An Efficient and Provably-Secure Identity-based Signcryption Scheme for Multiple PKGs *

Zhengping Jin[1, †], Huijuan Zuo[2, 1], Hongzhen Du[1, 3] and Qiaoyan Wen[1]

[1] *State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China*

[†] *E-mail: zhpjin@yahoo.cn*

[2] *Institute of Mathematics and Information, Hebei Normal University, Shijiazhuang 050016, China*

[3] *Mathematics Department, Baoji University of Arts and Sciences, Baoji 721007, China*

Abstract

In this paper, based on the scheme proposed by Barreto et al in ASIACRYPT 2005, an identity-based signcryption scheme in multiple Private Key Generator (PKG) environment is proposed, which mitigates the problems referred to users' private keys escrow and distribution in single PKG system. For security of the scheme, it is proved to satisfy the properties of message confidentiality and existential signature-unforgeability, assuming the intractability of the q-Strong Diffie-Hellman problem and the q-Bilinear Diffie-Hellman Inversion problem. For efficiency, compared with the state-of-the-art signcryption schemes of the same kind, our proposal needs less pairing computations and is shown to be the most efficient identity-based signcryption scheme for multiple PKGs up to date.

1. Introduction

The concept *Identity-based Cryptography* was first introduced by Shamir [12] in 1984. Its basic idea is that the users can choose arbitrary strings, such as their email addresses or other online identifies, as their public keys, and the corresponding private keys are created by binding the identity with a master private key of a trusted authority (called private key generation, or PKG for short). This eliminates much of the overhead associated with key management in conventional public key infrastructure. However, as pointed out in [13], it is unrealistic in practice to set up a single global private key generator mainly because of the inherent key escrow problem, i.e., the PKG knows all its users' private keys. Another flaw of this single PKG cryptographic system is that when distributing the users' private keys, so many secure channels between the PKG and its users are required. In order to mitigate these problems, Wang and Cao [13] proposed the multiple PKGs environment for identity-based cryptographic systems. Exactly speaking, in this multiple PKGs environment, sharing the common global system parameters, each administrator domain maintains its own domain PKG which generates its own master private key, computes and publishes the corresponding master public key, then generates and distributes private keys for the registered users within its domain. A reasonable requirement for this environment is that users could securely communicate with each other no matter whether they belong to the same domain or not. Actuality, the original idea of the multiple PKGs environment was first suggested in an authenticated key agreement protocol [5]. Later, a practical identity-based encryption scheme in multiple PKGs environment was presented in [13], and two identity-based signcryption schemes for multiple PKGs were respectively designed in [7, 8].

Signcryption, first proposed by Zheng [15], is a cryptographic primitive that performs digital signa-

* This work is supported by the National High Technology Research and Development Program of China (Grant No. 2006AA01Z419), the Major Research Plan of the National Natural Science Foundation of China (Grant No. 90604023) and the Natural Science Foundation of Beijing (Grant No. 4072020).

ture and public key encryption in a single operation, at lower computational costs and communication overheads than that of doing both operations sequentially. The first identity-based signcryption scheme was proposed by Malone-Lee [10], but it was pointed out by Libert and Quisquater [9] that this scheme was not semantically secure. Then, an identity-based signcryption scheme was designed by Boyen [4], which provides several strong security properties of confidentiality, non-reputation, etc. Later, Boyen's scheme was improved in efficiency in [1, 6], where Barreto et al's proposal [1], to the best of our knowledge, happens to be the most efficient identity-based signcryption scheme up to date.

In this paper, based on the scheme proposed by Barreto et al [1], we present an identity-based signcryption scheme for multiple PKGs. Our proposal is proved to satisfy the security of message confidentiality and existential signature-unforgeability, assuming the intractability of the q-Strong Diffie-Hellman problem and the q-Bilinear Diffie-Hellman Inversion problem which were formalized by Boneh and Boyen [2, 3, 1]. Thanks to the original advantages of Barreto et al's scheme, our identity-based signcryption scheme for multiple PKGs achieves high efficiency in implementation, which is better than the homogeneous schemes proposed in [7] and [8], and happens to be the most efficient identity-based signcryption scheme for multiple PKGs up to date.

This paper is organized as follows. Some preliminaries are given in section 2. The formal model and some security notions for our identity-based signcryption scheme for multiple PKGs are constructed in section 3. The details of the proposed scheme are elaborated in section 4. We prove compliance of our implementation with the security model and analyze the efficiency of our scheme in section 5. Finally, in section 6, we draw some conclusions.

2. Preliminaries

In this section, we describe the basic security theoretic concepts of bilinear map groups and the hard problems underlying our proposed algorithms.

Let k be a security parameter and p be a k-bit prime number. Let $\mathbb{G}_1, \mathbb{G}_2$ be cyclic additive groups generated by G_1, G_2 respectively, both of whose orders are p . Let $\mathbb{G}_T$ be a cyclic multiplicative group of the same order. We say that $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$ are *bilinear map groups* if there exists a bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_2 \to \mathbb{G}_T$ satisfying :

1. Bilinearity: $e(aP, bQ) = e(P, Q)^{ab}$ for all $(P, Q) \in \mathbb{G}_1 \times \mathbb{G}_2, a, b \in \mathbb{Z}_p$.
2. Non-degeneracy: There exists $P \in \mathbb{G}_1, Q \in \mathbb{G}_2$ such that $e(P, Q) \neq 1_{\mathbb{G}_T}$.
3. Computability: For all $(P, Q) \in \mathbb{G}_1 \times \mathbb{G}_2,\ e(P, Q)$ is efficiently computable.
4. There exists an efficient, publicly computable (but not necessarily invertible) isomorphism $\psi : \mathbb{G}_2 \to \mathbb{G}_1$ such that $\psi(G_2) = G_1$.

The computational assumptions for the security of our scheme were previously formalized by Boneh and Boyen [2, 3, 1] and are recalled in the following definition.

