5-2017

# Provably secure attribute based signcryption with delegated computation and efficient key updating

Hanshu HONG
*Nanjing University of Posts and Telecommunications*

Yunhao XIA
*Nanjing University of Posts and Telecommunications*

Zhixin SUN
*Nanjing University of Posts and Telecommunications*

Ximeng LIU
*Singapore Management University*, xmliu@smu.edu.sg

# Provably secure attribute based signcryption with delegated computation and efficient key updating

**Hanshu Hong[1], Yunhao Xia[1], Zhixin Sun[1*], Ximeng Liu[2]**
[1] Key Lab of Broadband Wireless Communication and Sensor Network Technology, Nanjing University of Posts and Telecommunications
Nanjing, China
[e-mail: 2014070244@njupt.edu.cn, 2015070108@njupt.edu.cn, sunzx@njupt.edu.cn]
[2] School of information systems, Singapore Management University
[e-mail: xmliu@smu.edu.sg]
*Corresponding author: Zhixin Sun

*Received September 22, 2016; revised December 18, 2016; revised January 24, 2017; revised February 13, 2017; accepted February 24, 2017; published May 31, 2017*

## Abstract

Equipped with the advantages of flexible access control and fine-grained authentication, attribute based signcryption is diffusely designed for security preservation in many scenarios. However, realizing efficient key evolution and reducing the calculation costs are two challenges which should be given full consideration in attribute based cryptosystem. In this paper, we present a key-policy attribute based signcryption scheme (KP-ABSC) with delegated computation and efficient key updating. In our scheme, an access structure is embedded into user's private key, while ciphertexts corresponds a target attribute set. Only the two are matched can a user decrypt and verify the ciphertexts. When the access privileges have to be altered or key exposure happens, the system will evolve into the next time slice to preserve the forward security. What's more, data receivers can delegate most of the de-signcryption task to data server, which can reduce the calculation on client's side. By performance analysis, our scheme is shown to be secure and more efficient, which makes it a promising method for data protection in data outsourcing systems.

***Keywords:*** attribute based encryption, signcryption, key evolution, efficient

This research is supported by the National Natural Science Foundation of China (61373135 and 61672299).

**https://doi.org/10.3837/tiis.2017.05.019** **ISSN : 1976-7277**

## 1. Introduction

Attribute based encryption (ABE) was initially proposed in [1]. Since then, many novel literatures constructed on ABE were presented [3-5]. In ABE, the concept of "access policy" is introduced, only the user's attributes suit with the policy can he complete decryption [7-8] [20]. A file owner may set a data centric access policy without concerning about the specific identity of each user in the system (note that the amount of user in the system may be very large). Consequently, ABE is a more effective tool for data protection in large data outsourcing platforms [2]. Later, attribute based signature (ABS) was put forward. Equipped with capability of achieving flexible authentication, ABS also becomes a resultful mechanism for providing data verification between users in different application scenarios.

Inspired by the notion signcryption [9], researchers successfully combined the merits of ABE and ABS and proposed several attribute based signcryption (ABSC) schemes [10-12] which provide both functions of ABE and ABS in a single step. Compared with the traditional sign-then-encrypt method, their schemes are shown to be outperformed with respect to efficiency.

However, there still exist some shortages in existing ABSC schemes. To begin with, the schemes proposed in [10-12] centered on the protection of data, but neglecting the protection of keys. In other words, they haven't taken backward and forward security into full consideration when user's privilege alternation or key leakage occurs. Image that when attribute revocation or key leakage occurs, the system will face threaten since the private key haven't been securely refreshed. Thus an efficient and effective key evolution mechanism [18][21] is urgently to be proposed.

Furthermore, the existing works related to ABSC consumes considerable computation overheads, which may add difficulty to users during data sharing. Since attribute based cryptosystem is extremely suitable for providing safeguard in data outsourcing systems, the computation task can also be delegated to the data server, which will minimizes the computation cost on the client side.

To provide a better method of data sharing in outsourcing systems, in this paper, the following constructions are established:

1) We proposed an attribute based signcryption with key exposure protection and delegated calculation for data outsourcing systems. In our scheme, the ciphertexts are labeled by a set of attributes while a user's private key accords with a structure. Only the two are matched can a user decrypt and verify the ciphertexts.

2) The ciphertexts generated by signer corresponds a certain time slice in the system. When key leakage happens, the system will evolve into the next time slice to preserve the forward security. The public parameters needn't to be changed during the evolution of user's private key, which minimizes the overheads brought by parameter synchronization.

3) During the process of data sharing, data receivers can delegate most of the de-signcryption task to data server, which can decrease the calculation burden on client side.

4) Via proof and efficiency analysis, our scheme is show to be confidential and unforgeable, which makes it a promising method for data protection in data outsourcing systems.

The rest of paper is arranged as follows:

Section 2 reviews the existing state of art related to our research. Section 3 gives the syntax and security models of our scheme. Section 4 contains a full description of the proposed KP-ABSC along with the correctness proof. Section 5 focuses on the security proof

and efficiency evaluation. Section 6 provide a real world application scenario of our scheme. Finally, the conclusion is made in Section 7.

