An efficient and secure attribute based signcryption scheme with LSSS access structure

Hanshu Hong and Zhixin Sun*

Abstract
Attribute based encryption (ABE) and attribute based signature (ABS) provide flexible access control with authentication for data sharing between users, but realizing both functions will bring about too much computation burden. In this paper, we combine the advantages of CP-ABE with ABS and propose a ciphertext policy attribute based signcryption scheme. In our scheme, only legal receivers can decrypt the ciphertext and verify the signature signed by data owner. Furthermore, we use linear secret sharing scheme instead of tree structure to avoid the frequent calls of recursive algorithm. By security and performance analysis, we prove that our scheme is secure as well as gains higher efficiency.

Keywords: Attribute based, Signcryption, LSSS structure, Security

Background
The notion of attribute based encryption (ABE) was first proposed by Sahai and Waters (2005). Since then, many typical ABE (Goyal et al. 2006; Waters 2011; Lewko et al. 2010; Goyal et al. 2008; Tian and Peng 2014) schemes have been proposed. In ABE, user’s access privileges are described by a set of attributes instead of a single identity string. A user can get access to the ciphertext only if his attributes satisfy with the policy which is set by the data owner. Due to its capability of providing fine-grained and flexible access control, ABE appears to be a promising tool for data encryption and data sharing between users. Attribute based signature (ABS) has been developed as a primitive to solve the data authentication problem of ABE, which was first introduced (Guo and Zeng 2008) in 2008. In ABS mechanisms (Maji et al. 2011), a signer can sign a message with the private key component corresponds with the attributes he processes. The signature can be verified to a certain set of attributes or an attribute access structure of which the data owner claims.

The notion of signcryption (Zheng 1997; Lim and Lee 1998; Tan 2008; Selvi et al. 2008) can be introduced to attribute based cryptography to present attribute based signcryption schemes. Signcryption (Paulo et al. 2005; Li and Khan 2012) is a single logical step to complete the function of both signature and encryption at the same time, thus it achieves better efficiency than the traditional sign-then-encryption method. However, research on attribute based signcryption has not been received much attention from
academia. Wang and Huang (2011) proposed a signcryption scheme from pairings. Their scheme provides the same functions of encryption and authentication and is proved to be more efficient than the simply combination of "CP-ABE + CP-ABS". Hu and Zhang (2013) proposed a fuzzy attribute based signcryption and apply it in the BAN (Body area network). Their scheme is a novel security mechanism and achieves outstand performance. However, the proposed (Wang and Huang 2011; Hu and Zhang 2013) schemes are based on the tree structure (Bethencourt et al. 2007) and threshold structure, which need frequent calls of recursive algorithm for the purpose of recovering the secret encryption component. Thus this will bring about external computation overhead.

To better improve the efficiency of attribute based signcryption scheme, in this paper, we propose an improved ciphertext policy attribute based signcryption scheme. We use LSSS structure (Beimel 1996) instead of access tree structure to avoid the frequent calls of recursive algorithm. By security and performance analysis, we prove that our scheme is secure as well as achieves higher efficiency.

**Preliminaries**

**Bilinear pairings**

Let $G_1$ and $G_2$ be two cyclic groups of prime order $q$. Let $g$ be a generator of $G_1$. A bilinear pairing $\hat{e}: G_1 \times G_1 \rightarrow G_2$ has these features:

- **Bilinearity**: for $a, b \in \mathbb{Z}_q$, we have $\hat{e}(g^a, g^b) = \hat{e}(g, g)^{ab}$.
- **Non-degeneracy**: for any $g \in G_1$, $\hat{e}(g, g) \neq 1$.
- **Computability**: the value of $\hat{e}(u, v)$ can be computed for any $u, v \in G_1$.

**Hardness assumption**

**Discrete logarithm assumption (DL)**

Given $P, Q \in G_1$, no probabilistic polynomial-time (PPT) algorithm can find an integer $n \in \mathbb{Z}_q^*$ such that $Q = P^n$ with non-negligible probability.