Definition 1. *Let $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$ be bilinear map groups with generators $P \in \mathbb{G}_1$ and $Q \in \mathbb{G}_2$. Two hard problems are described as follows:*
q-Strong Diffie-Hellman problem(q-SDHP).
Given a $(q+2)$-tuple $(P, Q, \alpha Q,\ \alpha^2 Q, \ldots, \alpha^q Q)$, find a pair $(c, \frac{1}{c+\alpha} P)$ with $c \in \mathbb{Z}_p^*$.
q-Bilinear Diffie-Hellman Inversion problem(q-BDHIP).
Given a $(q+2)$-tuple $(P, Q, \alpha Q, \alpha^2 Q, \ldots, \alpha^q Q)$, compute $e(P, Q)^{1/\alpha} \in \mathbb{G}_T$.

3. Formal Model of Identity-based Signcryption

3.1. Generic Scheme

An identity-based signcryption scheme for multiple PKGs consists of five algorithms: Global-Setup, Domain-Setup, Key-Extraction, Signcryption and Unsigncryption, whose functions are specified as follows.

Global-Setup. Given a security parameter k, the globally trusted third-party outputs the system's global public parameters `params`.
Domain-Setup. Given the common parameters `params`, each domain PKG_i generates its domain master private key s_i and the corresponding domain public key Q_{pub_i}.
Key-Extraction. Given an identity $\mathrm{ID_U}$, the domain $\mathrm{PKG}_{i_\mathrm{U}}$ computes the corresponding private key $S_{\mathrm{ID_U}}$, then secretly transmits it to its owner.
Signcryption. Given a message M and a receiver's identity $\mathrm{ID_B}$, the sender obtains the ciphertext σ by computing Signcryption$(M, S_{\mathrm{ID_A}}, \mathrm{ID_B})$.
Unsigncryption. Given a ciphertext σ and a sender's identity $\mathrm{ID_A}$, the intended receiver computes Unsigncryption$(\sigma, \mathrm{ID_A}, S_{\mathrm{ID_B}})$, then returns a message M and its valid signature, or outputs a distinguished symbol $\perp$ if σ does not decrypt into a message bearing the signer $\mathrm{ID_A}$'s signature.

For consistency, we of course require that if $\sigma =$ Signcryption$(M, S_{\mathrm{ID_A}}, \mathrm{ID_B})$, then M should be a part of Unsigncryption$(\sigma, \mathrm{ID_A}, S_{\mathrm{ID_B}})$.

3.2. Security Notions

The formal security notions for identity-based signcryption schemes have been defined in [4, 6, 1] , where Barreto et al [1] mainly considered the property of message confidentiality and the existentially signature-unforgeable security against adaptive chosen message and ciphertext attacks. We modify their definitions slightly to adapt for our identity-based signcryption scheme for multiple PKGs.

Definition 2. *An identity-based signcryption scheme for multiple PKGs, briefly called IBSCMP, is said to satisfy the* ***Message Confidentiality*** *property (or the indistinguishability against adaptive chosen ciphertext attacks property: IND-IBSCMP-CCA) if no probabilistic polynomial time (PPT) adversary has a non-negligible advantage in the following game.*

1. *The challenger $\mathcal{C}$ runs the Global-Setup and Domain-Setup algorithms on input of a security parameter k and sends the system's global-wide public parameter* `params` *and each domain-wide master public key Q_{pub_i} to the adversary $\mathcal{A}$.*
2. *In a find stage, $\mathcal{A}$ performs a polynomially bounded number of the following queries.*
   - *Key-extraction queries: $\mathcal{A}$ chooses an identity $\mathrm{ID_U}$ under PKG$_{i_{\mathrm{U}}}$, then $\mathcal{C}$ computes $S_{\mathrm{ID_U}} =$ Key-Extraction$(\mathrm{ID_U})$ and sends $S_{\mathrm{ID_U}}$ to $\mathcal{A}$.*
   - *Signcryption queries: $\mathcal{A}$ chooses a pair of identities $(\mathrm{ID_S}, \mathrm{ID_R})$ and a plaintext M, then $\mathcal{C}$ returns to $\mathcal{A}$ a ciphertext $\sigma =$ Signcryption$(M, S_{\mathrm{ID_S}}, \mathrm{ID_R})$, where $S_{\mathrm{ID_S}} =$ Key-Extraction$(\mathrm{ID_S})$.*
   - *Unsigncryption queries: $\mathcal{A}$ chooses a pair of identities $(\mathrm{ID_S}, \mathrm{ID_R})$ and a ciphertext σ, then $\mathcal{C}$ returns the result of Unsigncryption$(\sigma, \mathrm{ID_S}, S_{\mathrm{ID_R}})$ to $\mathcal{A}$, where $S_{\mathrm{ID_R}} =$ Key-Extraction$(\mathrm{ID_R})$.*
3. *$\mathcal{A}$ produces two equal length plaintexts M_0, M_1 and a pair of identities $(\mathrm{ID_S^*}, \mathrm{ID_R^*})$, where the private key of $\mathrm{ID_R^*}$ can not have been extracted. $\mathcal{C}$ computes $\sigma^* =$ Signcryption$(M_b, S_{\mathrm{ID_S^*}}, \mathrm{ID_R^*})$ for a random bit $b \in \{0,1\}$ and sends σ^* to $\mathcal{A}$.*
4. *In the guess stage, $\mathcal{A}$ makes new queries as in the find stage. This time, neither the key-extraction query on $\mathrm{ID_R^*}$ nor the unsigncryption query on σ^* could be asked.*
5. *$\mathcal{A}$ finally outputs a bit b' and wins the game if $b' = b$.*

The advantage of $\mathcal{A}$ is defined as $2\Pr[b' = b] - 1$.

Definition 3. *IBSCMP is said to be* ***Existentially Signature-unforgeable*** *against adaptive chosen message and ciphertext attacks (ESUF-IBSCMP-CMA) if no PPT adversary can succeed in the following game with a non-negligible advantage.*

1. *The challenger $\mathcal{C}$ and the adversary $\mathcal{A}$ respectively does the same as step 1 and 2 of the game in definition 2.*
2. *$\mathcal{A}$ produces a triple $(\sigma^*, \mathrm{ID_S^*}, \mathrm{ID_R^*})$, where the private key of $\mathrm{ID_S^*}$ was not previously asked. $\mathcal{A}$ wins the game if the result of unsigncryption$(\sigma^*, \mathrm{ID_S^*}, S_{\mathrm{ID_R^*}})$ is a valid message-signature pair (M^*, s^*) such that no signcryption query involved $M^*, \mathrm{ID_S^*}$ and some receiver $\mathrm{ID_R'}$ (possibly different from $\mathrm{ID_R^*}$) and resulted in a ciphertext σ' whose decryption under the private key $S_{\mathrm{ID_R'}}$ is the alleged forgery $(M^*, s^*, \mathrm{ID_S^*})$.*

The advantage of the adversary $\mathcal{A}$ is its probability of victory.