## 2. Related works

### 2.1 Attribute based Signcryption

Signcryption [9] can provide the merits of encryption and signature in a single phase. Meanwhile, the computation cost of signcryption is less than the traditional Encrypt-after-Sign method. With the advent of signcryption, many schemes based on this notion have been put forward. The proposed schemes are mainly constructed upon public key cryptography or identity-based cryptography, but much fewer with regard to attribute based cryptography. Actually, the notion of signcryption can also be introduced to attribute based cryptography to propose signcryption schemes which combine the encryption function of ABE and signature function of ABS. Hong et al. in [10] take the advantages of liner secret sharing mechanism and proposed an attribute based signcryption, which provides high decryption and authentication. Their scheme can be used for security preservation in date-centric scenarios. Wang et al. in [11] proposed a CP-ABSC scheme which combines ABE and ABS in one logic step, and the computation cost is much less than the traditional ABS+ABE method. In [12], Hu et al. proposed a fuzzy ABSC and achieves significant results in BAN system. Their scheme is a novel mechanism which realizes an appropriate balance between security and scalability. The above schemes have realized effciecnt protection of data, but neglecting the protection of keys[22-25]. In other words, they haven't taken backward and forward security into full consideration when user's privilege alternation or key leakage occurs. In ABSC, both privilige revocation and key leakage call for the demand of secure key evuolution[26], thus it's high time to introduce a fkxeible key refreshing mechanism in ABSC.

### 2.2 Proxy decryption

Proxy decryption is an effective method which can decrease the computation burden on user's client side. By delegation, the data server will undertake most of the decryption task. More importantly, the data are still confidential to the semi-trusteed data server, thus the user's privacy can be guaranteed. Many researchers have presented attribute based proxy decryption schemes in data outsourcing systems [6] [13-17]. Green et.al in [6] firstly proposed the ABE with proxy calculation. In their scheme, the private key of a user consists of two components: one is the kept private by the user himself while the other is used for proxy decryption. During the process of data sharing, user firstly sends the key for proxy decryption to data server. Data server decrypts the initial ciphertexts using the proxy key and sends the transformed ciphertexts back to user. Then user can finish the decryption and recover the plaintext at a very low cost. Lai et.al presented a verifiable ABE with delegated decryption in [13]. Their scheme provides flexible management over the ciphertext stored in the cloud and the computation cost is sharply decreased. Their scheme also allows a user to verify whether the ciphertexts from data server are correctly transformed. Qin et.al in [14] presented a framework for outsourcing system along with the concrete algorithms. The proposed scheme helps relieve the computation burden both on the cloud data server and user clients. Aim to tackle authentication related issues in outsourcing systems, Liu et.al proposed an ABS for cloud computing in [15]. By delegation, user's computation overheads are much more reduced during signing and verification. Similarly, schemes in [16-17] also

take the merits of outsourcing data server and achieve significant results. From what has been discussed above, it can be figured out that proxy computation can reduce the calculation cost on client side sharply, which in turn help users gain an enhanced experience during data sharing.

## 3. Models and assumptions

### 3.1 Models

The data sharing process of the proposed KP-ABSC is illustrated in **Fig. 1.** At the beginning, data signer signcrypts the plaintexts using the possessing private key and the target attribute set. In this way the plaintext is well encrypted and can be verified. Then he outsources the ciphertexts to data server. When a data receiver wants to get access to the ciphertexts, he firstly sends a request containing the proxy key to data server. Data server delegates most of the de-signcryption work in advance and returns the transformed ciphertexts to receiver. After that, receiver can recover the plaintext from the transformed ciphertext at a very low cost.

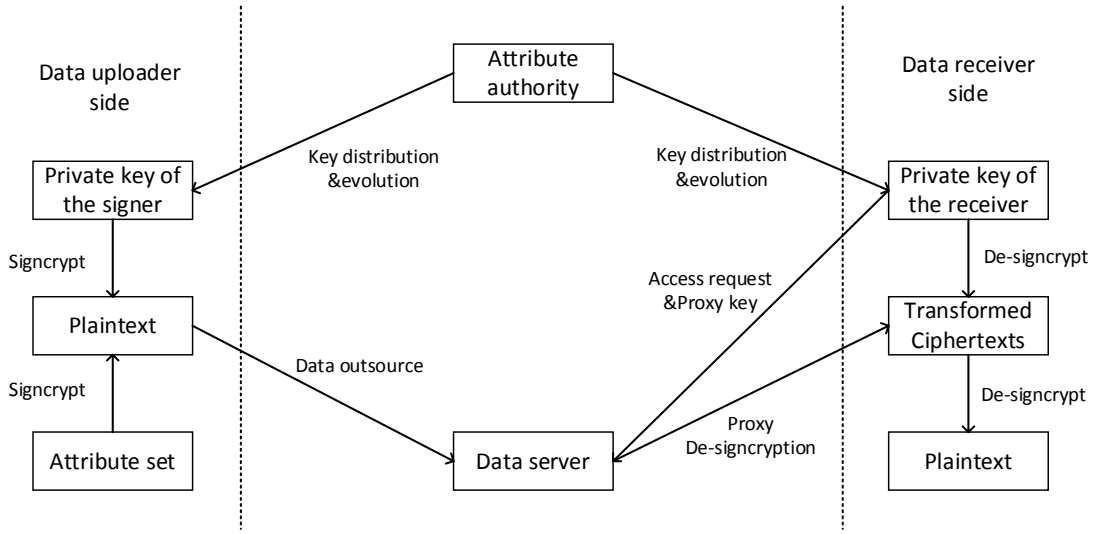



**Fig. 1.** Process of KP-ABSC

### 3.2 Syntax

Our scheme consist of the following algorithms:

$Setup$: It takes a security parameter as input and outputs the system master keys and public parameters.

$Key\ extraction$**:** It takes the system master keys and an access structure as input, outputs the private key of a user at the initial time slice.

$Key\ refresh$: It takes the system master keys and the information of time slices as input, outputs the key refresh components for the current time slice. Users update their temporal private keys by making calculations on these components.

$Signcrypt$: It takes a plaintext, public parameters and the temporal private keys a data owner processes as input, outputs a ciphertext.

$De-Signcrypt$: It takes the ciphertext and the temporal private keys a data receiver processes as input, outputs a valid plaintext or a reject symbol.

### 3.3 Security definitions

Since we present an attribute based signcryption which provides both the encryption and authentication, we will prove its confidentiality and unforgeability.