**Decision bilinear Diffie–Hellman problem (DBDH)**

For $a, b, c, z \in \mathbb{Z}_q^*$, given $\{g, g^a, g^b, g^c, z\}$, no probabilistic polynomial-time (PPT) algorithm can distinguish the following tuples $\{A = g^a, B = g^b, C = g^c, \hat{e}(g, g)^{abc}\}$ and $\{A = g^a, B = g^b, C = g^c, \hat{e}(g, g)^{z}\}$ with non-negligible probability.

**Our model and assumptions**

**Formulized definitions of our scheme**

Our scheme consists of the following algorithms:

**Setup** On input security parameter, it returns the system public parameter $PK$ and master key $MK$. $PK$ is shared by users while $MK$ is kept private by the private key generator.

**Private Key generation** On input the system public key $PK$, the master key $MK$, and an attribute set $\{A_i\}$, private key generator (PKG) outputs $D_i$ as the user’s attribute private key. To distinguish the role of signers and receivers, in this paper, we define the private key of signer as $D_s$ while the private key of receiver as $D_r$. 


Signcrypt This algorithm is run by a signer which takes the systems public parameter $PK$, a plaintext $M$, signer’s private key $D_s$ and an access structure as input. Then it outputs the ciphertext $CT\{U, V, E\}$.

De-signcrypt This algorithm is run by the receiver. The algorithm takes as input the ciphertext $CT\{U, V, E\}$ and the receiver’s private key $D_r$, it outputs either the plaintext $M$ or the reject symbol $\perp$.

Security model

**Definition 1** Our scheme has the essential confidentiality under chosen plaintext attack in selected model if no Adversary has non-negligible advantage in the challenge game.

**Setup**: Adversary claims a challenging attribute set $\gamma$. Challenger runs setup algorithm to obtain $PK$. It sends $PK$ to Adversary.

Adversary may make the following queries to Challenger.

**Private key generation query**: Adversary can request the private key of an attribute set (expect for the challenging attribute set).

**Challenge**: Adversary chooses two plaintexts $M_0$ and $M_1$. Challenger chooses $\mu \in \{0, 1\}$ randomly and calculates $C^* = \text{Signcrypt}\{PK, M_\mu, D_s\}$. Then Challenger sends the result back to Adversary.

Adversary cannot ask Challenger for Private key generation query for the challenging attribute set $\gamma$.

Adversary outputs a value $\mu^*$ as a conjecture of $\mu$. If $\mu^* = \mu$ then Adversary wins the game. Denote $\left| \Pr [\mu^* = \mu] - \frac{1}{2} \right|$ to be the advantage of Adversary.

**Definition 2** Our scheme has the existential unforgeability under chosen message attack in the selective model if no Adversary has non-negligible advantage in the challenge game.

**Setup**: Adversary claims a challenging attribute set $\gamma$. Challenger takes a security parameter and runs setup procedure to obtain the system parameters. It sends the $PK$ to Adversary.

**Private key generation query**: Adversary can request the private key of an attribute set (expect for the challenging attribute set).

**Signcrypt query**: Adversary chooses an attribute set $\{A_i\}$, an access structure, a plaintext $M$. Challenger calculates $D_s$ and runs the signcrypt procedure to calculate the ciphertext $CT = \text{Signcrypt}\{PK, M, D_s, \gamma\}$. After then, Challenger sends $CT$ to Adversary.

**Challenge**: Adversary computes a 3-tuple $CT^*\{U, V, E\}$, while $CT^*\{U, V, E\}$ was not from a signcrypt query.

Challenger de-signcrypts the ciphertext by running the $De$-signcrypt $\{PK, CT^*, D_r\}$.

Adversary wins the game if the output of De-signcrypt is not $\perp$.