We note that, in both of above definitions, inside attacks are considered.

4. An Identity-based Signcryption Scheme for Multiple PKGs

In this section, modifying Barreto et al's signcryption scheme proposed in [1], we design an identity-based signcryption scheme in multi-PKG environment as follows.

Global-Setup. Given $k \in \mathbb{Z}^+$, the globally trusted third-party does the following:

1. Chooses bilinear map groups $(\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T)$ of prime order $p > 2^k$ and generators $G_2 \in \mathbb{G}_2, G_1 = \psi(G_2) \in \mathbb{G}_1$, and computes $g = e(G_1, G_2) \in \mathbb{G}_T$.
2. Picks three hash functions $H_1 : \{0,1\}^* \times \mathbb{G}_2 \to \mathbb{Z}_p^*$, $H_2 : \{0,1\}^* \times \mathbb{G}_T \to \mathbb{Z}_p^*$ and $H_3 : \mathbb{G}_T \to \{0,1\}^n$.

The global public parameters are
`params` $:= \{\mathbb{G}_1, \mathbb{G}_2, \mathbb{G}_T, G_1, G_2, g, e, \psi, H_1, H_2, H_3\}$.

Domain-Setup. Given global public parameters, each domain PKG$_i$ does the following:

1. Randomly chooses $s_i \in \mathbb{Z}_p^*$ as the domain master private key and keeps it secret.
2. Calculates $K_{\mathrm{pub}_i} = s_i G_2$ as the domain master public key and publishes K_{pub_i}.

Key-Extraction. Given an identity $\mathrm{ID_U}$, this algorithm outputs the private key $S_{\mathrm{ID_U}}$ under the domain PKG$_{i_{\mathrm{U}}}$, where $S_{\mathrm{ID_U}} = \frac{1}{H_1(\mathrm{ID_U},\, K_{\mathrm{pub}_{i_U}}) + s_{i_{\mathrm{U}}}} G_2 \in \mathbb{G}_2$.

Signcryption. Given a message $M \in \{0,1\}^*$ and a receiver's identity $\mathrm{ID_B}$, the sender does as follows:

1. Randomly picks $x \in \mathbb{Z}_p^*$, computes $r = g^x$ and $c = M \oplus H_3(r) \in \{0,1\}^n$.
2. Sets $h = H_2(M, r) \in \mathbb{Z}_p^*$.
3. Computes $S = (x + h)\psi(S_{\mathrm{ID_A}})$, $T = x\big(H_1(\mathrm{ID_B},\, K_{\mathrm{pub}_{i_{\mathrm{B}}}})G_1 + \psi(K_{\mathrm{pub}_{i_{\mathrm{B}}}})\big)$.

The ciphertext is $\sigma = \langle c, S, T \rangle \in \{0,1\}^n \times \mathbb{G}_1 \times \mathbb{G}_1$.

Unsigncryption. Given a ciphertext $\sigma = \langle c, S, T \rangle$ and some sender's identity $\mathrm{ID_A}$, the intended receiver does the following:

1. Computes $r = e(T, S_{\mathrm{ID_B}}), M = c \oplus H_3(r)$, and $h = H_2(M, r)$.
2. Returns the message M and the signature $(h, S) \in \mathbb{Z}_p^* \times \mathbb{G}_1$ if $r = e\big(S, H_1(\mathrm{ID_A}, K_{\mathrm{pub}_{i_\mathrm{A}}})G_2 + K_{\mathrm{pub}_{i_\mathrm{A}}}\big)g^{-h}$ and the $\perp$ symbol otherwise.

It is easy to see that the proposed scheme is consistent.

5. Security Results and Efficiency Comparisons

The following theorems claim the security of our proposal under the same irreflexivity assumption as Boyen's scheme [4]: the signcryption algorithm is assumed to disallow messages from being addressed to the same identity as authored them.

Theorem 1. *Let $\mathcal{A}$ be an adversary against the IND-IBSCMP-CCA security of our scheme. If $\mathcal{A}$ has an advantage ϵ after running for time t, making at most q_{h_i}, q_s, q_u queries to H_i $(i = 1, 2, 3)$, the signcryption oracle and the unsigncryption oracle respectively, then we have an algorithm $\mathcal{B}$ that solves the q-BDHIP for $q = q_{h_1}$ with probability*

$$\epsilon' \geqslant \frac{\epsilon}{q_{h_1}(2q_{h_2} + q_{h_3})}\left(1 - q_s\frac{q_s + q_{h_2}}{2^k}\right)\left(1 - \frac{q_u}{2^k}\right)$$

and within a time $t' < t + O(q_s + q_u)t_p + O(q_{h_1}^2)t_m + O(q_u q_{h_2})t_e$, where k is the security parameter whereas t_p, t_m and t_e are respectively the costs of a pairing computation, a multiplication in $\mathbb{G}_2$ and an exponentiation in $\mathbb{G}_T$.

Proof. Algorithm $\mathcal{B}$ takes a random instance $(P, Q, \alpha Q, \alpha^2 Q, \ldots, \alpha^q Q)$ of the q-BDHIP as input, and attempts to extract $e(P, Q)^{1/\alpha}$ by running $\mathcal{A}$ as a subroutine and acting as $\mathcal{A}$'s challenger in the game of definition 2.