**Definition1**: The confidentiality of our scheme can be proved by the following security game.

$Setup$:

$Adversary$ claims $S$ to be challenge attribute set. Simulator generates the system parameters.

$Query$:

$Adversary$ can obtain temporal private key for an access structure $\gamma_q$ by making temporal private key generation queries to simulator.

$Challenge$:

$Adversary$ picks plaintexts $M_0$ and $M_1$. Simulator picks $\theta \in \{0,1\}$ and outputs $Signcrypt\{M_\theta, S\}$ as the ciphertext.

$Adversary$ outputs a value $\theta^*$ to be the guess of $\theta$. If $\theta^* = \theta$ then $Adversary$ wins the game.

Denote $Adv(A) = \left| Pr[\,\theta^* = \theta] - \frac{1}{2} \right|$ to be the advantage in the challenge game.

**Definition2**: The unforgeability of our scheme can be proved by the following security game:

$Setup$:

$Adversary$ claims an an access structure $\gamma_c$ to be challenge structure.
Simulator generates the system parameters.

$Query$:

$Adversary$ chooses an access structure $\gamma_q$ (containing attribute set $S$) and a plaintext $M$. Simulator outputs $Signcrypt\{M, \gamma_q\}$ as the ciphertext.

Note that $Adversary$ cannot ask for the $Signcrypt\ query$ of $\gamma_c$.

$Challenge$:

$Adversary$ computes a ciphertext. Simulator verifies the ciphertext by running $De - signcrypt$ algorithm.

$Adversary$ wins if the ciphertext can be verified correctly.

### 3.4 Decision Bilinear Diffie-Hellman hardness assumption (DBDH):

For $a,b,c,z \in Z_q^*$, given $(g,g^a,g^b,g^c,z)$, it is computational infeasible to distinguish ( $A=g^a,B=g^b,C=g^c,\hat{e}(g,g)^{abc}$ ) and ( $A=g^a,B=g^b,C=g^c,\hat{e}(g,g)^z$ ) within probabilistic polynomial-time.

## 4. Constructions

The concrete constructions of our KP-ABSC are described as follows:

$Setup$: Let $G_1$ and $G_2$ be two cyclic groups with prime order $p$.Denote $g$ is the generator of $G_1$.Let $\hat{e}: G_1 \times G_1 \to G_2$ be a bilinear pairing. Define three functions: $f_1:\{0,1\}^* \to G_1, f_2:\{0,1\}^* \to Z_p^*, f_3:\{0,1\}^* \to \{0,1\}^m$. AA randomly chooses $l,y \in Z_p^*$ with $a_i \in Z_p^*$ for each attribute in the system and computes $Y=\hat{e}(g,g)^y, A_i=g^{a_i}, L=g^l, L_{a_i}=L^{a_i}$. The system master keys are $\{a_i, y, l\}$, while the system public parameters can be denoted by $\{G_1,G_2,p,g,\hat{e},A_i,Y,L,L_{a_i},f_1,f_2,f_3\}$.

$Key\ extraction$: AA picks a unique secret number $d_u \in Z_p^*$ for each user in the system. Without loss of generality, at time period $t_0$,for a signer with attribute structure $\gamma$, its initial private key is denoted by $SK_{t_0}=\{D_1,D_2,D_3\}=\left\{g^{\frac{q_x(0)}{d_u a_i}}\cdot f_1(A_i,t_0)^l, d_u, g^{\frac{q_x(0)}{a_i}}\cdot f_1(A_i,t_0)^l, i\in\gamma\right\}$.

$Key\ refresh$: In order to update user's private key from time slice $t_m$ to $t_{m+1}$, AA calculates the updated key component $u_{i,t_{m+1}}$ for each attribute $i$ as $\left(\frac{f_1(A_i,t_{m+1})}{f_1(A_i,t_m)}\right)^l$ and sends the key refreshing component to users. Upon receiving the updating information, users update their temporal private keys by computing $SK_{t_{m+1}}=\{D_1\cdot u_{i,t_{m+1}}, D_2, D_3\cdot u_{i,t_{m+1}}\}$.

$Signcrypt$: To separate the roles of signer and receiver, we denote $A_j$ to be the attributes owned by signer $A_i$ to be that of receiver. The signer picks $x,k \in Z_p^*$ and calculates:

$$\begin{aligned} C_0 &= k\cdot Y^x \\ C_{1,i} &= {A_i}^x \\ C_{2,i} &= f_1(A_i,t_m)^x \\ C_{3,i} &= {D_3}^{x+f_2(M,k)} \\ C_{4,i} &= f_1(A_j,t_m)^x \\ C_5 &= f_3(k)\oplus M \end{aligned} \tag{1}$$

Then signer sends $\{C_0,C_{1,i},C_{2,i},C_{3,i},C_{4,i},C_5\}$ to data server.

$De-Signcrypt$: The process of $De-Signcrypt$ consists of two steps:

First step: The receiver sends an access request and outsources $D_1$ to data server. Data server calculates:

$$m=\prod_{i\in\gamma}\frac{\hat{e}(D_1,C_{1,i})}{\hat{e}(C_{2,i},L_{a_i})}$$

$$v=\prod_{i\in\gamma}\hat{e}(C_{3,i},A_j) \tag{2}$$

**Data server** sends $m,v$ back to receiver.

Second step:

The receiver calculates

$$M^* = f_3(\frac{C_0}{m^{D_2}}) \oplus C_5 \tag{3}$$

And verifies:

$$v = m^{D_2} \cdot Y^{H_2(M^*)} \prod_{j\in\gamma} \hat{e}\left(L_{a_j}, C_{4,i} \cdot f_1(A_j, t_m)^{f_2(M^*+k)}\right) \tag{4}$$

If lemma (4) holds, then the signature is valid and it outputs $M^*$ as the correct plaintext.