Denote $\text{Adv}(A) = \left| \Pr [\text{Result} = M] \right|$ to be the advantage of Adversary.
Our contributions to attribute based signcryption scheme

Let $G_1$ and $G_2$ be two cyclic groups of prime order $p$, while $g$ is the generator of $G_1$. Let $\hat{e} : G_1 \times G_1 \rightarrow G_2$ be a bilinear pairing. Define 2 functions: $H_1, H_2$. The function $H_1$ associates attributes to rows of access Matrix (the number of rows $\in Z_p^n$). $H_2 : \{0,1\}^n \rightarrow Z_p^*$

Setup PKG randomly chooses $\alpha_i \in Z_p^*$ for each attribute $i$ in the system. Besides, PKG chooses another secret number $\alpha \in Z_p^*$. The system outputs the system master keys $\{g^\alpha, \alpha_i\}$, public parameters $\{\hat{e}(g,g)^{\alpha}, \hat{e}(g,g)^{\alpha H_1(i)}, H_1, H_2, G_1, G_2, p, g\}$.

Private key generation For signer’s attribute set $\{A_i\}$, PKG chooses $u \in Z_p^*$ and calculates its private key $\{D_{s,1}, D_{s,2}, D_{s,3}\} = \{g^{u+\alpha_i H_1(i)}, g^{u+\alpha_i} \cdot \hat{e}(g,g)^u\}$. Likewise, for receiver’s attribute set $\{A_i\}$ PKG chooses $h \in Z_p^*$ calculates its private key $\{D_{r,1}, D_{r,2}, D_{r,3}\} = \{g^{\alpha_i H_1(i)+h}, g^{\alpha_i+h} \cdot \hat{e}(g,g)^h\}$. PKG transfers the private key to each user through secure channels.

Signcrypt Signer firstly picks $x \in Z_p^*$ and a LSSS access structure Matrix, then chooses random vector $\vec{v} = (x, v_{r_1}, v_{r_2}, \ldots, v_{r_n}) \in Z_p^n$. Let $\vec{v}_i = \hat{v} \cdot Matrix_i$. ($Matrix_i$ stands for the $i$th row of the corresponding Matrix). Finally, signer randomly picks $t_i \in Z_p^*$ and calculates the signcryption information:

$$U = \{\hat{e}(g,g) \sum_{j \in S} \alpha_i H_1(i) \cdot x\}$$

$$t = H_2(U||M)$$

$$V : \{v_1 = \prod_{j \in S} D_{s,1}^{x+t}, v_2 = \prod_{j \in S} D_{s,3}^{x+t}\}$$

$$E : \{C_0 = M \hat{e}(g,g)^{\alpha x}, C_1 = g^x, C_{2,i} = \hat{e}(g,g)^{-\alpha_i H_1(i) \cdot \vec{v}_i}, C_{3,i} = g^{\vec{v}_i}\}$$  \hspace{1cm} (1)

Signer sends $CT = \{U, V, E\}$ to the receiver.

De-signcrypt Let $\{\omega_i \in Z_p\}_{i \in I}$ be a set of constants such that if $\{\vec{v}_i\}$ are valid shares of secret $x$ according to $Matrix$, then $\sum_{i \in I} \omega_i \vec{v}_i = x$. Receiver calculates $M^*$ as follows:

$$M^* = \frac{C_0}{\prod_{i \in I} (\hat{e}(C_3, D_{r,1}) \cdot C_{2,i})^{-\alpha_i} \cdot \hat{e}(C_1, D_{r,2})}$$  \hspace{1cm} (2)

Then, receiver verifies if

$$\hat{e}(v_1, g) = U \cdot v_2 \cdot \hat{e}(g,g) \sum_{j \in S} \alpha_i H_1(i) \cdot t$$  \hspace{1cm} (3)

If Eq. (3) holds then the algorithm outputs plaintext $M$ with the signature. If not, it outputs reject “\(\perp\)”.

