2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing

Threshold Attribute-Based Signcryption in Standard Model

Haibin Zheng
School of Mathematics
Shandong University
Jinan, China
zhenghaibin900529@163.com

Jing Qin*
School of Mathematics
Shandong University
Jinan, China
qinjing@sdu.edu.cn
**Corresponding Authoor*

Jiankun Hu
School of Engineering and IT
University of New South Wales
Australia
J.Hu@adfa.edu.au

Qianhong Wu
School of Electronics and Information Engineering
Beihang University
Beijing, China
qianhong.wu@buaa.edu.cn

***Abstract*—Signcryption is a public key cryptosystem that achieves the functions of digital signature and public key encryption simultaneously. It significantly reduces the cost of traditional signature-then-encryption approach. Although a large body of signcryption schemes have been proposed, few works have been done on attribute-based signcrytion (ABSC) which simultaneously achieves the functionalities of attribute-based encryption (ABE) and attribute-based signature (ABS), two important cryptographic primitives proposed to enforce fine-grained access control and user authentication in cloud computing applications. In this paper, we present a threshold attribute-based signcryption (TABSC) scheme. The scheme is proven secure under the well-established Decisional Bilinear Diffie-Hellman (DBDH) and the standard Computational Diffie-Hellman (CDH) assumptions in the standard model. Compared with the state of the ABSC art, our scheme has comparable efficiency without relying on any random oracle.**

***Keywords*-Signcryption; Attribute-based signcryption; Standard model; Threshold cryptosystem; Threshold signcryption**

I. Introduction

Consider a scenario where two people, say, Alice and Bob, who have never seen each other before want to communicate on the internet. For secure communication such that only they two can understand each other, in the traditional way Alice first signs the message, then encrypts the message (and the signature) and finally, sends the encrypted message together with the signature of the message to Bob. In 1997, Zheng introduced the concept of signcryption [1] which achieves the functionalities of signature scheme and and encryption scheme simultaneously. The point is to provide authenticity and confidentiality in one step at less cost than the traditional sign-then-encrypt approach using the underlying signature and encryption schemes.

Since Zheng's seminal work, a large body of signcryption schemes has been proposed in different settings. Unlike Zheng's scheme in the discrete logarithm setting, the signcryption constructions in [2],[3] are based on integer factorization and the RSA cryptosystem. Built from bilinear groups, the first identity-based Signcryption (IBSC) was introduced by Malone-Lee in 2002 [4]. In contrast to conventional signcryption in the public-key infrastructure setting, IBSC eliminates the requirement to certify the public keys of the users and thus relieves the system from complicated certificates management. The idea is to use a user's recognizable identity, e.g., his/her national identity card number, email address, telephone number or/and face photo, to serve as the user's public key and identify the user. Duan [5] proposed a threshold identity-based signcryption scheme in which only a threshold of users or more can jointly generate a signcryption ciphertext in the identity-based cryptosystem (IBC).

Attribute-based cryptosysm (ABC) extends IBC with flexibility and versatility. Specially, instead of an explicit identity, a number of attributes are used to identify a user. The private key of a user is associated with his/her attributes. A policy can be made so that only the users whose attributes meet the policy can generate a valid signature or decrypt a ciphertext. This feature makes ABC applicable to cloud applications where one may do not explicitly know who will access his/her data when they are outsourced to the cloud, but may know the attributes of the visitors. Then the data owner can make a policy, i.e., a subset of the attributes, so that later only the users meeting the policy can authenticate themselves to the cloud or can decrypt the encrypted data labelled with the policy. Although ABC is very versatile, few attribute-based signcryption schemes have been proposed [6],[7],[8],[9]. These schemes are either in the random oracle model is too weak to provide practical security, or in the standard model but at the cost of large signcryption ciphertext expansion and/or heavy computation burden. Another important issue in some applications is that these schemes do not protect the user's privacy, that is, his/her attributes may exposed to the adversary.

DOI 10.1109/CSCloud.2015.16

In this paper, we propose a TABSC scheme in the standard model without using random oracles. Our TABSC scheme simultaneously achieves the functionalities of the attribute-based encryption (ABE) scheme due to Sahai and Waters [10], and the attribute-based signature (ABS) schemes in [11],[12]. The security of our scheme does not rely on any random oracle. It is proven secure under the well-established Decisional Bilinear Diffie-Hellman (DBDH) and the standard Computational Diffie-Hellman (CDH) assumptions in the standard model. Compared with the state of the ABSC schemes, our scheme has desirable efficiency without relying on any random oracle. Compared to the only known TABSC construction [9] in the standard model, our scheme enjoys its faster secret key extraction, shorter ciphertext, without sacrificing security.

II. Related Work

The concept of signcryption has been realized in different settings. The early signcryption schemes based on integer factorization [2] or using RSA [3] are in the PKI setting. Subsequently, S. Sharmila [13] proposed a certificateless signcryption scheme secure in the random oracle model. Recently, Hu [14] proposed a certficateless signcryption scheme without using random oracles.