**Correctness proof:**

The correctness of delegating de-signcryption made by data server is proved by lemma (5):

$$\begin{aligned} m &= \prod_{i\in\gamma} \frac{\hat{e}(D_1, C_{1,i})}{\hat{e}(C_{2,i}, L_{a_i})} \\ &= \prod_{i\in\gamma} \frac{\hat{e}(g^{\frac{q_x(0)}{d_u a_i}} \cdot f_1(A_i, t_m)^l, {A_i}^x)}{\hat{e}(f_1(A_i, t_m)^x, L^{a_i})} \\ &= \prod_{i\in\gamma} \frac{\hat{e}(g^{\frac{q_x(0)}{d_u a_i}} \cdot f_1(A_i, t_m)^l, g^{a_i x})}{\hat{e}(f_1(A_i, t_m)^x, g^{l a_i})} \\ &= \prod_{i\in\gamma} \frac{\hat{e}(g^{\frac{q_x(0)}{d_u a_i}}, g^{a_i x}) \cdot \hat{e}(f_1(A_i, t_m)^l, g^{a_i x})}{\hat{e}(f_1(A_i, t_m)^x, g^{l a_i})} \\ &= \prod_{i\in\gamma} \hat{e}(g^{\frac{q_x(0)}{d_u a_i}}, g^{a_i x}) \\ &= \prod_{i\in\gamma} \hat{e}(g, g)^{\frac{q_x(0)x}{d_u}} \\ &= \hat{e}(g, g)^{\frac{yx}{d_u}} \end{aligned} \tag{5}$$

The correctness of de-signcryption made by receiver is proved by lemma (6) (7):

$$\begin{aligned} k &= \frac{C_0}{m^{D_2}} = \frac{k \cdot Y^x}{m^{d_u}} \\ &= \frac{k \cdot \hat{e}(g, g)^x}{\hat{e}(g, g)^{\frac{yx}{d_u} d_u}} \\ &= k \end{aligned}$$

$$M^* = f_3(k) \oplus C_5 = f_3(k) \oplus f_3(k) \oplus M = M \tag{6}$$

$$\begin{aligned} v &= \prod_{j\in\gamma} \hat{e}\left({D_3}^{x+H_2(M^*)}, A_j\right) \\ &= \prod_{j\in\gamma} \hat{e}\left((g^{\frac{q_x(0)}{a_j}} \cdot f_1(A_j, t_m)^l)^{x+f_2(M^*,k)}, g^{a_j}\right) \\ &= \prod_{j\in\gamma} \hat{e}(g^{\frac{q_x(0)}{a_j}}, g^{a_j})^{x+f_2(M^*,k)} \cdot \hat{e}(f_1(A_j, t_m)^l, g^{a_j})^{x+f_2(M^*,k)} \end{aligned}$$

$$= \prod_{j\in\gamma} \hat{e}(g,g)^{q_x(0)\cdot(x+f_2(M^*,k))} \cdot \hat{e}(f_1(A_j,t_m), g^{la_j})^{x+f_2(M^*,k)}$$

$$= \hat{e}(g,g)^{y\cdot(x+f_2(M^*,k))} \cdot \prod_{j\in\gamma} \hat{e}\left(f_1(A_j,t_m)^{x+f_2(M^*,k)}, g^{la_j}\right)$$

$$= \hat{e}(g,g)^{\frac{yx}{d}\cdot d} \cdot \hat{e}(g,g)^{y\cdot f_2(M^*,k)} \cdot \prod_{j\in\gamma} \hat{e}\left(g^{la_j}, f_1(A_j,t_m)^{x} \cdot f_1(A_j,t_m)^{f_2(M^*,k)}\right)$$

$$= m^{D_2} \cdot Y^{f_2(M^*,k)} \cdot \prod_{j\in\gamma} \hat{e}\left(L_{a_j}, C_{4,i} \cdot f_1(A_j,t_m)^{f_2(M^*,k)}\right) \quad (7)$$

## 5. Performance analysis

### 5.1 Confidentiality

**Theorem 1:** The proposed KP-ABSC is secure if DBDH hardness assumption holds.

Proof: If an $Adversary$ breaks our KP-ABSC with advantage $\varepsilon$ in the selective model, then a simulator can be constructed to break the DBDH hardness assumption with an advantage of $\varepsilon/2$.

The security game is as follows:

$Setup$: Define cyclic groups of prime order $p$, $G_1$ and $G_2$ .Denote $g$ to be a generator of $G_1$. Let $\hat{e}: G_1 \times G_1 \to G_2$ be a pairing. Define 2 functions: $f_1: \{0,1\}^* \to G_1, f_2: \{0,1\}^* \to Z_p^*$.

Picks $\theta \in \{0,1\}, a, b, c, z \in Z_p^*$ at random and sets:

$$\begin{cases} tuple\ 1 = \left(g^a, g^b, g^c, \hat{e}(g,g)^{abc}\right) & if\ \theta = 0 \\ tuple\ 2 = \left(g^a, g^b, g^c, \hat{e}(g,g)^z\right) & if\ \theta = 1 \end{cases}$$

The goal of $Challenger$ is to guess the $\theta$ according to the response made by $Adversary$.

$Adversary$ claims an attribute set $S$.

$Query$:

Simulator picks $a_i \in Z_p^*$ for each attribute and sets $A_i$ to be:

$$A_i = \begin{cases} g^{a_i}, if\ i \in S \\ g^{b\cdot a_i}, if\ i \notin S \end{cases}$$

When $Adversary$ asks for the result of temporal private key of structure $\gamma_q$, simulator responds as follows:

When $i \in S$, sets $SK_{t_m} = \{g^{\frac{q_x(0)}{d_u a_i}} \cdot f_1(A_i,t_0)^l, d_u, g^{\frac{q_x(0)}{a_i}} \cdot f_1(A_i,t_0)^l, i \in \gamma_q\}$.