Correctness proof:
The aim of simulator is to output a value in the following settings:

Phase 1
The simulator simulates the role of Challenger. Let \( M \) be two cyclic groups of prime order \( p \), while \( g \) is the generator of \( G_1 \). Let \( \hat{e} : G_1 \times G_1 \rightarrow G_2 \) be a bilinear pairing. Define 2 functions: \( H_1 \) associates attributes to rows of access Matrix, \( H_2 : \{0, 1\}^* \rightarrow \mathbb{Z}_p^* \).

**Theorem 1** If Adversary can break our scheme under chosen plaintext attack in the selective model, then a simulator can solve the DBDH problem.

**Proof** In the challenge game, if there exists an Adversary which has advantage \( \varepsilon \) in attacking our scheme, there exists a simulator solving the DBDH problem with an advantage of \( \varepsilon/2 \).

The simulator is constructed as follows:

**Phase 1 Setup:** Adversary claims a challenging attribute set \( \gamma \). Challenger defines a set of attributes \( \{A_i\} \). Let \( G_1 \) and \( G_2 \) be two cyclic groups of prime order \( p \), while \( g \) is the generator of \( G_1 \). Let \( \hat{e} : G_1 \times G_1 \rightarrow G_2 \) be a bilinear pairing. Define 2 functions: \( H_1 \) associates attributes to rows of access Matrix, \( H_2 : \{0, 1\}^* \rightarrow \mathbb{Z}_p^* \).

Challenger randomly chooses \( \mu \in \{0, 1\} \), \( a, b, c \in \mathbb{Z}_p^* \).

Let

\[
\begin{align*}
(A, B, C, Z) &= \left( g^a, g^b, g^c, \hat{e}(g, g)^{abc} \right) \quad \text{if } \mu = 0 \\
(A, B, C, Z) &= \left( g^a, g^b, g^c, \hat{e}(g, g)^3 \right) \quad \text{if } \mu = 1
\end{align*}
\]

The aim of simulator is to output a value \( \mu^* \) as a conjecture of \( \mu \).

The simulator simulates the role of Challenger and runs Adversary's algorithm as subprogram.

**Phase 2 Queries:**
Adversary asks for private key for attributes \( A_i \). Simulator picks \( u, y, a_i \in \mathbb{Z}_p^* \) and makes the following settings:

\[
M^* = \prod_{i \in \gamma} \left( \hat{e}(C_{3,i}, D_{r,1}) \cdot C_{2,i} \right)^{a_i} \cdot \hat{e}(C_{1, D_{r,2}}) = \prod_{i \in \gamma} \left( \hat{e}(g^{a_i H_1(i) + u}, g)\hat{e}(g, g)^{a_i H_1(i) + u} \right)^{a_i}
\]

\[
\hat{e}(g, g)^{a_i} \cdot \hat{e}(g, g)^{M_{\mu}} = \hat{e}(g, g)^{\sum_{i \in \gamma} a_i}
\]

\[
t = H_3(U || |M|
\]

\[
\hat{e}(v_1, g) = \hat{e} \left( g^{\sum_{j \in \gamma} H_1(i)(x+t)}, g^s \right) = \hat{e}(g, g)^{\sum_{j \in \gamma} a_i H_1(i)(x+t)} \cdot \hat{e}(g, g)^{a_i H_1(i) + u(x+t)}
\]

\[
= \hat{e}(g, g)^{\sum_{j \in \gamma} a_i H_1(i)} \cdot \hat{e}(g, g)^{a_i H_1(i) + u(x+t)}
\]

\[
= \hat{e}(g, g)^{\sum_{j \in \gamma} a_i H_1(i)} \cdot \hat{e}(g, g)^{a_i H_1(i) + u(x+t)}
\]

\[
= U \cdot v_2 \cdot \hat{e}(g, g)^{\sum_{j \in \gamma} a_i H_1(i)}
\]

\[
(4)
\]

\[
(5)
\]
The queries like Phase 2 can be asked by Adversary for a bounded times.

Phase 3 Challenge:
Adversary picks plaintext $M_0, M_1$ and a challenging LSSS containing attribute set $\gamma$. Simulator chooses $\mu \in \{0, 1\}$ and calculates $CT_\mu = \text{Signcrypt}\{PK, M_\mu, D_\sigma\}$.
Simulator sends $CT_\sigma$ to Adversary.