Sahai introduced the notion of fuzzy identity-based encryption (FIBE) in 2005 [10], only someone whose properties satisfying the specified access policy can decrypt the ciphertext. Similarly, in a fuzzy identity-based signature (FIBS), only someone whose properties satisfying the policy can complete the verification [15]. In FIBS and FIBE, a user is identified with a set of attributes, instead of his/her explicit identity information. This features also gives the notion of attribute-based cryptosystems. There are two kinds of ABE schemes, i.e., key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In the former, the access structure is associated with user's private key, ciphertext is labeled with attribute set and only the user whose attributes satisfied the access is able to decrypt [16]; while in CP- ABE, the access structure is associated with user's ciphertexts[17].

A number of attribute-based signcryption schemes have been proposed. Huang presented an ABSC scheme in the key-policy setting. The security of these attribute-based signcryption schemes rely on random oracles [18]. Recently, ciphertext-policy ABSC schemes have also been constructed [19],[20],[21]. Deng proposed a attribute-based signcryption with constant ciphertext [22]. With this technique, they also managed to reduce the number of pairing operations in signcryption. Threshold signcryption was first mentioned in Duan's scheme in 2004 [5]. The first signcryption scheme of threshold attribute-based in the standard model was mentioned by Martin and Reihaneh in 2010, which has a better application than the schemes in the random oracles [9]. The threshold mechanims was familiar to us because of its blind for user's attributes. Zhang presented a dynamic threshold attribute-based signcryption scheme in 2012 [23].

III. Preliminaries

Here we briefly discuss the basic tools needed for our scheme.

A. Bilinear Groups

Our schemes are built from bilinear maps. Let $\mathcal{G}(1^\ell)$ be a generator which takes as input a security parameter ℓ and outputs the description of the (symmetric) bilinear group of order p. We denote by $(p, \mathbf{G}, \mathbf{G_T}, \hat{e})$ the output of $\mathcal{G}(1^\ell)$, where $\mathbf{G}$ and $\mathbf{G_T}$ are two cyclic groups of prime order p and $\hat{e} : \mathbf{G} \times \mathbf{G} \to \mathbf{G_T}$ is an efficient map having the following properties:

- **Bilinearity**: for all $u, v \in \mathbf{G}$ and all $a, b \in \mathbf{Z_p}$, $\hat{e}(u^a, v^b) = \hat{e}(u^b, v^a) = \hat{e}(u, v)^{ab}$;
- **Non-degeneracy**: $\hat{e}(u, v) \neq 1$.

We say that $\mathbf{G}$ is a bilinear group if the group operations in $\mathbf{G}$ and the bilinear map $\hat{e} : \mathbf{G} \times \mathbf{G} \to \mathbf{G_T}$ can be efficiently computed. We note that we build our schemes on symmetric bilinear groups for simplicity, but it can be extended to asymmetric bilinear ones in a standard way

B. Complexity Assumptions

The security of our scheme depends on the well established DBDH assumption CDH assumption in blinear groups. The two assumptions are briefly reviewed.

Definition 1.(DBDH Assumption) Suppose that $e : \mathbf{G_1} \times \mathbf{G_1} \to \mathbf{G_2}$ is a bilinear map and g be a generator of $\mathbf{G_1}$. Let $u, v, w \in \mathbf{Z_p}$ and $h \in \mathbf{G_2}$ be chosen at random. The DBDH assumption states that no polynomial-time adversary is able to distinguish the tuple $(A = g^u, B = g^v, C = g^w, Z = e(g, g)^{uvw})$ from $(A = g^u, B = g^v, C = g^w, Z = h)$ with more than a negligible advantage.

Definition 2.(CDH Assumption) Let $\mathbf{G_1}$ be a group with the prime order p, g a generator of $\mathbf{G_1}$. The CDH assumption states that, given $g, g^{\cdot} g^v \in \mathbf{G_1}$ for unknown $u, v \in \mathbf{Z_p}$, no polynomial-time adversary can compute g^{uv}.

IV. Threshold Attribute-based Signcryption

A. Symstem Model

A TABSC scheme is comprised of four polynomial-time algorithms: Setup, KeyGeneration, Signcryption and Unsigncryption.

Setup. On input a security parameter 1^k, the private key generator (PKG) generates the system public parameters mpk and a master secret key msk.

KeyGeneration. Suppose that the attributes of sender is a set w_θ. Given w_θ, a threshold d, and the system master key msk, the PKG outputs a private key $sk_{w_\theta,d}$. Suppose that the attributes of the receiver is a set w_r. Given w_r, a threshold d, and the system master key msk, the PKG outputs the private key $sk_{w_r,d}$.

Signcryption. On input the public parameters mpk, a message m, the senders' signcryption attribute sets w_e and w_s, and the sender's secret key $sk_{w_s,d}$, $w_s \subset w_\theta$ and $|w_s| = d$, the Signcryption algorithm outputs a ciphertext C signcrypted with attributes w_e and w_s. Here, w_e is a set chosen by the sender for encryption, $w_s$is sender's attribute set.