When $i \notin S$, sets $SK_{t_m} = \{g^{\frac{q_x(0)}{d_u b\cdot a_i}} \cdot f_1(A_i,t_0)^l, d_u, g^{\frac{q_x(0)}{a_i\cdot b}} \cdot f_1(A_i,t_0)^l, i \in \gamma_q\}$.

$Challenge$:

$Adversary$ picks $M_0, M_1$. Simulator randomly picks $x \to Z_p^*$ and calculates

$$CT_\theta = \{k \cdot Y^x, {A_i}^x, f_1(A_i,t_m)^x, f_3(k) \oplus M_\theta\} \quad (8)$$

Let $f_1(A_i,t_m)^x = g^s$ then we have:

$$CT_\theta = \begin{cases} k\hat{e}(g,g)^{abc}, C^{a_i}, C^t, f_3(k) \oplus M_0, \theta = 0 \\ k\hat{e}(g,g)^z, C^{a_i}, C^t, f_3(k) \oplus M_1, \theta = 1 \end{cases} \quad (9)$$

When $\theta = 1$, $CT_\theta$ is a random number. Under this circumstance simulator guesses $\theta^*$ randomly.

$$Pr(\theta^* = \theta|\theta = 1) = \frac{1}{2} \tag{10}$$

When $\theta = 0$, $CT_\theta$ is a valid ciphertext. Under this circumstance the advantage of $Adversary$ is $\varepsilon$.

$$Pr(\theta^* = \theta|\theta = 0) = \frac{1}{2} + \varepsilon \tag{11}$$

Consequently, the overall advantage is:

$$\begin{aligned} &\frac{1}{2}Pr(\theta^* = \theta|\theta = 1) + \frac{1}{2}Pr(\theta^* = \theta|\theta = 0) - \frac{1}{2} \\ &= \frac{1}{2} \times \frac{1}{2} + \frac{1}{2}\left(\frac{1}{2} + \varepsilon\right) - \frac{1}{2} \\ &= \frac{\varepsilon}{2} \end{aligned} \tag{12}$$

## 5.2 Unforgeability

**Theorem 2:** The proposed KP-ABSC has the unforgeability if CDH hardness assumption holds.

Proof: If an $Adversary$ can forge a legal ciphertext with an non-neglectable advantage in the chosen message model, then a simulator can be constructed to break the CDH hardness assumption. Note that we have proved the confidentiality of KP-ABSC, thus in this proof we only focus on the unforgeability. For clearness, the construction of ciphertext is a little different, but it will not influence the final result.

$Setup$: Set the same parameters like **Theorem 1.**

Randomly chooses $a, b \in Z_p^*$.

$Adversary$ claims an attribute set $S$. The aim of simulator is to calculate the value of $g^{ab}$ under the condition that the value of $g^a$ and $g^b$ are known.

$Query$:

Simulator picks $a_j \in Z_p^*$ for each attribute and sets $A_j$ to be:

$$A_i = \begin{cases} g^{a_j}, if\ j \in S \\ g^{b \cdot a_j}, if\ j \notin S \end{cases}$$

When $Adversary$ asks for a $Signcrypt$ query of a plaintext and structure $\gamma_q$, simulator responds as follows:

Firstly, simulator calculates the temporal private key of $\gamma_q$.

When $i \in S$, sets $SK_{t_m} = \{g^{\frac{q_x(0)}{d_u a_j}} \cdot f_1(A_j, t_0)^l, d_u, g^{\frac{q_x(0)}{a_j}} \cdot f_1(A_j, t_0)^l, j \in \gamma_q\}$.

When $i \notin S$, sets $SK_{t_m} = \{g^{\frac{q_x(0)}{d_u b \cdot a_j}} \cdot f_1(A_j, t_0)^l, d_u, g^{\frac{q_x(0)}{a_j \cdot b}} \cdot f_1(A_j, t_0)^l, j \in \gamma_q\}$.

Then, simulator picks $x \in Z_p^*$ and calculates

$$C_{3,i} = (g^{\frac{q_x(0)}{a_j}} \cdot f_1(A_j, t_0)^l)^{x + f_2(M^*, k)}, C_{4,i} = f_1(A_j, t_m)^x \tag{13}$$

$Challenge$: $Adversary$ outputs a signature for plaintext $M_c$.

Simulator outputs as the solution to CDH hardness assumption.

$$\left(B^{H_2(M_c)}\right)^{-1} \prod_{j \in \gamma_c} \frac{{C_{3,i}}^{a_j}}{{C_{4,i}}^{l \cdot a_j} \cdot f_1(A_j, t_m)^{l \cdot a_j \cdot f_2(M_c, k)}} \tag{14}$$

Proof: If the signature is a valid one, then we have:

$$g^{ab} = \left(B^{f_2(M_c, k)}\right)^{-1} \prod_{j \in \gamma_c} \frac{{C_{3,i}}^{a_j}}{{C_{4,i}}^{l \cdot a_j} \cdot f_1(A_j, t_m)^{l \cdot a_j \cdot f_2(M_c, k)}} \tag{15}$$

Thus:

$$\prod_{j\in\gamma_c}\hat{e}\left({C_{3,i}}^{a_j},g\right)=\hat{e}\left(g^{ab},g\right)\cdot\hat{e}\left(g^{b\cdot f_2(M_c,k)},g\right)\cdot\prod_{j\in\gamma_c}\hat{e}\left({C_{4,i}}^{la_j}\cdot f_1\left(A_j,t_m\right)^{l\cdot a_j\cdot f_2(M_c,k)},g\right)$$

$$\prod_{j\in\gamma_c}{C_{3,i}}^{a_j}=g^{ab}\cdot g^{b\cdot f_2(M_c,k)}\cdot\prod_{j\in\gamma_c}{C_{4,i}}^{la_j}\cdot f_1\left(A_j,t_m\right)^{l\cdot a_j\cdot f_2(M_c,k)}$$

$$\left(\prod_{j\in\gamma_c}{C_{4,i}}^{la_j}\cdot f_1\left(A_j,t_m\right)^{l\cdot a_j\cdot f_2(M_c,k)}\cdot g^{b\cdot f_2(M_c,k)}\right)^{-1}\cdot\prod_{j\in\gamma_c}{C_{3,i}}^{a_j}=g^{ab} \quad (16)$$