Let $x = c$, according to the previous setting in the Setup phase:

$$CT_\mu : \begin{cases} 
C_0 = \hat{M} \hat{e}(g, g)^{abc}, & \text{if } \mu = 0 \\
C_1 = \hat{g}^x, C_{2i} = \hat{e}(g, g)^{-a_i H_1(j) \lambda_i}, C_{3i} = g^{\lambda_i} 
\end{cases}$$

(7)

Adversary outputs a value $\mu^*$ as a guess of $\mu$. If $\mu^* = \mu$ Adversary wins the game.

Then we will discuss simulator’s advantage in distinguishing the following two tuples $
\{A = g^a, B = g^b, C = \hat{g}^c, \hat{e}(g, g)^{abc}\}$ and $\{A = g^a, B = g^b, C = \hat{g}^c, \hat{e}(g, g)^{z}\}$.

When $\mu = 1$, $E$ is an illegal ciphertext and Adversary cannot acquire useful information of $\sigma$.

$$\Pr(\mu^* \neq \mu | \mu = 1) = \frac{1}{2}$$

(8)

Since when $\mu^* \neq \mu$, the simulator outputs $\mu = 1$, so:

$$\Pr(\mu^* = \mu | \mu = 1) = \frac{1}{2}$$

(9)

When $\mu = 0$, $E$ is a legal ciphertext. According to the assumption, Adversary has an advantage $\varepsilon$.

$$\Pr(\mu^* = \mu | \mu = 0) = \frac{1}{2} + \varepsilon$$

(10)

Since when $\mu^* = \mu$ the simulator outputs $\mu = 1$, so

$$\Pr(\mu^* = \mu | \mu = 0) = \frac{1}{2} + \varepsilon$$

(11)

As is mentioned above, the advantage of simulator is

$$\frac{1}{2} \Pr(\mu^* = \mu | \mu = 0) + \frac{1}{2} \Pr(\mu^* = \mu | \mu = 1) - \frac{1}{2}$$

$$= \frac{1}{2} \left( \frac{1}{2} + \varepsilon \right) + \frac{1}{2} \times \frac{1}{2} - \frac{1}{2}$$

$$= \varepsilon$$

(12)
Unforgeability

**Theorem 2** If an Adversary can break our scheme chosen message attack in the selective model, then it can be constructed that a simulator with a non-negligible advantage solves the DBDH problem.

**Proof** In the challenge game, if there exists an Adversary which has advantage \( \varepsilon \) in forging a legal ciphertext, there exists a simulator which can solve the DBDH problem with an advantage of \( \varepsilon/2 \).

Phase 1 Setup:

Adversary claims a challenging attribute set \( \gamma \). Challenger defines a set of attributes \( \{A_i\} \);
Let \( G_1 \) and \( G_2 \) be two cyclic groups of prime order \( p \), while \( g \) is the generator of \( G_1 \). Let \( \hat{\varepsilon} : G_1 \times G_1 \rightarrow G_2 \) be a bilinear pairing. Define 2 functions: \( H_1 \) associates attributes to rows of access Matrix, \( H_2 : \{0, 1\}^* \rightarrow Z_p^* \).

Challenger randomly chooses \( b \in \{0, 1\}, a, b, c \in Z_p^* \):

\[
\begin{align*}
(A, B, C, Z) &= \begin{cases} 
(g^a, g^b, g^c, \hat{\varepsilon}(g, g)^{abc}) & \text{if } \mu = 0 \\
(g^a, g^b, g^c, \hat{\varepsilon}(g, g)^z) & \text{if } \mu = 1
\end{cases}
\end{align*}
\]

Let \( \{D_{s,1}, D_{s,2}, D_{s,3}\} \)

The aim of simulator is to output a value \( \mu^* \) as a conjecture of \( \mu \).