At first, $\mathcal{B}$ does some preparations for interacting with $\mathcal{A}$. It randomly selects $R_1, \ldots, R_q$ from $\mathbb{Z}_p^*$ and $\xi \in \{1, 2, \ldots, q\}$. For $i \in \{1, \ldots, q\}\backslash\{\xi\}$, it computes $x_i = x_\xi - R_i$ where $x_\xi = R_\xi$. Then it sets up generators $G_2 \in \mathbb{G}_2, G_1 = \psi(G_2) \in \mathbb{G}_1$ and another element $X = \alpha G_2 \in \mathbb{G}_2$ such that it knows $q - 1$ pairs $(R_i, I_i = \frac{1}{R_i + \alpha}G_2), i \in \{1, \ldots, q\}\backslash\{\xi\}$. To do so,

1. It expands $f(z) = \prod_{i=1,\ i\neq\xi}^{q}(z + R_i)$ to obtain $c_0, \ldots, c_{q-1} \in \mathbb{Z}_p^*$ so that $f(z) = \sum_{j=1}^{q-1} c_j z^j$, and sets generators $G_2 = \sum_{j=0}^{q-1} c_j(\alpha^j Q) = f(\alpha)Q \in \mathbb{G}_2$ and $G_1 = \psi(G_2) = f(\alpha)P \in \mathbb{G}_1$. Another element $X \in \mathbb{G}_2$ is fixed to $X = \sum_{j=1}^{q} c_{j-1}(\alpha^j Q) = \alpha G_2$ although $\mathcal{B}$ does not know α.
2. For $i \in \{1, \ldots, q\}\backslash\{\xi\}$, it expands $f_i(z) = \frac{f(z)}{z + R_i} = \prod_{k=1,\ k\neq\xi,\ k\neq i}^{q}(z + R_k)$ to get $d_0, d_1, \ldots, d_{q-2} \in \mathbb{Z}_p^*$ such that $f_i(z) = \sum_{j=0}^{q-2} d_j z^j$, and computes the pair (R_i, I_i) by calculating $I_i = \sum_{j=0}^{q-2} d_j(\alpha^j Q) = f_i(\alpha)Q = \frac{f(\alpha)}{\alpha + R_i}Q = \frac{1}{R_i + \alpha}G_2$.

Subsequently, $\mathcal{B}$ randomly selects $y_j \in \mathbb{Z}_p^*$ for $j = 1, 2, \ldots, N$, where $N(< q)$ is the total number of domain PKGs. The domain-wide master public key of PKG_j is chosen as $K_{pub_j} = -X - (x_\xi + y_j)G_2 = (-\alpha - x_\xi - y_j)G_2$ so that its unknown private key is implicitly set to $s_j = -\alpha - x_\xi - y_j \in \mathbb{Z}_p^*$. For $i \in \{1, \ldots, q\}, j \in \{1, \ldots, N\}$, let $H_{i,j} = x_i + y_j$, then $\mathcal{B}$ has pairs $(H_{i,j}, -I_i) = (H_{i,j}, \frac{1}{H_{i,j} + s_j}G_2), i \in \{1, \ldots, q\}\backslash\{\xi\}, j \in \{1, \ldots, N\}$.

$\mathcal{B}$ then initializes a counter l to 1 and starts $\mathcal{A}$ on input of $(G_1, G_2, K_{pub_1}, \ldots, K_{pub_N})$. During the game, $\mathcal{A}$ will consult $\mathcal{B}$ for answers to the random oracles H_1, H_2 and H_3, and $\mathcal{B}$ generates these answers randomly, but to maintain the consistency and to avoid collision, $\mathcal{B}$ keeps three lists L_1, L_2, L_3 respectively to store the answers.

- H_1-queries on input ID_U under some PKG, say PKG_j : if it is the first time for ID_U to query H_1 , $\mathcal{B}$ returns $H_{l,j}$, stores the information $(ID_U, K_{pub_j}, H_{l,j})$ in L_1, and increments l; otherwise, returns the corresponding value $H_{i,j}$ in L_1.
- H_2-queries on input (M, r): $\mathcal{B}$ returns the defined value if it exists and a random value $h_2 \in \mathbb{Z}_p^*$ otherwise. To anticipate possible subsequent unsigncryption requests, $\mathcal{B}$ additionally simulates H_3 on its own to obtain $h_3 = H_3(r) \in \{0,1\}^n, c = M \oplus h_3, \gamma = r \cdot e(G_1, G_2)^{h_2}$, and stores the information (M, r, h_2, c, γ) in L_2.
- H_3-queries on input $r \in \mathbb{G}_T$: $\mathcal{B}$ returns the previously assigned value if it exists and a random value $h_3 \in \{0,1\}^n$ otherwise. In the latter case, the input r and the response h_3 are stored in L_3.
- Key-extraction queries on input ID_l under some PKG_j: if $l = \xi$, then $\mathcal{B}$ fails. Otherwise, it knows that $H_1(ID_l, K_{pub_j}) = H_{l,j}$ and returns $-I_l = \frac{1}{H_{l,j} + s_j}G_2 \in \mathbb{G}_2$.