Thus we have:

$$g^{ab}=\left(B^{f_2(M_c,k)}\right)^{-1}\prod_{j\in\gamma_c}\frac{{C_{3,i}}^{a_j}}{{C_{4,i}}^{l\cdot a_j}\cdot f_1\left(A_j,t_m\right)^{l\cdot a_j\cdot f_2(M_c,k)}} \quad (17)$$

### 5.3 Efficiency

This part discusses the efficiency of our KP-ABSC. We mainly analyze the amount of pairing and exponentiation (note that these two consumes much more than other operations in discrete group [19]) in each algorithm of our KP-ABSC. Denote "$n$" to be the number of universal attributes, "$i$" and "$j$"to be the attributes of signer and receivers respectively. The results with are listed in **Table 1**.

**Table 1.** Performance evaluation

| Algorithms | Exponentiation | Pairing |
|---|---|---|
| Setup | $2n+1$ | 1 |
| Key extraction | $2n$ | 0 |
| Key update | $n$ | 0 |
| Signcrypt | $2i+2j+1$ | 0 |
| De-signcrypt(Total) | $i+j+2$ | $j+3i$ |
| De-signcrypt(Client) | $i+2$ | $i$ |
| De-signcrypt(Server) | $j$ | $3j$ |

We compare our scheme with Guo's ABSC scheme in [27] and Wei's in [28]. The comparison are conducted in terms of the relative computation in de-signcryption as well as the sizes of ciphertexts and private keys. Denote "$d$" to be the threshold value and "$\rho$" to be the length of a user's identity in [27].

**Table 2.** Performance comparison

| Scheme | Access structure | De-signcryption | Sizes of private keys | Sizes of ciphertexts | Key evolution |
|---|---|---|---|---|---|
| [27] | Key policy | $O(\lvert\rho\rvert+\lvert j\rvert)$ | $O(\lvert n\rvert^2+\lvert d\rvert^2)$ | $O(\lvert\rho\rvert+\lvert j\rvert)$ | No |
| [28] | Key policy | $O(\lvert i\rvert)$ | $O(\lvert n\rvert)$ | $O(\lvert i\rvert+\lvert j\rvert)$ | No |
| Ours | Key policy | $O(\lvert i\rvert+\lvert j\rvert)$ | $O(\lvert n\rvert)$ | $O(\lvert i\rvert+\lvert j\rvert)$ | Yes |

It can been seen from **Table 2** that the sizes of private keys are smaller in our scheme, while the load of de-signcryption and sizes of ciphertexts are in the same order of magnitude. However, in our scheme since most of the de-signcryption task has been delegated to the data server, thus the computation cost of de-signcrypt algorithm is also lower in our KP-ABSC. What's more, our scheme supports key evolution and the process will not bring new system parameters to the system, this will reduce the overheads which parameter synchronization brings.

Then we conduct the experimental setups of schemes in [27] [28] and our scheme. The comparison mainly focus on the de-signcryption time cost on the client side. The experiments are conducted on PBC (Pairing-Based Cryptography) library underlying pairing-based cryptosystems. The operating system on the experimental computer is Ubuntu 12.04 with 6GB RAM. We set the order of elliptic curve group to be 160 bits. The comparison results are shown in **Fig. 2**.

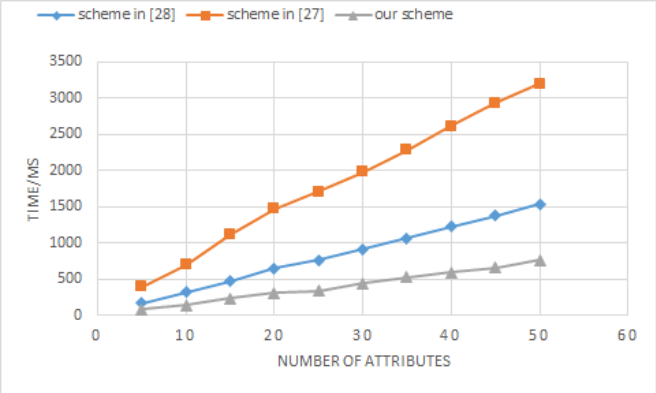



**Fig. 2.** Comparison results

From **Fig. 2**, it can be seen that with the number of attributes increasing in the system, our scheme needs much less time cost for de-signcryption, thus our scheme archives better efficiency.

## 6. Application of KP-ABSC

A typical application of our scheme is pay TY system, which has gained increasingly popularity nowadays. In the scenario, the television programme is encrypted using several attributes while user's privileges are described by an access structure. For instance, if a user has paid for becoming a VIP of "Sports" and "Movie", then his structure can be illustrated as **Fig. 3**. If the TV programme 1 is encrypted by {"Sports", "VIP"} or TV programme 2 {"Movie", "VIP"}, then the user can correctly decrypt these encrypted programme.