Phase 2 Queries:

**Private key generation query**: Adversary chooses a set of attributes \( \{A_i\} \), a plaintext \( M \) and a LSSS. Simulator picks \( u, y, a_i, b_i, y_i \in Z_p^* \) and makes the following settings:

\[
D_{s,1} = g^u + a_i b_i H_1(i), \quad g^{ab+u} \hat{\varepsilon}(g, g)^u, \quad \text{if } A_i \in \gamma
\]

\[
D_{s,2} = g^{u+y_i H_1(i)} g^{\gamma+u} \hat{\varepsilon}(g, g)^u, \quad \text{if } A_i \notin \gamma
\]

(13)

**Signcrypt query**: Adversary picks a message \( M \) for signcrypt query. Simulator runs algorithm Signcrypt \( \{M, D_s, PK\} \) and returns the result \( CT = \{U, V, E\} \) to Adversary.

The queries like Phase 2 can be asked by Adversary for a bounded times.

Phase 3 Challenge:

Adversary outputs a ciphertext \( CT^* = \{U^*, V^*, E^*\} \). Adversary makes the forges the illegal ciphertext as the following process:

\[
U^* = \begin{cases} 
\hat{\varepsilon}(g, g)^{a_i b_i H_1(i) - x}, & A_i \in \gamma \\
\hat{\varepsilon}(g, g)^{y_i H_1(i) - x}, & A_i \notin \gamma
\end{cases}
\]

\[
t = H_2(U^* || M)
\]

\[
V = \{v_1^*, v_2^*\} = \begin{cases} 
g^{(a_i b_i H_1(i) + u) - (x + t)}, \hat{\varepsilon}(g, g)^{(u-x-t)}, & A_i \in \gamma \\
g^{(y_i H_1(i) + u) - (x + t)}, \hat{\varepsilon}(g, g)^{(u-x-t)}, & A_i \notin \gamma
\end{cases}
\]

\[
E^* = \{C_0 = M\hat{\varepsilon}(g, g)^{abx}, C_1 = g^x, C_2,i = \hat{\varepsilon}(g, g)^{-a_i H_1(i) \cdot \gamma_i}, C_3,i = g^{\gamma_i} \}
\]

(14)
Simulator verifies the ciphertext $CT^* \{ U^*, V^*, E^* \}$. Simulator firstly calculates the legal private key of receivers’ attribute set $\{ A_i \}$:

$\{ D_{s,1}, D_{s,2} \} = \begin{cases} \{ g^{a_i b_i H_i(j) + u} \cdot g^{u}, A_j \in \gamma \} \\
\{ g^{g H_i(j) + u}, g^u, A_j \notin \gamma \} \end{cases}$  \hspace{1cm} (15)

Then decrypts and verifies:

$M^* = C_0 \prod_{i \in l} \hat{e}(C_3, D_{r,1})^{a_i} \cdot \hat{e}(C_1, D_{r,2})$,

$t = H_2(U||M)$

$\hat{e}(v_1^*, g) = \begin{cases} \hat{e}(g^{a_i b_i H_i(j) + u} \cdot g^{u}), & A_j \in \gamma \\
\hat{e}(g^{g H_i(j) + u} \cdot g^{u}), & A_j \notin \gamma \end{cases}$

$= \begin{cases} \hat{e}(g, g)^{a_i b_i H_i(j) \cdot x} \cdot \hat{e}(g, g)^{a_i b_i H_i(j) \cdot t} \cdot \hat{e}(g, g)^{u(x + t)}, & A_j \in \gamma \\
\hat{e}(g, g)^{g H_i(j) \cdot x} \cdot \hat{e}(g, g)^{g H_i(j) \cdot t} \cdot \hat{e}(g, g)^{u(x + t)}, & A_j \notin \gamma \end{cases}$  \hspace{1cm} (16)

Let $f = \hat{e}(g, g)^{a_i b_i H_i(j) \cdot t + u(x + t)}, g^{H_i(j) \cdot x} = g^c$, according to the previous setting in the $Setup$ phase:

$\hat{e}(v_1^*, g) = \begin{cases} f \cdot v_1^* \cdot \hat{e}(g, g)^{abc}, & \text{if } u = 0 \\
f \cdot v_2^* \cdot \hat{e}(g, g)^{zx}, & \text{if } u = 1 \end{cases}$  \hspace{1cm} (17)

When $\mu = 1$, $\hat{e}(v_1^*, g)$ is a random number and $Adversary$ fails to forge a legal ciphertext.

