CONCURRENCY AND COMPUTATION: PRACTICE AND EXPERIENCE
Concurrency Computat.: Pract. Exper. 2016; **28**:1237–1245
Published online 18 August 2015 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/cpe.3623

SPECIAL ISSUE PAPER

Security analysis of a privacy-preserving decentralized ciphertext-policy attribute-based encryption scheme

Minqian Wang, Zhenfeng Zhang*,† and Cheng Chen

Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing, China

SUMMARY

As it does not require a central authority or the cooperation among multiple authorities, decentralized attribute-based encryption is an efficient and flexible multi-authority attribute-based encryption system. In most existing multi-authority attribute-based encryption schemes, a global identifier (GID) is introduced to act as the linchpin to resist collusion attacks. Because GID as well as some sensitive attributes used to apply for secret keys will lead to the compromise of user's privacy, some schemes towards solving these privacy issues have been proposed. Nevertheless, only the privacy of GID was considered in prior works. Recently in ESORICS 2014, Han *et al.* put forward a privacy-preserving decentralized ciphertext-policy attribute-based encryption scheme in the standard model to address the additive privacy of attributes. In their work, a privacy-preserving key extract protocol is presented to protect both user's identifier and attributes. In this paper, we point out the security weakness of the scheme of Han *et al.* We present a collusion attack on their basic decentralized ciphertext-policy attribute-based encryption scheme and additionally show that the privacy protection of attributes in their privacy-preserving key extract protocol cannot be provided.

Received 10 April 2015; Revised 25 June 2015; Accepted 21 July 2015

KEY WORDS: privacy-preserving; decentralized attribute-based encryption; security analysis

1. INTRODUCTION

As a new public-key encryption paradigm, attribute-based encryption (ABE) is deemed to be a capable primitive for implementing fine-grained access control of encrypted data. In a typical ABE system, secret keys issued by a central authority are associated with descriptive attributes $\mathbf{x}$, ciphertexts are labeled with attributes $\mathbf{y}$, and a secret key decrypts the ciphertext if and only if $\mathbf{P}(\mathbf{x}, \mathbf{y}) = 1$ for some boolean predicate $\mathbf{P}$. To mitigate the key escrow issue, Chase [1] introduced the concept of multi-authority ABE system, allowing multiple authorities to manage attributes and distribute users the corresponding secret keys collaboratively. Then, Lewko and Waters [2] proposed a new multi-authority ABE, named decentralized ABE, where any party can act as an authority and work independently without a central authority or any coordination.

One technique hurdle in constructing multi-authority ABE scheme is to make it collusion resistance. To that end, a unique global identifier (GID), tying a user's private key components obtained from different authorities together, was utilized in prior works [1–5]. Thus, to obtain corresponding secret keys, a user must submit his attributes along with his GID to each authority. However, the use of a consistent GID as well as some sensitive attributes may be exploited by

*Correspondence to: Zhenfeng Zhang, Trusted Computing and Information Assurance Laboratory, Institute of Software, Chinese Academy of Sciences, Beijing, China.
†E-mail: zfzhang@tca.iscas.ac.cn

malicious authorities. More specifically, multiple malicious authorities can cooperate to pool the user's attributes by tracing his GID and then they can identify the target user or even personate him for illegal activities. Furthermore, some sensitive attributes (without GID) is sufficiently used to identify a specific user or lead to user's privacy disclosure, like attributes describing one's medical or financial status. Hence, the protection of user's privacy is an essential demand in many applications, especially in decentralized ABE system where each authority seems not to be fully trusted.

Focusing on privacy issues in multi-authority ABE, some schemes have been proposed [3–5], whereas only the privacy of GID is considered. Very recently, Han *et al.* [6] claimed to provide a complete solution to these issues compared with previous schemes. They put forward a privacy-preserving decentralized ciphertext-policy attribute-based encryption (PPDCP-ABE) scheme in the standard model, for which, a privacy-preserving key extract protocol was presented to keep both user's identifier and attributes private. Namely, a user can obtain secret keys from multiple authorities without revealing any information about his GID and attributes.

In this paper, we give a security analysis of PPDCP-ABE scheme of Han *et al.* Firstly, we observe that their basic decentralized ciphertext-policy ABE scheme cannot resist collusion attacks. Secondly, we show an attack on their privacy-preserving key extract protocol, which allows the authority to reveal user's credentials, hence, the privacy protection of attributes cannot be provided.

The remainder of this paper is organized as follows. In Section 2, we give a brief review of PPDCP-ABE scheme of Han *et al.* [6]. In Section 3 and Section 4, we respectively present our security analysis on basic decentralized ciphertext-policy ABE scheme and privacy-preserving key extract protocol. We conclude the paper in Section 5.

2. REVIEW OF PRIVACY-PRESERVING DECENTRALIZED CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTION SCHEME OF HAN *ET AL.*

In this section, we give the necessary background on decentralized ciphertext-policy attribute-based encryption (DCP-ABE) scheme and then present a brief review of the scheme of Han *et al.* [6]: They firstly constructed a DCP-ABE scheme in the standard model and then replaced the key-generating algorithm with a privacy-preserving key extract protocol. We refer the reader to the original article [6] for more details.

2.1. Decentralized ciphertext-policy attribute-based encryption scheme

In a DCP-ABE system, without requirement of a central authority or any global cooperation, any party can become an authority and issue private keys to users. Ciphertext is generated under a policy written over attributes monitored by multiple authorities. A user obtains private keys from different authorities and is able to decrypt if his attributes match the policy specified in the ciphertext. The basic security requirement of DCP-ABE is collusion resistance, that is, preventing any group of unauthorized users to decrypt the ciphertext successfully. Hence, in the security model, the adversary is allowed to query for any private keys that cannot decrypt the challenge ciphertext.