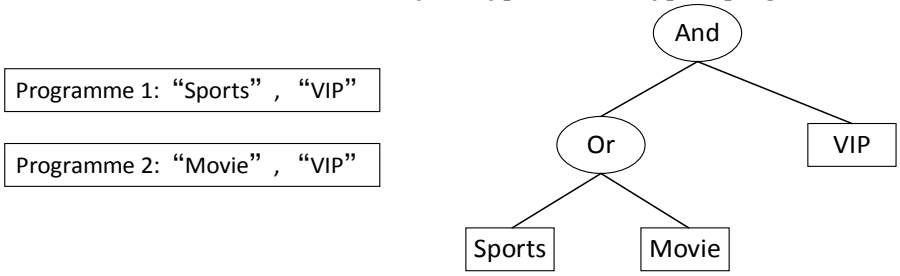



**Fig. 3.** An example of user's access structure

If the user no longer wants to renew his "Sports" services in the coming time slice, then he will not receive the key evolution component of the attribute "Sports", then his access structure will be altered as **Fig. 4** shows. If a TV programme is encrypted by {"Movie", "VIP"}, the user can still get access to the programme since he still holds the attribute of "Movie". On the contrary, he can no longer get access to the programme related to "Sports" since this attribute has been revoked.

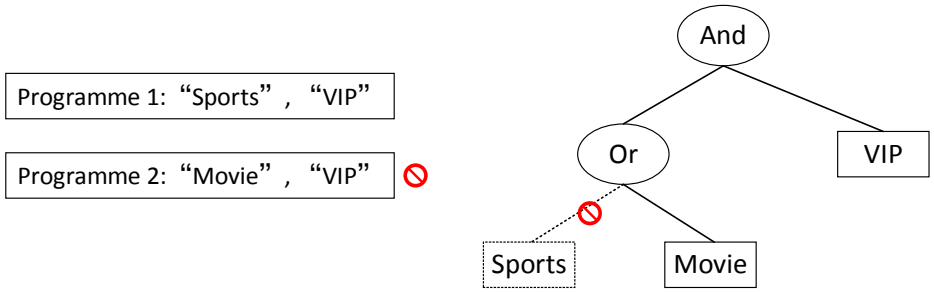



**Fig. 4.** An example of user’s access structure after revocation

The advantage of this application is that the programme publishers can set a data centric access policy without concerning about the specific identity of each user in the pay TV system, thus the encryption is very efficient.

Our scheme can also be applied to other data outsourcing systems such as database system, video-on-demand system, etc.

## 7. Conclusion

In this paper, we proposed a KP-ABSC with key exposure protection and delegated calculation for data outsourcing systems. Our scheme achieves flexible access management along with verification over the encrypted data. During the process of data sharing, data receivers can delegate most of the de-signcryption task to data server, which will relieve the client devices from heavy calculation. By performance analysis, our scheme is shown to be secure and achieves high efficiency at the same time.

## References

[1] V. Goyal, O. Pandey, A. Sahai and B. Waters, “Attribute Based Encryption for Fine-Grained Access Control of Encrypted Data,” in *Proc. of ACM conference on Computer and Communications Security*, pp. 89-98.Oct.30-Nov.3, 2006. Article (CrossRef Link)

[2] Han ND, Han LZ, Tuan DM, In HP, Jo M, "A scheme for Data Confidentiality in Cloud-assisted Wireless Body Area Networks,” *Information Sciences*, vol. 284, no.10, pp 157-166, Nov.,2013. Article (CrossRef Link)

[3] Waters, B., “Ciphertext policy attribute based encryption: an expressive, efficient, and provably secure realization,” in *Proc. of Int. Conf. PKC 2011*, pp. 53-70, Mar. 6-9, 2011. Article (CrossRef Link)

[4] A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, “Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption,” in *Proc. of Advances in Cryptology—EUROCRYPT 2010*, pp. 62-91, Springer, Berlin, Germany, May 30-Jun.3,2010. Article (CrossRef Link)

[5] A. Lewko and B. Waters, “Decentralizing attribute-based encryption,” in *Proc. of Advances in Cryptology–EUROCRYPT 2011*, pp.568–588, May 15-19, 2011. Article (CrossRef Link)

[6] M.Green, S. Hohenberger, B.Waters, “Outsourcing the decryption of ABE ciphertexts,” in *Proc. of the 20th USENIX conference on Security (SEC'11)*, Berkeley, CA, USA, 2011. Article (CrossRef Link)

[7] J. Han, W. Susilo, Y. Mu, and J. Yan, “Privacy-preserving decentralized key-policy attribute-based encryption,” in *Proc. of 2012 IEEE Transactions on Parallel and Distributed Systems*, vol.23, no.11, pp.2150-2162, Nov.,2012. Article (CrossRef Link)

[8] Li J, Ren K, Zhu B, "Privacy-Aware Attribute-Based Encryption with User Accountability," *Volume 5735 of the series Lecture Notes in Computer Science*, pp. 347-362,Sep.7-9,2009. Article (CrossRef Link)

[9] Y. Zheng, "Digital Signcryption or How to Achieve Cost (Signature &Encryption) ≪Cost (Signature) + Cost (Encryption)," *Advances in Cryptology — CRYPTO '97*, pp.165–179, California, USA August 17–21, 1997. Article (CrossRef Link)

[10] Hong HS, Sun ZX, "An efficient and secure attribute based signcryption scheme with LSSS access structure," *SpringerPlus*, vol.5, no.1, pp.1-10, Dec., 2016. Article (CrossRef Link)

[11] Wang CJ, Huang JS, "Attribute based Signcryption with Ciphertext policy and Claim predicate Mechanism," in *Proc. of 2011 Seventh International Conference on Computational Intelligence and Security*, pp. 905-909, Sanya, China, Dec. 3-4, 2011. Article (CrossRef Link)

[12] Hu CQ, Zhang N, "Body Area Network Security: A Fuzzy Attribute-Based Signcryption Scheme," *IEEE Journal on Selected Areas in Communications/SUPPLEMENT*, vol.31, no.9, pp 37-46, Sep., 2013. Article (CrossRef Link)