$Pr(\mu^* = \mu | \mu = 1) = 1/2$  \hspace{1cm} (18)

When $\mu = 0$, $E$ is a legal ciphertext and $Adversary$ successfully forges the ciphertext. According to the assumption, $Adversary$ has an advantage $\varepsilon$.

$Pr(\mu^* = \mu | \mu = 0) = 1/2 + \varepsilon$  \hspace{1cm} (19)

As is mentioned above, the advantage of simulator is

$\frac{1}{2} Pr(\mu^* = \mu | \mu = 0) + \frac{1}{2} Pr(\mu^* = \mu | \mu = 1) - \frac{1}{2}$

$= \frac{1}{2} \left( 1 + \varepsilon \right) + \frac{1}{2} \times 1 - \frac{1}{2}$

$= \frac{\varepsilon}{2}$  \hspace{1cm} (20)
Efficiency analysis
In this paper, we compare the proposed scheme with Wang's and Hu's schemes with respect to the computation cost and access control method. Due to the fact that the computation cost of add operation and multiply operation is much smaller than that of exponential operation and bilinear pairing operation, consequently, we mainly compare the number of exponential operation and bilinear pairing operation in different schemes. We denote “Exp” and “Pair” by exponential operation and bilinear pairings. Detailed results are listed in Table 1.

From Table 1, we can figure out that the number of exponential operation in the sign-cryption in our CP-ABSC is more than those in Wang and Huang (2011) and Hu and Zhang (2013), however, the number of bilinear pairing operation in the de-sign-cryption is decreased greatly. Since the computation burden of bilinear pairing operation is heavier than that of exponential operation, the total computation cost has been reduced in our scheme. What’s more, our CP-ABSC adopts LSSS to realize data access control, which differs from the access structures in Wang and Huang (2011) and Hu and Zhang (2013). The LSSS access structure not only avoids the frequent calls of recursive algorithm used in access tree structure model, but also provides more flexible control management and increases the overall efficiency of the cryptosystem.

Conclusion
In this paper, we propose an optimized attribute based signcryption scheme. By security analysis, we prove that it meets the security demands of confidentiality, unforgeability and non-repudiation. Besides, by introducing LSSS structure to implement the access control function, the flexibility and efficiency of the whole attributed based signcryption system has been improved.

Our future work should focus on the attribute revocation and key refreshing in the attribute based encryption. Since users with the same set of attributes share the same private key, once a single user’s private key has been leaked, a group of users’ privacy and privilege will be damaged. Consequently, protecting users’ privacy and refreshing private keys at a lower cost when private key leakage happens is a problem urgently to be solved and should be taken into our future research direction.

| Schemes                    | Access control method | Signcryption computation cost | De-signcryption computation cost |
|----------------------------|-----------------------|-----------------------------|---------------------------------|
| Wang and Huang (2011)      | Access tree           | 2 Exp + 1Pair               | (1 + 2nlog n) Exp + (4n + 1)Pair |
| Hu and Zhang (2013)        | Threshold             | (2n + 5) Exp                | 2n Exp + (3n + 2)Pair           |
| Our scheme                 | LSSS matrix           | (5n + 2) Exp                | (n + 1) Exp + (2n + 1)Pair      |
**Authors’ contributions**

HH: Carried out the attribute based signcryption studies, participated in the design of scheme and drafted the manuscript. ZS: Participated in the performance analysis of the scheme. Both authors read and approved the final manuscript.