Unsigncryption. Given the ciphertext C and receiver's private key $sk_{w_r,d}$, if $|w_e \cap w_r| \geq d$, the Unsigncryption algorithm can decrypt the signencrypted message and verify the sigcryption from the sender against w_s. Otherwise the algorithm returns $\perp$.

B. Security Definitions

Since a signcryption scheme performs encryption and signing simultaneously, the security of a signcryption scheme consists of message confidentiality and ciphertext unforgeability. As a TABSC scheme, we also need to consider the security property introduced by the threshold mechanism.

Message Confidentiality Definition. The message confidentiality is defined via the indistinguishability against a selective chosen ciphertext attack. It requires any polynomially time bounded adversary $\mathcal{A}$ has only negligible advantage in the following attack game played with a challenger.

- Initial: The adversary $\mathcal{A}$ picks up partial signcryption attribute set w_e^* and sends it to challenger.
- Setup: The challenger runs the Setup algorithm and sends the public parameters to adversary $\mathcal{A}$.

Phase 1: During this phase, the adversary makes a polynomial bounded number of the following queries to the challenger:

- KeyGeneration Queries: Adversary $\mathcal{A}$ chooses signcryption attribute sets w_e^*, w_s and a threshold d, the challenger computes $sk_{w_s,d} = KeyGeneration(mpk, msk, w_s, d)$, and sends it to $\mathcal{A}$; adversary $\mathcal{A}$ chooses an unsigncryption attribute set w_r and a threshold d, where $|w_e^* \cap w_r| < d$, the challenger computes $sk_{w_r,d} = KeyGeneration(mpk, msk, w_r, d)$, and sends it to $\mathcal{A}$.
- Signcryption Queries: Adversary $\mathcal{A}$ chooses a message m, a threshold d and signcryption attribute sets w_e^*, w_s, the challenger first computes $sk_{w_s,d}$ from KeyGeneration phase, then answers the query by performing the Signcryption algorithm, and sends it to $\mathcal{A}$.
- Unsigncryption Queries: Adversary $\mathcal{A}$ chooses a ciphertext C, a threshold d and unsigncryption attribute set w_r, the challenger first computers $sk_{w_r,d}$ from KeyGeneration phase, then answers the query by performing the Unsigncryption algorithm, and sends it to $\mathcal{A}$.

Challenge: Once the phase 1 is over, the adversary $\mathcal{A}$ generates two challenge messages m_0, m_1, and a sender's attribute set w_s^*. The challenger chooses a bit $b \in \{0, 1\}$ randomly, then computes the sigcryption key $sk_{w_s^*,d} = KeyGeneration(mpk, msk, w_s^*, d)$, and generates the challenge ciphertext

$$C^* = SignCryption(mpk, m_b, w_e^*, w_s^*, sk_{w_s^*,d})$$

Phase 2: Adversary $\mathcal{A}$ makes a polynomial bounded queries as in Phase 1. But the adversary is not allowed to make a KeyGeneration query for w_r when $|w_e^* \cap w_r| \geq d$ and Unsigncryption query for C associated with this w_r.

Guess: Eventually, adversary $\mathcal{A}$ outputs a bit b' and it wins in the game if $b' = b$.

The advantage of the adversary is defined as $Adv(\mathcal{A}) = |2\Pr[b' = b] - 1|$.

Definition 3. (Message Confidentiality) A TSBSC scheme has message confidentiality if for any polynomial-time adversary $\mathcal{A}$, its advantage $Adv(\mathcal{A})$ is negligible in the above game.

Ciphertext Unforgeability Definition. A TABSC scheme has existentially unforgeability against chosen message attacks, if there exists no polynomially time adversary $\mathcal{A}$ has a non-negligible advantage as in the following attack game with a challenger.

- Initial: The adversary $\mathcal{A}$ picks up partial signcryption attribute set w_s^*, here $|w_s^*| < d$ and sends it to challenger.
- Setup: The challenger runs Setup algorithm and sends the public parameters to adversary $\mathcal{A}$.

Query Phase: During this phase, the adversary makes the following polynomial bounded queries to the challenger:

- KeyGeneration Queries: Adversary $\mathcal{A}$ chooses a threshold d and signcryprion attribute sets w_e, w_s^*, the challenger computers $sk_{w_s^*,d} = KeyGeneration(mpk, msk, w_s^*, d)$, and sends it to $\mathcal{A}$. The adversary queries an unsigncryption attribute set w_r, and a threshold d, the challenger computers $sk_{w_r,d} = KeyGeneration(mpk, msk, w_r, d)$, and sends it to $\mathcal{A}$.
- Signcryption Queries: Adversary $\mathcal{A}$ chooses a message m, signcryption attribute sets w_e, w_s^* and a threshold d, the challenger first computes $sk_{w_s^*,d}$ from KeyGeneration phase, then answers the query by performing the Signcryption algorithm, and sends it to $\mathcal{A}$.

Forgery Phase: Eventually, adversary $\mathcal{A}$ outputs a forged ciphertext C^* and a partial signcryption attribute set w_e^*. The adversary wins if the ciphertext is valid, that is $Unsigncrypt(C^*, sk_{w_r,d}) = m \neq\perp$ where $sk_{w_r,d} = KeyGeneration(mpk, msk, w_r, d)$.