– Signcryption queries for a plaintext M and identities $(ID_S, ID_R) = (ID_\mu, ID_\nu)$ under PKG$_{i_\mu}$ and PKG$_{i_\nu}$ respectively, $\mu, \nu \in \{1, \ldots, q\}, i_\mu, i_\nu \in \{1, \ldots, N\}$: We assume that $\mu = \xi$ (and hence $\nu \neq \xi$ by the irreflexivity assumption), because otherwise $\mathcal{B}$ knows the sender's private key $S_{ID_\mu} = -I_\mu$ and answers the query according to the Signcryption algorithm. Thus $\mathcal{B}$ randomly chooses $\lambda, h \in \mathbb{Z}_p^*$ and computes $S = \lambda\psi(S_{ID_\nu}) = -\lambda\psi(I_\nu), T = \lambda\psi(H_{\xi,i_\mu}G_2 + K_{pub_{i_\mu}}) - h\psi(H_{\nu,i_\nu}G_2 + K_{pub_{i_\nu}})$ in order to obtain the desired equality $r = e(T, S_{ID_\nu}) = e(S, H_{\xi,i_\mu}G_2 + K_{pub_{i_\mu}})e(G_1, G_2)^{-h} = e\big(\psi(S_{ID_\nu}), H_{\xi,i_\mu}G_2 + K_{pub_{i_\mu}}\big)^\lambda e(G_1, G_2)^{-h}$ before patching the hash value $H_2(M, r)$ to h ($\mathcal{B}$ fails if H_2 is already defined but this only happens with probability $\frac{q_s+q_{h_2}}{2^k}$). At last, $\mathcal{B}$ returns the ciphertext $\sigma = \langle M \oplus H_3(r), S, T\rangle$.
– Unsigncryption queries on a ciphertext $\sigma = \langle c, S, T\rangle$ for identities $(ID_S, ID_R) = (ID_\mu, ID_\nu)$ under PKG$_{i_\mu}$ and PKG$_{i_\nu}$ respectively: we assume that $\nu = \xi$ for similar reasons as in signcryption queries, hence $\mu \neq \xi$ by the irreflexivity assumption. Therefore, $\mathcal{B}$ has the sender's private key S_{ID_μ} and also knows that, for all valid ciphertexts, $\log_{S_{ID_\mu}}\big(\psi^{-1}(S) - hS_{ID_\mu}\big) = \log_{\psi(Q_{ID_\nu})}(T)$, where $h = H_2(M, r)$ is obtained in the Signcryption algorithm and $Q_{ID_\nu} = H_{\nu,i_\nu}G_2 + K_{pub_{i_\nu}}$. Hence,
$$\begin{aligned} &e(T, S_{ID_\mu}) \\ &= e\big(\psi(Q_{ID_\nu}), \psi^{-1}(S) - hS_{ID_\mu}\big) \\ &= e\big(\psi(Q_{ID_\nu}), \psi^{-1}(S)\big)e\big(\psi(Q_{ID_\nu}), S_{ID_\mu}\big)^{-h} \quad (*) \\ &= e(S, Q_{ID_\nu})e\big(\psi(Q_{ID_\nu}), S_{ID_\mu}\big)^{-h}. \end{aligned}$$
Thus, $\mathcal{B}$ computes $\gamma = e(S, Q_{ID_\mu})$, where $Q_{ID_\mu} = H_{\mu,i_\mu}G_2 + K_{pub_{i_\mu}}$, and searches through list L_2 for entries of the form $(M_i, r_i, h_2^{(i)}, c, \gamma)$ indexed by $i \in \{1, \ldots, q_{h_2}\}$. If none is found, σ is rejected. Otherwise, each one of them is further examined for the corresponding indexes, $\mathcal{B}$ checks if
$$\begin{aligned} &e(T, S_{ID_\mu}) \\ &= e(S, Q_{ID_\nu})e\big(\psi(Q_{ID_\nu}), S_{ID_\mu}\big)^{-h_2^{(i)}}, \qquad (**) \end{aligned}$$
meaning that $(*)$ is satisfied. The pairings are computed only once and at most q_{h_2} exponentiations are needed. If the unique $i \in \{1, \ldots, q_{h_2}\}$ satisfying $(**)$ is detected, the matching pair $(M_i, \langle h_{2,i}, S\rangle)$ is returned. Otherwise, σ is rejected. Overall, an inappropriate rejection occurs with probability smaller than $\frac{q_u}{2^k}$ across the game.

At the challenge phase, $\mathcal{A}$ outputs mesages (M_0, M_1) and identities (ID_S, ID_R) under PKG$_{i_S}$ and PKG$_{i_R}$ respectively for which she never obtained ID_R's private key. If $ID_R \neq ID_\xi$, $\mathcal{B}$ aborts. Otherwise, it randomly picks $\beta \in \mathbb{Z}_p^*$, $c \in \{0,1\}^n$ and $S \in \mathbb{G}_1$ to return the challenge $\sigma^* = \langle c, S, T\rangle$ where $T = -\beta G_1 \in \mathbb{G}_1$. If we define $\rho = \beta/\alpha$ and since $s_{i_R} = -\alpha - I_\xi - y_{i_R} = -\alpha - H_{\xi,i_R}$ where $i_R \in \{1, \ldots, N\}$, we can check that
$$\begin{aligned} T = -\beta G_1 &= -\alpha\rho G_1 = (H_{\xi,i_R} + s_{i_R})\rho G_1 \\ &= \rho H_{\xi,i_R}G_1 + \rho\psi(K_{pub_{i_R}}). \end{aligned}$$
$\mathcal{A}$ cannot recognize that σ^* is not a proper ciphertext unless she queries H_2 or H_3 on $e(G_1, G_2)^\rho$. Along the guess stage, her view is simulated as before and her eventual output is ignored. Standard arguments can show that a successful $\mathcal{A}$ is very likely to query H_2 or H_3 on the input $e(G_1, G_2)^\rho$ if the simulation is indistinguishable from a real attack environment.

To produce a result, $\mathcal{B}$ fetches a random entry (M, r, h_2, c, γ) or (r, h_3) from the lists L_2 or L_3. With probability $\frac{1}{2q_{h_2}+q_{h_3}}$, the chosen entry will contain the right element $r = e(G_1, G_2)^\rho = e(P, Q)^{f(\alpha)^2\beta/\alpha}$, where $f(z) = \sum_{i=0}^{q-1} c_i z^i$ is the polynomial for which $G_2 = f(\alpha)Q$. At last, the q-BDHIP solution can be extracted by $e(P, Q)^{1/\alpha} = r^{(c_0^2\beta)^{-1}}\pi^{-(c_0^2)^{-1}}$ where $\pi = \left(e\big(\sum_{i=0}^{q-2} c_{i+1}(\alpha^i P),\ c_0 Q\big)e\big(G_1,\ \sum_{j=0}^{q-2} c_{j+1}(\alpha^j Q)\big)\right)$.

In an analysis of $\mathcal{B}$'s advantage, we note that it succeeds in above game if and only if all of the following independent events happen:

E_1: ID_ξ is challenged, which implies that no key-extraction query is made on ID_ξ.
E_2: There is no collision on H_2 in a signcryption query.
E_3: No valid ciphertext is rejected.
E_4: $\mathcal{B}$ selects the correct element from L_2 or L_3 at the last phase.