**Authors’ information**

Dr. Zhixin Sun is the dean of Internet of Things institute, Nanjing University of Posts and Telecommunications. He has published more than 50 literatures on journals worldwide. His research area includes information security, computer networks, computer science, etc. Dr. Hanshu Hong is a PhD candidate in Nanjing University of Posts and Telecommunications. His research area includes information security, cryptology.

**Acknowledgements**

This research is supported by the National Natural Science Foundation of China (60973140, 61170276, 61373135). The authors thank the sponsors for their support and the reviewers for helpful comments.

**Competing interests**

The authors declare that they have no competing financial interests.

**Received:** 21 February 2016  **Accepted:** 5 May 2016

**Published online:** 17 May 2016

**References**

Beimel A (1996) Secure schemes for secret sharing and key distribution. Ph.D. thesis, Israel Institute of Technology, Technion, Haifa, Israel

Bethencourt J, Sahai A, Waters B (2007) Ciphertext-policy attribute based encryption. In: Proceedings of the 2007 IEEE symposium on security and privacy. Washington: IEEE Computer Society, pp 321–334

Goyal V, Pandey O, Sahai A, Waters B (2006) Attribute based encryption for fine-grained access control of encrypted data. In: ACM conference on computer and communications security, pp 89–98

Goyal V, Jain A, Pandey O, Sahai A (2008) Bounded ciphertext policy attribute based encryption. In: Proceedings of the 35th international colloquium, pp 579–591, Reykjavik, Iceland, 2008

Guo SQ, Zeng YP (2008) Attribute based signature scheme. In: International conference on information security and assurance, pp 509–511

Hu C, Zhang N (2013) Body area network security: a fuzzy attribute based signcryption scheme. IEEE J Sel Areas Commun Suppl 31(9):37–46

Lewko A, Okamoto T, Sahai A, Takashima K, Waters B (2010) Fully secure functional encryption: attribute based encryption and (hierarchical) inner product encryption. In: Advances in cryptology—EUROCRYPT 2010, pp 62–91, Springer, Berlin, Germany, 2010

Li F, Khan MK (2012) A biometric identity-based signcryption scheme. Future Gener Comput Syst 28(1):306–310

Lim CH, Lee PJ (1998) A study on the proposed Korean digital signature algorithm. In: Advanced in cryptography—ASIACRYPT’98, pp 175–185

Maji H, Prabhakaran M, Rosulek M (2011) Attribute based signatures. In: CT-RSA 2011, pp 376–392, Springer

Paulo SLM, Barreto BL, McCullagh N, Quisquater J-J (2005) Efficient and provably-secure identity-based signatures and signcryption from bilinear maps. Adv Cryptol ASIACRYPT LNCS 3788:515–532

Sahai A, Waters B (2005) Fuzzy identity-based encryption. In: Proceedings of the international conference on EUROCRYPT 2005, pp 457–473, Aarhus, Denmark

Selvi S, Vivek S, Shukla D, Chandrasekaran P (2008) Efficient and provably secure certificateless multi-receiver signcryption. ProSec 5324:52–67

Tan C (2008) On the security of provably secure multi-receiver ID-based signcryption scheme. IEICE transactions on fundamentals of electronics. Commun Comput Sci E91-A(7):1836–1838

Tian Y, Peng Y (2014) An attribute based signcryption scheme with revocation for fine-grained access control in wireless body area networks. Int J Distrib Sens Netw 2014:9, Article ID 259798

Wang C, Huang J (2011) Attribute based signcryption with ciphertext policy and claim predicate mechanism. In: CIS, 2011 Seventh international conference, pp 905–909

Waters B (2011) Ciphertext policy attribute based encryption: an expressive, efficient, and provably secure realization. In: Proceedings of International Conference on PKC 2011, pp 53–70, Taormina, Italy, March 2011

Zheng Y (1997) Digital signcryption or how to achieve cost (signature & encryption) < cost (signature) + cost (encryption). In: CRYPTO 1997, pp 165–179, Springer