The advantage of the adversary is defined as $Adv(\mathcal{A}) = \Pr[win]$.

Definition 4.(Ciphertext Unforgeability) A TSBSC scheme has ciphertext unforgeability if for any polynomial-time adversary $\mathcal{A}$, its advantage $Adv(\mathcal{A})$ is negligible in the above game.

C. The proposed TABSC

In this part, we will specifically present our threshold attribute-based signcryption construction.

Let $\mathbf{G_1}, \mathbf{G_2}$ be two cyclic multiplicative groups of the same prime order p, and g is a generator of $\mathbf{G_1}$. Let $e : \mathbf{G_1} \times \mathbf{G_1} \rightarrow \mathbf{G_2}$ be the bilinear map. Let n be the length of the Signcryption attribute, and l_m be the message size.

Setup(n, d**).** Randomly picks a secret value $y \in \mathbf{Z_p}$, and an element $g_2 \in \mathbf{G_1}$, computes $g_1 = g^y$ and $Y = e(g_1, g_2)$. Next , chooses $h, t_1, t_2, \ldots, t_{n+1}$ at random from $\mathbf{G_1}$, chooses a collision-resistant hash function $H : \{0,1\}^* \rightarrow \{0,1\}^{l_m}$. Let N be the set $\{1, 2, ..., n+1\}$ and we define a function T as

$$T(x) = g_2^{x^n} \prod_{i=1}^{n+1} t_i^{\Delta_{i,N}(x)}$$

The public parameters of the system is $mpk = (g, g_1, g_2, t_1, t_2, ..., t_{n+1}, h, H, Y)$, the master key is $msk = y$.

KeyGeneration(mpk, msk, w, d**).** Randomly selects a $d-1$ degree polynomial $q(x)$ such that $q(0) = y$. Picks up $r_1, r_2, ..., r_n \in \mathbf{Z_p}$, and obtains the private key sets $sk_{w,d} = (D_i, d_i)_{i \in w}$ constructed by

$$D_i = g_2^{q(i)} T(i)^{r_i}, d_i = g^{r_i}$$

So, the private keys of sender and receiver can be computed by

$$sk_{w_s,d} = (D_i, d_i)_{i \in w_s} = (g_2^{q(i)T(i)^{r_i}}, g^{r_i})_{i \in w_s}$$

$$sk_{w_r,d} = (D_i, d_i)_{i \in w_r} = (g_2^{q(i)T(i)^{r_i}}, g^{r_i})_{i \in w_r}$$

Here, $|w_s| = d, w_s \subset w_\theta$.

Signcryption($mpk, m, w_e, w_s, sk_{w_s}, d$**).** Given the signcryption attribute sets w_e and w_s, the Signcryption algorithm chooses random $\alpha \in \mathbf{Z_p}$ and computes $\sigma_1 = g^\alpha$, $\sigma_2 = D_i \cdot (g_1^m h)^\alpha$ for $i \in w_s$, $\sigma_3 = g^{r_i}$ for $i \in w_s$, $\sigma_4 = (T(i))^\alpha$ for $i \in w_s$, $k_e = Y^\alpha$, $c = H(k_e) \oplus m$. The signcrypt of m is $C = \{w_e, w_s, \sigma_1, \sigma_2, \sigma_3, \sigma_4, c\}$.

Unsigncryption($mpk, C, w_r, sk_{w_r,d}$**).** Given the ciphertext $C = \{w_e, w_s, \sigma_1, \sigma_2, \sigma_3, \sigma_4, c\}$, the Unsigncrytion algorithm proceeds as following:

- Chooses a subset $D' \subset (w_r \cap w_e)$, and D' contains d attributes. If there is no such subset, outputs $\perp$.
- Computes $k_e = \prod_{i \in D'} \left(\frac{e(D_i, \sigma_1)}{e(d_i, \sigma_4)}\right)^{\Delta_{i,D'}(0)}$.
- Computes $m = H(k_e) \oplus c$.
- Tests the following equation
$$\prod_{i \in w_s} \left(\frac{e(\sigma_2, g)}{e(T(i), \sigma_3) e(g_1^m h, \sigma_1)}\right)^{\Delta_{i,w_s}(0)} = e(g_1, g_2) = Y$$
If the above equation is satisfied, we can judge that the message is exactly from the sender, then we accept the ciphertext C, otherwise, we reject it.

D. Correctness Analysis

The correctness of this construction is justified by the following equation.