Clearly, $\Pr[E_1] = \frac{1}{q_{h_1}}$, $\Pr[E_2] \geqslant 1 - \frac{q_s(q_s+q_{h_2})}{2^k}$, $\Pr[E_3] \geqslant 1 - \frac{q_u}{2^k}$, $\Pr[E_4] = \frac{1}{2q_s+q_u}$. Thus,
$$\begin{aligned} \epsilon' &= \epsilon \cdot \Pr[E_1 \wedge E_2 \wedge E_3 \wedge E_4] \\ &\geqslant \frac{\epsilon}{q_{h_1}(2q_{h_2} + q_{h_3})}\big(1 - q_s\frac{q_s + q_{h_2}}{2^k}\big)\big(1 - \frac{q_u}{2^k}\big). \end{aligned}$$
On the other hand, $\mathcal{B}$'s workload is dominated by $O(q_{h_1}^2)$ multiplications in the preparation phase, $O(q_s+q_u)$ pairing calculations and $O(q_u q_{h_2})$ exponentiations in $\mathbb{G}_T$ in its emulation of the signcryption and unsigncryption oracles, thus it totally takes a time $t' < t + O(q_s + q_u)t_p + O(q_{h_1}^2)t_m + O(q_u q_{h_2})t_e$. □

Theorem 2. *Let $\mathcal{A}$ be an adversary against the ESUF-IBSCMP-CMA security of our scheme. If $\mathcal{A}$ produces a forgery with probability $\epsilon \geqslant 10q_{h_1}(q_s + 1)(q_s + q_{h_2})/(2^k - 1)$ after running a time t, and making at most*

q_{h_i} queries to random oracles H_i $(i = 1, 2, 3)$, q_s signcryption queries and q_u unsigncryption queries, then we have an algorithm $\mathcal{B}$ that is able to solve the q-SDHP for $q = q_{h_1}$ in expected time t'

$$\leqslant 120686 q_{h_1} q_{h_2} \frac{t + O\big((q_s+q_u)t_p\big) + q_u q_{h_2} t_e}{\epsilon(1-1/2^k)(1-q/2^k)} + O(q^2 t_m),$$

where t_p, t_e, t_m denote the same quantities as in theorem 1.

Proof. Algorithm $\mathcal{B}$ takes a random instance $(P, Q, \alpha Q, \alpha^2 Q, \ldots, \alpha^q Q)$ of the q-Strong Diffie-Hellman problem as input, and attempts to extract a pair $(\omega, \frac{1}{\omega+\alpha}P), \omega \in \mathbb{Z}_p^*$ by running $\mathcal{A}$ as a subroutine and acting as $\mathcal{A}$'s challenger in the game of definition 3.

At first, we will show that a forger in the ESUF-IBSCMP-CMA game implies a forger in a chosen-message and *given* identity attack.

Before it, we need some preparations. $\mathcal{B}$ randomly selects $R_i \in \mathbb{Z}_p^*$ for $i \in \{1, \ldots, q-1\}$. With the technique used in the proof of theorem 1, it sets up generators $G_2 \in \mathbb{G}_2, G_1 = \psi(G_2) \in \mathbb{G}_1$ and another element $X = \alpha G_2 \in \mathbb{G}_2$ such that it knows $q-1$ pairs $(R_i, \frac{1}{R_i+\alpha}G_2)$ for $i \in \{1, \ldots, q-1\}$. Subsequently, $\mathcal{B}$ randomly selects $y_j \in \mathbb{Z}_p^*$ for $j = 1, 2, \ldots, N$, where $N(< q)$ is the total number of domain PKGs. The domain-wide master public key of PKG$_j$ is chosen as $K_{pub_j} = X - y_j G_2 = (\alpha - y_j)G_2$ so that its unknown private key is implicitly set to $s_j = \alpha - y_j \in \mathbb{Z}_p^*$. For $i \in \{1, \ldots, q-1\}$ and $j \in \{1, \ldots, N\}$, let $H_{i,j} = R_i + y_j$, then we have pairs $(H_{i,j}, \frac{1}{H_{i,j}+s_j}G_2)$. $\mathcal{B}$ then initializes a counter v to 1 and randomly chooses an identity $ID^* \in \{0,1\}^*$ under PKG$_j, j \in \{1, \ldots, N\}$ as the sender's identity of a challenge to some forger in a chosen-message and *given* identity attack against our scheme. Now we describe the oracles that $\mathcal{B}$ needed for answering necessary consultations. To maintain the consistency and to avoid collision, $\mathcal{B}$ keeps three lists L_1, L_2, L_3 respectively to store the random answers of the random oracles H_1, H_2 and H_3.

