife for identity-based cryptography. In *Advances in Cryptology-CRYPTO 2003*, LNCS 2729, pp. 383–399, Springer-Verlag, 2003.
8. L. Chen and C. Kudla. Identity based authenticated key agreement protocols from pairings. In *16th IEEE Computer Security Foundations Workshop-CSFW'03*, pp. 219–233, Pacific Grove, USA, 2003.
9. L. Chen and J. Malone-Lee. Improved identity-based signcryption. In *Public Key Cryptography-PKC 2005*, LNCS 3386, pp. 362–379, Springer-Verlag, 2005.
10. 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. In *Information Security and Cryptology-ICISC 2003*, LNCS 2971, pp. 352–369, Springer-Verlag, 2004.
11. H. Deng and D.P. Agrawal. TIDS: threshold and identity-based security scheme for wireless ad hoc networks. *Ad Hoc Networks*, Vol. 2, No. 3, pp. 291–307, 2004.
12. C. Gamage, J. Leiwo, and Y. Zheng. Encrypted message authentication by firewalls. In *Public Key Cryptography-PKC'99*, LNCS 1560, pp. 69–81, Springer-Verlag, 1999.
13. F. Hess. Efficient identity based signature schemes based on pairings. In *Selected Areas in Cryptography-SAC 2002*, LNCS 2595, pp. 310–324, Springer-Verlag, 2003.
14. H.Y. Jung, D.H. Lee, J.I. Lim, and K.S. Chang. Signcryption schemes with forward secrecy. In *Information Security Application-WISA 2001*, pp. 463–475, Seoul, Korea, 2001.
15. D. Kidston and J. Robinson. Distributed network management for coalition deployments. In *21st Century Military Communications Conference-MILCOM 2000*, Vol. 1, pp. 460–464, Los Angeles, USA, 2000.
16. S. Kim, H. Lee, and H. Oh. Enhanced ID-based authenticated key agreement protocols for a multiple independent PKG environment. In *Information and Communications Security-ICICS 2005*, LNCS 3783, pp. 323–335, Springer-Verlag, 2005.
17. H. Lee, D. Kim, S. Kim, and H. Oh. Identity-based key agreement protocols in a multiple PKG environment. In *Computational Science and Its Applications-ICCSA 2005*, LNCS 3483, pp. 877–886, Springer-Verlag, 2005.

18. G. Li and W. Han. A new scheme for key management in ad hoc networks. In *4th International Conference on Networking-ICN 2005*, LNCS 3421, pp. 242–249, Springer-Verlag, 2005.
19. B. Libert and J.J. Quisquater. A new identity based signcryption schemes from pairings. In *2003 IEEE information theory workshop*, pp. 155–158, Paris, France, 2003.
20. J. Malone-Lee. Identity based signcryption. *Cryptology ePrint Archive*, Report 2002/098, 2002. Available from: http://eprint.iacr.org/2002/098.
21. J. Malone-Lee and W. Mao. Two birds one stone: signcryption using RSA. In *Topics in Cryptology-CT-RSA 2003*, LNCS 2612, pp. 211–226, Springer-Verlag, 2003.
22. Y. Mu and V. Varadharajan. Distributed signcryption. In *Progress in Cryptology-INDOCRYPT 2000*, LNCS 1977, pp. 155–164, Springer-Verlag, 2000.
23. B.N. Park, J. Myung, and W. Lee. ISSRP: a secure routing protocol using identity-based signcryption scheme in ad-hoc networks. In *Parallel and Distributed Computing: Applications and Technologies-PDCAT 2004*, LNCS 3320, pp. 711–714, Springer-Verlag, 2004.
24. B.N. Park and W. Lee. ISMANET: a secure routing protocol using identity-based signcryption scheme for mobile ad-hoc networks. *IEICE Transactions on Communications*, Vol. E88-B, No. 6, pp. 2548–2556, 2005.
25. M. Seo and K. Kim. Electronic funds transfer protocol using domain-verifiable signcryption scheme. In *Information Security and Cryptology-ICISC'99*, LNCS 1787, pp. 269–277, Springer-Verlag, 1999.
26. A. Shamir. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology-CRYPTO'84*, LNCS 196, pp. 47–53, Springer-Verlag, 1984.
27. D.H. Yum and P.J. Lee. New signcryption schemes based on KCDSA. In *Information Security and Cryptology-ICISC 2001*, LNCS 2288, pp. 305–317, Springer-Verlag, 2002.
28. Y. Zheng. Digital signcryption or how to achieve cost (signature & encryption) $\ll$ cost (signature) + cost(encryption). In *Advances in Cryptology-CRYPTO'97*, LNCS 1294, pp. 165–179, Springer-Verlag, 1997.
29. Y. Zheng and H. Imai. How to construct efficient signcryption schemes on elliptic curves. *Information Processing Letters*, Vol. 68, No.5, pp. 227–233, 1998.