Since $|w_s| = d$, so it is a d-element set, using Lagrange Interpolation, we can get

$$\begin{aligned}
&\prod_{i \in w_s} \left(\frac{e(\sigma_2, g)}{e(T(i), \sigma_3) e(g_1^m h, \sigma_1)}\right)^{\Delta_{i,w_s}(0)} \\
&= \prod_{i \in w_s} \left(\frac{e(g_2^{q(i)} T(i)^{r_i} (g_1^m h)^\alpha, g)}{e(T(i), g^{r_i}) e(g_1^m h, g^\alpha)}\right)^{\Delta_{i,w_s}(0)} \\
&= \prod_{i \in w_s} e\left(g_2^{q(i)}, g\right)^{\Delta_{i,w_s}(0)} = e(g_1, g_2) = Y
\end{aligned}$$

After the receiver obtains the ciphertext C, according to the C, he can calculate the private k_e.

$$\begin{aligned}
&\prod_{i \in D'} \left(\frac{e(D_i, \sigma_1)}{e(d_i, \sigma_4)}\right)^{\Delta_{i,D'}(0)} \\
&= \prod_{i \in D'} \left(\frac{e(g_2^{q(i)} T(i)^{r_i}, g^\alpha)}{e(g^{r_i}, T(i)^\alpha)}\right)^{\Delta_{i,D'}(0)} \\
&= \prod_{i \in D'} \left(e(g_2^{q(i)}, g^\alpha)\right)^{\Delta_{i,D'}(0)} = e(g_1, g_2)^\alpha = Y^\alpha
\end{aligned}$$

E. Security Analysis

Theorem 1.(IND-sTABSC-CCA secure) The proposed TABSC scheme satisfies message confidentiality against selective chosen ciphertext attacks under the Decisional Bilinear Diffie-Hellman (DBDH) assumption in the standard model.

We introduce two notations to simplify the description. $DBDH(t', \varepsilon')$ means that the adversary $\mathcal{A}$ has an advantage ε' in attacking the DBDH problem with the maximum time t'. We use $TABSC(t, q_K, q_S, q_{US}, \varepsilon)$ to denote that the adversary $\mathcal{A}$ has an advantage ε in attacking the $TABSC$ scheme at most q_k, q_s, q_{US} times queries to KeyGeneration, Signcryption, Unsigncryption phase respectively with the maximum time t.

Suppose that an adversary $\mathcal{A}$ has an advantage ε in attacking the proposed scheme, then we build an algorithm $\mathcal{T}$ to solve the DBDH problem. By algorithm $\mathcal{T}$, we get the relationship between ε and ε'. It means, if adversary $\mathcal{A}$ breaks the scheme with the advantage ε, then we can break the DBDH scheme with the advantage ε', but that is impossible, because the DBDH problem is hard, so the TABSC scheme is IND-sTABSC-CCA secure. The following is describing the algorithm $\mathcal{T}$ to create a scheme to solve the DBDH problem.

Proof. Assume the advantage of adversary $\mathcal{A}$ attacking the scheme is ε, we now build the algorithm $\mathcal{T}$ to solve the DBDH problem. It means, given (g, g^x, g^y, g^z, h), algorithm $\mathcal{T}$ can judge whether $h = e(g, g)^{xyz}$. According to the step of the security model definition, the algorithm $\mathcal{T}$ interacts with adversary $\mathcal{A}$ as follows.

- Initial: The adversary $\mathcal{A}$ picks up partial signcryption attribute set w_e^*, and sends w_e^* to $\mathcal{T}$.
- Setup: The algorithm $\mathcal{T}$ sets $g_1 = g^x, g_2 = g^y$ and sends the public parameters to adversary $\mathcal{A}$.

Phase 1: Adversary $\mathcal{A}$ makes a polynomial bounded queries to $\mathcal{T}$, the query process is equal to the security model definition phase. At the end of queries phase, adversary $\mathcal{A}$ generates two challenge message m_0^*, m_1^* and a attribute set of sender w_s^*.

Challenge: The algorithm $\mathcal{T}$ chooses a bit $b \in \{0, 1\}$ randomly, then it computes the sigcryption key $sk_{w_s^*,d} = KeyGeneration(mpk, msk, w_s^*, d)$, and generates the challenge ciphertext C^* as follows.

Choose random $\alpha \in \mathbf{Z_p}$. Compute $k_e^* = h^\alpha$, $c_b^* = H(k_e^*) \oplus m_b^*$, $\sigma_1^* = g^{z\alpha}$, $\sigma_2^* = D_i(g_1^m h)^\alpha$ for $i \in w_s^*$, $\sigma_3^* = g^{r_i}$ for $i \in w_s^*$, $\sigma_4^* = (T(i))^{z\alpha}$ for $i \in w_s^*$.

The algorithm $\mathcal{T}$ sends $C^* = \{w_e^*, w_s^*, \sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, c_b^*\}$ to the adversary $\mathcal{A}$. So, if $h = e(g, g)^{xyz}$, then C^* is a legitimate ciphertext from the adversary's perspective. The reason is that, suppose the attribute set of receiver is w_r, choose $D' \subset w_e^* \cap w_r$, then

$$k_e^* = \prod_{i \in D'} \left(\frac{e(D_i, \sigma_1)}{e(d_i, \sigma_4)} \right)^{\Delta_{i,D'}(0)}$$

$$= \prod_{i \in D'} \left(\frac{e(g_2^{q(i)} T(i)^{r_i}, g^{z\alpha})}{e(g^{r_i}, T(i)^{z\alpha})} \right)^{\Delta_{i,D'}(0)}$$

$$= \prod_{i \in D'} \left(e(g_2^{q(i)}, g^{z\alpha}) \right)^{\Delta_{i,D'}(0)} = e(g_1, g_2)^{z\alpha} = e(g, g)^{xyz\alpha}$$

Phase 2: As the security model definition phase.