[13] Lai JZ, Deng Robert, Guan CW, "Attribute-Based Encryption With Verifiable Outsourced Decryption," *IEEE Transactions on Information Forensics and Security* ,vol 8,no 8, pp 1343 – 1354, Aug., 2013. Article (CrossRef Link)

[14] Qin BD, Deng Robert, et al., "Attribute-Based Encryption with Efficient Verifiable Outsourced Decryption," *IEEE Transactions on Information Forensics and Security*, vol.10, no.7, pp 1384-1393, Jul., 2015. Article (CrossRef Link)

[15] Liu ZS, Yan HY, Li ZK, "Server-aided anonymous attribute-based authentication in cloud computing," *Future Generation Computer Systems*, vol 52, pp 61-66, Feb. 2015. Article (CrossRef Link)

[16] Ma H, Zhang R, Wan ZG, et al., "Verifiable and Exculpable Outsourced Attribute-Based Encryption for Access Control in Cloud Computing," *IEEE Transactions on Dependable and Secure Computing,online*, Nov., 2015. Article (CrossRef Link)

[17] Fang YJ, Wen ZL, Shen QN, et al., "POSTER: Ciphertext-Policy Attribute-Based Encryption Method with Secure Decryption Key Generation and Outsourcing Decryption of ABE Ciphertexts," *Volume 164 of the series Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, pp 585-589,Jan.,2016. Article (CrossRef Link)

[18] Hong HS, Zhixin Sun and Ximeng Liu, "A key-insulated CP-ABE with key exposure accountability for secure data sharing in the cloud," *KSII Transactions on Internet and Information Systems*, vol. 10, no. 5, pp. 2394-2406, May., 2016. Article (CrossRef Link)

[19] Chen L, Cheng Z, and Smart N P., "Identity-based key agreement protocols from Pairings," *International Journal of Information security*, vol.6, no.4, pp. 213-241, Jul., 2007. Article (CrossRef Link)

[20] Attrapadung N, Libert B, De Panafieu E., "Expressive key-policy attribute-based encryption with constant-size ciphertexts," in *Proc. of Public Key Cryptography—PKC 2011*, vol. 6571 of LNCS. Springer, pp. 90-108, Mar. 6-9, 2011. Article (CrossRef Link)

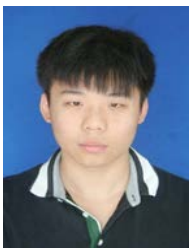
[21] Hong HS, Sun ZX, "High efficient key-insulated attribute based encryption scheme without bilinear pairing operations," *SpringerPlus*, vol.5, no.1, pp.1-12, Dec., 2016. Article (CrossRef Link)

[22] P.Vijayakumar, M.Azees, A.Kannan, L.Jegatha Deborah, "Dual Authentication and Key Management Techniques for Secure Data Transmission in Vehicular Ad-hoc Networks," *IEEE Transactions on Intelligent Transportation Systems*, vol.17, no.4, 1015 - 1028, 2016. Article (CrossRef Link)

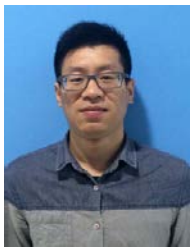
[23] P.Vijayakumar, R.Naresh, L. Jegatha Deborah, SK Hafizul Islam, "Computation Cost Efficient Group Key Agreement Protocol for Secure Peer to Peer Communication," *Security and Communication Networks, Wiley, Accepted for Publication*, DOI:10.1002/Sec. 1578. 2016. Article (CrossRef Link)

[24] P.Vijayakumar, R.Naresh, SK Hafizul Islam, L. Jegatha Deborah "An Effective Key Distribution for Secure Internet Pay-TV using Access Key Hierarchies," *Security and Communication*

*Networks*, Wiley,. DOI: 10.1002/sec.1680. Oct. 2016. Article (CrossRef Link)
[25] P.Vijayakumar, S. Bose, A. Kannan, L.Jegatha Deborah, "Computation and Communication Efficient Key Distribution Protocol for Secure Multicast Communication," *KSII Transactions on Internet and Information Systems*, Vol.7, No.4, pp.878-894, 2013. Article (CrossRef Link)
[26] Minho Jo, Nguyen Thi Thanh Huyen, Dung Nguyen, Eui-nam Huh., "A Beneficial Analysis of Deployment Knowledge for Key Distribution in Wireless Sensor Networks," *Security and Communication Networks*, vol.5, no.5 pp.485-495, May., 2012. Article (CrossRef Link)
[27] Guo ZZ, Li MC, Fan XX, "Attribute-based ring signcryption scheme," *Security and Communication Networks*, vol.6, no.6, pp.790-796, Jun., 2013. Article (CrossRef Link)
[28] Wei J, Hu X, Liu W., "Traceable attribute-based signcryption," *Security and Communication Networks*, vol.7, no.12, pp. 2302-2317, Dec. 2015. Article (CrossRef Link)



**Dr Hanshu Hong** is a PHD candidate in Nanjing University of Posts and Telecommunications. He received his B.S degree from Nanjing University of Posts and Telecommunications in 2013. His research area mainly includes information security, cryptology.



**Dr Yunhao Xia** is a PHD candidate in Nanjing University of Posts and Telecommunications. He received his B.S degree from Nanjing University of Posts and Telecommunications in 2013. His research area mainly includes computer science, soft computing.

**Dr Zhixin Sun** is the dean of Internet of Things institute, Nanjing University of Posts and Telecommunications. He received his PHD degree in Nanjing University of Aeronautics and Astronautics, China in 1998 and worked as a post doctor in Seoul National University, South Korea between 2001 and 2002. He has published more than 50 literatures on journals worldwide. His research area includes information security, computer networks, computer science, etc.

**Dr Ximeng Liu** is a research fellow in Singapore Management University. His research is in the areas of cryptography and network security.