- H_1-queries on input identity ID_U under some PKG$_{i_U}$: if it is the first time for ID_U to query H_1, $\mathcal{B}$ returns $\omega + y_j$(ω is randomly chosen from $\mathbb{Z}_p^*$) if $ID_U = ID^*$ and returns H_{v,i_U} if $ID_U \neq ID^*$, then stores the answer in L_1 and increments v; otherwise, returns the corresponding value in existed information.
- H_2-queries on input (M, r) and H_3-queries for an input $r \in \mathbb{G}_T$ are exactly the same as those proposed in the proof of theorem 1.
- Key-extraction queries on an input ID_v under some PKG$_j$: if $ID_v = ID^*$, then $\mathcal{B}$ fails. Otherwise, it knows that $H_1(ID_v, K_{pub_j}) = H_{v,j}$ and returns $\frac{1}{H_{v,j}+s_j}G_2 \in \mathbb{G}_2$.
- Signcryption queries for a plaintext M and identities $(ID_S, ID_R) = (ID_\mu, ID_\nu)$ under PKG$_{i_\mu}$ and PKG$_{i_\nu}$ respectively, $\mu, \nu \in \{1, \ldots, q\}, i_\mu, i_\nu \in \{1, \ldots, N\}$: we assume that $ID_\mu = ID^*$ for the same reason proposed in the signcryption query during the proof of theorem 1, and hence $ID_\nu \neq ID^*$ by the irreflexivity assumption. $\mathcal{B}$ randomly chooses λ, $h \in \mathbb{Z}_p^*$, and computes $S = \lambda\psi(S_{ID_\nu}) = \lambda\psi(\frac{1}{H_{\nu,i_\nu}+s_{i_\nu}}G_2)$, $T = \lambda\psi((\omega + y_{i_\mu})G_2 + K_{pub_{i_\mu}}) - h\psi(H_{\nu,i_\nu}G_2 + K_{pub_{i_\nu}})$ in order to obtain the equality $r = e(T, S_{ID_\nu}) = e(S, (\omega + y_{i_\mu})G_2 + K_{pub_{i_\mu}})e(G_1, G_2)^{-h} = e\big(\psi(S_{ID_\nu}), (\omega + y_{i_\mu})G_2 + K_{pub_{i_\mu}}\big)^\lambda e(G_1, G_2)^{-h}$ before patching the hash value $H_2(M, r)$ to h ($\mathcal{B}$ fails if H_2 is already defined but this only happens with probability at most $\frac{q_s+q_{h_2}}{2^k}$). At last, the ciphertext $\sigma = \langle M \oplus H_3(r), S, T\rangle$ is returned.
- Unsigncryption queries on a ciphertext $\sigma = \langle c, S, T\rangle$ for identities $(ID_S, ID_R) = (ID_\mu, ID_\nu)$ under PKG$_{i_\mu}$ and PKG$_{i_\nu}$ respectively: we assume that $ID_\nu = ID^*$(and hence $ID_\mu \neq ID^*$ by the irreflexivity assumption) because otherwise $\mathcal{B}$ knows the receiver's private key and can normally run the Unsigncryption algorithm. Therefore, $\mathcal{B}$ has the sender's private key $S_{ID_\mu} = \frac{1}{H_{\mu,i_\mu}+s_{i_\mu}}G_2$ and also knows that, for all valid ciphertexts, $\log_{S_{ID_\mu}}\big(\psi^{-1}(S) - hS_{ID_\mu}\big) = \log_{\psi(Q_{ID_\nu})}(T)$, where $h = H_2(M, r)$ is obtained in the Signcryption algorithm and $Q_{ID_\nu} = (\omega + y_{i_\nu})G_2 + K_{pub_{i_\nu}}$. Hence, what $\mathcal{B}$ should do is the same as that described in the unsigncryption query during the proof of theorem 1.

Now we show how to design an algorithm $\mathcal{F}$ in a chosen-message and given identity attack to our scheme by running the ESUF-IBSCMP-CMA attacker $\mathcal{A}$ that makes q_{h_i} queries to random oracles H_i $(i = 1, 2, 3)$, q_s signcryption queries and q_u queries to unsigncryption oracle. For any ID under some PKG, our algorithm $\mathcal{F}$ is as follows:

1. $\mathcal{F}$ Chooses $l \in \{1, \ldots, q\}$ randomly. Denote by $(ID_j, K_{pub_{i_j}})$ the input of the j-th query to H_1 asked by $\mathcal{A}$, $\mathcal{F}$ sets $(ID_j^*, K_{pub_{i_j}}^*)$ to be (ID, K_{pub}) if $j = l$ and $(ID_j, K_{pub_{i_j}})$ otherwise.
2. $\mathcal{F}$ Runs $\mathcal{A}$ with the given system parameters and responds to $\mathcal{A}$'s queries to H_1, H_2, H_3, signcryption oracle and unsigncryption oracle by taking the place of $\mathcal{A}$'s input ID_j with ID_j^* and running corresponding oracles.
3. Denote the output of $\mathcal{A}$ as (ID_{out}, m, σ). If $ID_{out} = ID$ and (ID, m, σ) is valid, then $\mathcal{F}$ outputs (ID, m, σ); otherwise, $\mathcal{F}$ fails.

We can see that the advantage of $\mathcal{F}$ is $\epsilon^* \geqslant (1 - \frac{1}{2^k})\frac{1}{q_{h_1}}\epsilon \geqslant 10(q_s+1)(q_s+q_{h_2})/2^k$, and its running time is almost the same as $\mathcal{A}$ needs.

Subsequently, $\mathcal{B}$ runs $\mathcal{F}$ which is a forger in a chosen-message and given identity attack to our scheme as a subroutine instead of $\mathcal{A}$ and attempts to solve the q-SDHP. It is noted that $\mathcal{F}$ can extract private keys associated to any identity but ID^* by querying the key-extraction oracle. Therefore, thanks to the irreflexivity assumption, it is able to extract clear message-signature pairs from ciphertexts produced by the forger as it knows the private key of the receiving identity. Thus, we just consider the message-signature pairs which are decrypted from ciphertexts produced by the forger and could be seen as ID^*'s valid signature. Applying the forking lemma [11, Theorem 13], from the forger $\mathcal{F}$, we can build an algorithm $\mathcal{F}'$ that replays $\mathcal{F}$ a sufficient number of times on the input (ID^*, K_{pub_j}) to obtain two suitable forgeries which can be decrypted into two valid message-signature pairs $\langle m, r, h_1, S_1\rangle, \langle m, r, h_2, S_2\rangle$ with $h_1 \neq h_2$, in expected time $t^* \leqslant 120686 q_{h_1} t/\epsilon$. Since both forgeries satisfy the verification equation, we obtain

$$e(S_1, Q_{ID^*})g^{-h_1} = e(S_2, Q_{ID^*})g^{-h_2},$$

where $Q_{ID^*} = (\omega+y_j)G_2 + K_{pub_j} = (\omega+\alpha)G_2$. Then it comes that

$$e\big((h_1-h_2)^{-1}(S_1-S_2), Q_{ID^*}\big) = e(G_1, G_2),$$

and hence $(h_1-h_2)^{-1}(S_1-S_2) = \frac{1}{\omega+\alpha}G_1$. Proceeded as in [2], $\mathcal{B}$ can extract $\frac{1}{\omega+\alpha}P$ from $\frac{1}{\omega+\alpha}G_1$ as follows: it first obtains $\gamma_{-1}, \gamma_0, \ldots, \gamma_{q-2} \in \mathbb{Z}_p^*$ for which $\frac{f(z)}{z+\omega} = \frac{\gamma_{-1}}{z+\omega} + \sum_{i=0}^{q-2}\gamma_i z^i$ where $f(z) = \prod_{i=0}^{q-1}(z+R_i)$ obtained at the preparation phase and eventually computes $\frac{1}{\gamma_{-1}}\big(\frac{1}{\omega+\alpha}G_1 - \sum_{i=0}^{q-2}\gamma_i\psi(\alpha^i Q)\big) = \frac{1}{\omega+\alpha}P$. Thus, $\mathcal{B}$ gets the pair $(\omega, \frac{1}{\omega+\alpha}P)$.