Guess: Eventually, adversary $\mathcal{A}$ outputs a bit b' and it wins the game if $b' = b$.

Therefore, the algorithm $\mathcal{T}$ can know that $h = e(g, g)^{xyz}$ if the adversary $\mathcal{A}$ wins in the game, and then solve the DBDH problem.

According to the analysis in [10], to make sure that $\mathcal{A}$ wins the game, it needs $|w_r \cap w_e^*| \geq d$ for all arbitrary w_r which we choose, the probability is

$$p_1 = \frac{C_n^d + C_n^{d+1} + ... + C_n^n}{C_n^0 + C_n^1 + ... + C_n^n} = \frac{C_n^d + C_n^{d+1} + ... + C_n^n}{2^n} < 1$$

and the probability of $w_r \neq w_s^*$ is that

$$p_2 = 1 - \frac{q_k}{C_n^0 + C_n^1 + ... + C_n^n} = 1 - \frac{q_k}{2^n}$$

In addition, there are q_K, q_S, q_{US} times queries to Key-Generation, Signcryption, Unsigncryption phase respectively with advantage ε. Therefore, we could get the advantage ε' of solving the DBDH problem by algorithm $\mathcal{T}$.

$$\varepsilon' = \frac{\varepsilon \cdot p_1 p_2}{q_K q_S q_{US}} < \frac{\varepsilon \cdot (1 - \frac{q_k}{2^n})}{q_K q_S q_{US}}$$

So, because of the hardness of solving the DBDH problem, we get the conclusion that our scheme possesses the message confidentiality.

Theorem 2.(EUF-TABSC-CMA secure) This TABSC scheme has existentially unforgeability against chosen message attacks under the modified Computational Diffie-Hellman assumption. That is, there is no polynomially bounded adversary can attack the scheme with a non-negligible advantage.

We use $CDH(t', \varepsilon')$ to denote that the adversary $\mathcal{A}$ has an advantage ε' in attacking the Computational Diffie-Hellman problem with the maximum time t'. We use $TASBC(t, q_K, q_S, q_{US}, \varepsilon)$ to represent that the adversary $\mathcal{A}$ has an advantage ε in attacking the $TASBC$ scheme at most q_K, q_S, q_{US} times queries to KeyGeneration, Signcryption, Unsigncryption phase respectively with the maximum time t.

Suppose that an adversary $\mathcal{A}$ has an advantage ε in attacking the proposed scheme, then we intended to build an algorithm $\mathcal{F}$ to solve the CDH problem. By algorithm $\mathcal{F}$, we get the relationship between ε and ε'. It means, if adversary $\mathcal{A}$ breaks the scheme with the advantage ε, then we can break the CDH scheme with the advantage ε', but that is impossible, because the CDH problem is hard, so the TABSC protocol is EUF-TABSC-CMA secure. The following is describing the algorithm $\mathcal{F}$ to create a scheme to solve the CDH problem.

Proof. Assume the advantage of adversary $\mathcal{A}$ attacking the scheme is ε, we now build an algorithm $\mathcal{F}$ to solve the CDH problem. It means, given (g, g^x, g^y) , the algorithm $\mathcal{F}$ can compute g^{xy}. According to the security definition, the algorithm $\mathcal{F}$ interacts with the adversary $\mathcal{A}$ as follows.

- Initial: The adversary $\mathcal{A}$ picks up partial signcryption attribute set w_s^*, and sends w_s^* to $\mathcal{F}$.
- Setup: The algorithm $\mathcal{F}$ sets $g_1 = g^x, g_2 = g^y$. Then $\mathcal{F}$ chooses two n degree polynomial functions $f(x)$ and $v(x)$ randomly, where $v(x) = -x^n$ if $x \in w_s^*$, and $v(x) \neq -x^n$ for other x. Then, $\mathcal{F}$ sets $t_i = g_2^{v(i)} g^{f(x)}$ for $i = 1, ..., n+1$. Now, we implicitly have $T(x) = g_2^{x^n + v(x)} g^{f(x)}$, since

$$T(x) = g_2^{x^n} \prod_{i=1}^{n+1} t_i^{\Delta_{i,N}(x)} = g_2^{x^n} \prod_{i=1}^{n+1} \left(g_2^{v(i)} g^{f(i)} \right)^{\Delta_{i,N}(x)}$$

$$= g_2^{x^n} g_2^{\sum_{i=1}^{n+1} v(x)\Delta_{i,N}(x)} g^{\sum_{i=1}^{n+1} f(x)\Delta_{i,N}(x)}$$

$$= g_2^{x^n+v(x)} g^{f(x)}$$

Then $\mathcal{F}$ chooses γ randomly in $\mathbf{Z_p}$ and sets $h = g_1^{-m} \cdot g^{\gamma}$. Finally, the algorithm $\mathcal{F}$ sends $\mathcal{A}$ the public key $mpk = (g, g_1, g_2, t_1, t_2, ..., t_{n+1}, h, H, Y)$.

Query Phase: Adversary $\mathcal{A}$ makes a polynomial bounded queries to $\mathcal{F}$, the query process is equal to the security model definition phase.

Forgery Phase: As the security model definition phase.

Finally, the adversary $\mathcal{A}$ outputs a forgery $C^* = (w_e^*, w_s^*, \sigma_1, \sigma_2, \sigma_3, \sigma_4, c)$ for the verification. According to the Unsigncryption phase, we have

$$\prod_{i \in w_s^*} \left(\frac{e(\sigma_2, g)}{e(T(i), \sigma_3) e(g_1^m h, \sigma_1)} \right)^{\Delta_{i,w_s^*}(x)} = e(g_1, g_2)$$

Accordingly, C^* is a valid converted Signcrytion result. Now, note that $h = g_1^{-m} \cdot g^{\gamma}$ and for $x \in w_s^*$, $T(i) = g_2^{x^n+v(x)} g^{f(i)} = g^{f(i)}$.

The equation above can rewritten in the following way:

$$\prod_{i \in w_s^*} \left(\frac{e(\sigma_2, g)}{e(T(i), \sigma_3) e(g_1^m h, \sigma_1)} \right)^{\Delta_{i,w_s^*(0)}}$$

$$= \prod_{i \in w_s^*} \left(\frac{e(\sigma_2, g)}{e(\sigma_3^{f(i)}, g) e(\sigma_1^{\gamma}, g)} \right)^{\Delta_{i,w_s^*(0)}}$$

$$= \prod_{i \in w_s^*} e\left(\frac{\sigma_2}{\sigma_3^{f(i)} \sigma_1^{\gamma}}, g \right)^{\Delta_{i,w_s^*(0)}}$$

Note that

$$\prod_{i \in w_s^*} \left(\frac{e(\sigma_2, g)}{e(T(i), \sigma_3) e(g_1^m h, \sigma_1)} \right)^{\Delta_{i,w_s^*(0)}} = e(g_1, g_2) = e(g, g^{xy})$$

We have

$$\prod_{i \in w_s^*} \left(\frac{\sigma_2}{\sigma_3^{f(i)} \sigma_1^{\gamma}} \right)^{\Delta_{i,w_s^*(0)}} = g^{xy}$$

Therefore, the algorithm $\mathcal{F}$ could compute g^{xy} and solve the CDH problem. According to the analysis in [11], to make sure that $|w_s^*| = d$, the probability is

$$p_1 = \frac{C_n^d}{C_n^0 + C_n^1 + ... + C_n^n} = \frac{n!}{(n-d)!d!2^n}$$

because the adversary $\mathcal{A}$ can't issue a Signcryption query on (m, w_e^*, w_s^*), the probability is

$$p_2 = 1 - \frac{q_S}{C_n^0 + C_n^1 + ... + C_n^n} = 1 - \frac{q_S}{2^n}$$

In addition, there are q_K, q_S, q_{US} times queries to Key-Generation, Signcryption, Unsigncryption phase respectively with advantage ε. Therefore, we could get the advantage ε' of solving the CDH problem by algorithm $\mathcal{F}$.

$$\varepsilon' = \frac{\varepsilon \cdot p_1 p_2}{q_K q_S q_{US}} = \frac{\varepsilon \cdot n!(1 - \frac{q_S}{2^n})}{(n-d)!d!2^n q_K q_S q_{US}}$$

For the hardness of solving the CDH problem, we get the conclusion that our scheme possesses the ciphertext unforgeability.

Table I
COMPARISON WITH RELATED WORKS

Protocol	M. $\mathbf{G_1}$	K.E	Sign Dim	CCA	CMA
[10]+[8]	$n+7$	$4n$	$(4n+5)\lvert\mathbf{G_1}\rvert + \lvert\mathbf{G_2}\rvert$	NO	YES
[9]	$n+4$	$5n$	$l_m + 2(n+3)\lvert\mathbf{G_1}\rvert + \tau$	YES	YES
Ours	$n+4$	$4n$	$l_m + 2(n+1)\lvert\mathbf{G_1}\rvert$	YES	YES

F. Efficiency Analysis

Because the signcryption we proposed is committed to solve the long-winded ciphertext problem existed in Martin's scheme, so here we compare our scheme's efficiency against Martin's scheme. According to the analysis in [9], we add the ABE and ABS schemes at the same time. The comparison is in the view of system group multiplication, user private key exponentiation, signcryptext dimensions and security concept. The result is given in table 1 below.

Here, $|\mathbf{G_1}|$ and $|\mathbf{G_2}|$ denote the size of group $\mathbf{G_1}$ and $\mathbf{G_2}$ emerged in the construction respectively, n is the maximum attribute set's size, l_m is the messages' size, τ is the size of a tag appeared in Martin's scheme. M.$\mathbf{G_1}$ represents the multiplication in $\mathbf{G_1}$, K.E represents users' private key exponentiation, Sign Dim represents signcryptext dimensions.