It finally comes that, since $\mathcal{F}$ makes a forgery in a time t with probability $\epsilon^* \geqslant (1-\frac{1}{2^k})\frac{1}{q_{h_1}}\epsilon \geqslant 10(q_s+1)(q_s+q_{h_2})/2^k$, $\mathcal{B}$ solves the q-SDHP in time less than

$$120686 q_{h_1} q_{h_2} \frac{t + O\big((q_s+q_u)t_p\big) + q_u q_{h_2} t_e}{\epsilon(1-1/2^k)(1-q/2^k)} + O(q^2 t_m),$$

where the last term accounts for the cost of the preparation phase. □

In the rest of this section, let us analyze the efficiency of our identity-based signcryption scheme for multiple PKGs. Table 1 summaries the number of relevant basic operations underlying several identity-based signcryption schemes for multiple PKGs, namely, $\mathbb{G}_T$ exponentiations, scalar point multiplications, and pairing evaluations. It is noted that the computation of the pairing is the most time-consuming in pairing based cryptographic schemes [14]. It is easy to see from Table 1 that our proposal needs less pairing computations , so it is more efficient than that of Li et al 's [8] and Lal-Kushwah's [7].

Table 1. Efficiency comparison

		Li-Hu-Zhang	Lal-Kushwah	ours
SC	exp	1	1	1
	mult	2	3	2
	pairing	1	1	
USC	exp	1		1
	mult		1	
	pairing	4	3	2

Note: SC – Signcryption; USC – Unsigncryption

6. Conclusion

We have proposed a new identity-based signcryption scheme for multiple PKGs, which is proved to be indistinguishable against adaptive chosen ciphertext attacks and signature-unforgeable against adaptive chosen plaintext and ciphertext attacks based on some computational assumptions. Compared with the state-of-the-art signcryption schemes of the same kind, our scheme needs less pairing computations and is the most efficient identity-based signcryption scheme in multiple PKGs environment up to date.

References

[1] P. S. L. M. Barreto, B. Libert, N. McCullagh and J. Quisquater, "Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps", *Advances in Cryptology–Proceedings of ASIACRYPT'05*, Vol. 3788 of LNCS, Springer-Verlag, Berlin, 2005, pages 515–532.

[2] D. Boneh and X. Boyen, "Short Signature without Random Oracles", *Advances in Cryptology–Proceedings of EUROCRYPT'04*, Vol. 3027 of LNCS, Springer-Verlag, Berlin, 2004, pages 56–73.

[3] D. Boneh and X. Boyen, "Efficient Selective-ID Secure Identity Based Encryption without Random Oracles", *Advances in Cryptology–Proceedings of EUROCRYPT'04*, Vol. 3027 of LNCS, Springer-Verlag, Berlin, 2004, pages 223–238.

[4] X. Boyen, "Multipurpose Identity-based Signcryption: A Swiss Army Knife for Identity-based Cryptography", *Advances in Cryptology–Proceedings of CRYPTO'03*, Vol. 2729 of LNCS, Springer-Verlag, Berlin, 2003, pages 383–399.

[5] L. Chen and C. Kudla, "Identity Based Authenticated Key Agreement Protocols from Pairings", *Proceedings*

of the 16th IEEE Computer Security Foundations Workshop (CSFW 2003), Pacific Grove, USA, 2003, pages 219–233.

[6] L. Chen and J. Malone-Lee, "Improved Identity-based Signcryption", *Proceedings of Public Key Cryptography 2005 (PKC 2005)*, Vol. 3386 of LNCS, Springer-Verlag, Berlin, 2005, pages 362–379.

[7] S. Lal and P. Kushwah, "Multi-PKG ID Based Signcryption", Cryptology ePrint Archive, Report 2008/050, 2008. `http://eprint.iacr.org/2008/050`.

[8] F. Li, Y. Hu and C. Zhang, "An Identity-based Signcryption Scheme for Multi-domain Ad Hoc Networks", *Proceedings of the 5th International Conference on Applied Cryptography and Network Security (ACNS 2007)*, Vol. 4521 of LNCS, Springer-Verlag, Berlin, 2007, pages 373–384.

[9] B. Libert and J.-J. Quisquater, "A New Identity Based Signcryption Scheme from Pairings", *Proceedings of the IEEE Information Theory Workshop (ITW 2003)*, Paris, France, 2003, pages 155–158.

[10] J. Malone-Lee, "Identity Based Signcryption", Cryptology ePrint Archive, Report 2002/098, 2002. `http://eprint.iacr.org/2002/098`.

[11] D. Pointcheval and J. Stein, "Security arguments for digital signatures and blind signatures", *Journal of Cryptology*, Vol. 13, No. 3, Springer-Verlag, Berlin, 2000, pages 361–396.

[12] A. Shamir, "Identity-based Cryptosystem and Signature Scheme", *Advances in Cryptology–Proceedings of CRYPTO'84*, Vol. 0196 of LNCS, Springer-Verlag, Berlin, 1984, pages 47–53.

[13] S. Wang and Z. Cao, "Practical Identity-based Encryption (IBE) in Multiple-PKG Environment and Its Applications", Cryptology ePrint Archive, Report 2007/100, 2007. `http://eprint.iacr.org/2007/100`.

[14] F. Zhang, R. Safavi-Naini and W. Susilo, "An Efficient Signature Scheme from Bilinear Pairings and Its Applications", *Proceedings of Public Key Cryptography 2004 (PKC 2004)*, Vol. 2947 of LNCS, Springer-Verlag, Berlin, 2004, pages 277–290.

[15] Y. Zheng, "Digital Signcryption or How to Achieve Cost(Signature & Encryption) $\ll$ Cost(Signature) + Cost(Encryption)", *Advances in Cryptology–Proceedings of CRYPTO'97*, Vol. 1294 of LNCS, Springer-Verlag, Berlin, 1997, pages 165–179.