From this table, we can get that, whether system group multiplication, user private key exponentiation, or signcryptext dimensions, our scheme is more efficient than others.

V. CONCLUSION

In order to overcome the disadvantages of traditional public key infrastructure certificate management, and improve the security of attributed-based signcryption, this paper proposes an efficient threshold attributed-based signcryption scheme in the standard model by using bilinear on technology, analyzes the security of the program by establishing a simulate algorithm to proof the scheme satisfies message confidentiality and unforgeability based on the DBDH and CDH assumption, and gives the efficiency analysis at last. Through the above content, we can get that this proposed threshold attribute-based signcryption is an efficient, secure and wide applicable protocol, and has a certain theoretical and practical value.

ACKNOWLEDGMENT

This work is supported by the National Nature Science Foundation of China under Grant 61272091, the National

Nature Science Foundation of Shandong Province under Grant ZR2012FM005.

References

[1] Y. Zheng. Digital signcryption or how to achieve cost (signature & encryption). Cost (signature) + cost (encryption). Advances in Cryptology-CRYPTO'97, LNCS 1294, Springer-Verlag, 1997. 165-179.

[2] R. Steinfeld, Y. Zheng. A signcryption scheme based on integer factorization. Information Security Workshop-ISW 2000, LNCS 1975, Springer-Verlag, 2000. 308-322.

[3] J. Malone-Lee and W. Mao, Two birds one stone: signcryption using RSA. Topics in Cryptology-CT-RSA 2003, LNCS 2612, Springer- Verlag, 2003. 211-226.

[4] J. Malone-Lee Identity based signcryption. IACR Cryptology ePrint Archive, Report, 2002, 098, 2002.

[5] S. Duan, Z. Cao, and R. Lu. Robust ID-based threshold signcryption scheme from pairings. In Proc. 2004 International Conference on Information security, pp. 33-37, Shanghai, China, 2004.

[6] M. G. Muniz and P. Laud. Strong forward security in identity-based signcryption. IACR Cryptology ePrint Archive, Report, 2011/156,2011.

[7] H. Wang. Unrestricted identity-based aggregate signcryption in the standard model from multilinear maps. Cryptology ePrint Archive, 2014/141, 2014.

[8] S. F. Shahandashti, R. Safavi-Naini, Threshold attribute-based signatures and their application to anonymous credential systems[C]. Springer, Heidelberg, 2009.

[9] M. Gagne, S. Narayan, and R. Safavi-Naini. Threshold attribute-based signcryption. SCN 2010, LNCS 6280, pp. 154-171, 2010.

[10] A. Sahai and B. Waters. Fuzzy identity-based encryption. EUROCRYPT 2005, LNCS 3494, pp. 457-473, 2005.

[11] J. Li and K.Kim. Attribute-based ring signatures. IACR Cryptology ePrint Archive, Report, 2008/394, 2008.

[12] J. Li and M. H. Au. Attribute-based signature and its applications. Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, Beijing, China, Apr. 13-16, 2010: 60-69.

[13] S. S. D. Selvi, S. S. Vivek and C. P. Rangan. Certficateless KEM and hybrid signcryption schemes revisited. IACR Cryptology ePrint Archive, Report, 2009/462, 2009.

[14] H. Xiong. Toward certificateless signcryption scheme without random oracles. IACR Cryptology ePrint Archive, 2014/162, 2014.

[15] Piyi Yang, Zhenfu Cao and Xiaolei Dong. Fuzzy Identity-Based Signature. IACR Cryptology ePrint Archive, 2008.

[16] V.Goyal, O.Pandey, A.Sahai and B.Water. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. Cryptology ePrint Archive, Report, 2006/309, 2006.

[17] John B, Amit S and Brent W. Ciphertext-policy attribute-based encryption. Cryptology ePrint Archive, Report, 2008, 290, 2008.

[18] J. Kar. Provably secure identity-based aggregate signcryption scheme in random oracles.IACR Cryptology ePrint Archive, Report, 2013/037, 2013.

[19] C. Hu, N. Zhang and H. Li. Body area network security: A fuzzy attribute-based signcryption scheme. IEEE journal on selected areas in communications. vol.31, no.9, September 2013.

[20] C. Zhou. Cryptanalysis and Improvement of a Multi-Receiver Generalized Signcryption Scheme. IACR Cryptology ePrint Archive, Report, 2012/638, 2012.

[21] P. Kushwah and S. Lal. Identity based signcryption schemes without random oracles. IACR Cryptology ePrint Archive, Report, 2011/372, 2011.

[22] L. Deng, S. Li and X. Wang. Attribute based signcryption with constant ciphertext length. Journal of Discrete Mathematical Sciences and Cryptography. 07 Mar, 2014.

[23] G. Zhang, X. Fu, C. Ma. A dynamic threshold attributes-based signcryption scheme. Journal of Electronics & Information Technology. vol.34, no.11. Nov. 2012.