The formal definition of DCP-ABE system and its security model is given in Appendix A.

2.2. Basic decentralized ciphertext-policy attribute-based encryption scheme of Han et al.

The basic DCP-ABE scheme in [6] is roughly as follows:

- *Global setup*: Let $\{\mathbb{G}, \mathbb{G}_{\mathbb{T}}\}$ be groups of prime order p, with an efficient computable mapping $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_{\mathbb{T}}$. Let g, h, and f be generators of $\mathbb{G}$. Assume there are N authorities $\{A_1, A_2, \ldots A_N\}$, and A_i monitors attribute-set $\tilde{A}_i = \{a_{i,1}, a_{i,2}, \ldots, a_{i,n_i}\}$ for $i = 1, 2, \ldots, N$. Then publish the public parameters: $PP = (g, h, f, e, p, \mathbb{G}, \mathbb{G}_{\mathbb{T}})$.
- *Authorities setup*: For each authority A_i, it randomly selects $\alpha_i, x_i, \beta_i, \gamma_i \in Z_p$ and sets $H_i = e(g, g)^{\alpha_i}$, $A_i = g^{x_i}$, $B_i = f^{\beta_i}$, $\Gamma_i^1 = g^{\gamma_i}$ and $\Gamma_i^2 = h^{\gamma_i}$. Then, it randomly chooses $z_{i,j} \in Z_p$ for each attribute $a_{i,j} \in \tilde{A}_i$ and computes $Z_{i,j} = g^{z_{i,j}}$ and $T_{i,j} = h^{z_{i,j}} g^{\frac{1}{\gamma_i + a_{i,j}}}$.

DOI: 10.1002/cpe

Then, $\breve{A}_i$ publishes the public key $PK_i = \left\{H_i, A_i, B_i, (\Gamma_i^1, \Gamma_i^2), (Z_{i,j}, T_{i,j})_{a_{i,j} \in \tilde{A}_i}\right\}$ and keeps the master secret key as $SK_i = \left(\alpha_i, x_i, \beta_i, \gamma_i, (z_{i,j})_{a_{i,j} \in \tilde{A}_i}\right)$.

- *Encrypt*: When encrypting a message $m \in \mathbb{G}_T$, it works as follows.

  Let I be a set that consists of the indexes of the authorities whose attributes are selected to encrypt m. For each $j \in I$, this algorithm first selects an access structures (M_j, ρ_j) and a vector $\overrightarrow{v_j} = \left(s_j, v_{j,2}, \ldots, v_{j,n_j}\right)$, where $s_j, v_{j,2}, \ldots, v_{j,n_j}$ is randomly chosen from Z_p, and M_j is an $l_j \times n_j$ matrix. Then, it computes $\lambda_{j,i} = M_j^i \overrightarrow{v_j}$, where M_j^i is the corresponding ith row of M_j. Finally, it selects $r_{j,1}, r_{j,2}, \ldots, r_{j,l_j} \in_R Z_p$ and generates the ciphertext $\mathbf{C}$ as follows:

$$C_0 = m \cdot \prod_{j \in I} e(g,g)^{\alpha_j s_j},\ \left\{X_j = g^{s_j},\ Y_j = f^{s_j},\ E_j = B_j^{s_j}\right\}_{j \in I}$$

$$\left\{\left(C_{j,i} = g^{x_j \lambda_{j,i}} Z_{\rho_j(i)}^{-r_{j,i}},\ D_{j,i} = g^{r_{j,i}}\right)_{i=1,\ldots,l_j}\right\}_{j \in I}$$

- *KeyGen*: For a user U with attribute-set $\tilde{U}$ and GID u, $\breve{A}_i$ randomly selects $t_{U,i}, w_{U,i} \in Z_p$, and computes

$$K_i = g^{\alpha_i} g^{x_i w_{U,i}} f^{t_{U,i}} f^{\frac{\beta_i + u}{t_{U,i}}},\ P_i = g^{w_{U,i}},\ L_i = g^{t_{U,i}},\ R_i = g^{\frac{1}{t_{U,i}}},\ \left(F_x = Z_x^{w_{U,i}}\right)_{a_x \in \tilde{U} \cap \tilde{A}_i}.$$

- *Decrypt*: To decrypt a ciphertext $\mathbf{C}$, the user computes

$$\frac{C_0 \cdot \prod_{j \in I} e(L_j, Y_j) e(R_j, E_j) e(R_j, Y_j)^u \prod_{j \in I} \prod_{i=1}^{l_j} \left(e(C_{j,i}, P_j) e(D_{j,i}, F_{\rho_j(i)})\right)^{\omega_{j,i}}}{\prod_{j \in I} e(K_j, X_j)} = m,$$

  where $\{\omega_{j,i} \in Z_p\}_{i=1}^{l_j}$ is a set of constants such that $\sum_{i=1}^{l_j} \omega_{j,i} \lambda_{j,i} = s_j$, if $\{\lambda_{j,i}\}_{i=1}^{l_j}$ are valid shares of the secret value s_j according to the access structure (M_j, ρ_j).

The correctness of scheme is given in Appendix B.

In addition, under the decisional q-BDHE assumption, the DCP-ABE scheme described previously is claimed to be provably secure in selective security model.

Remark 1

As shown previously, the policy attached to the ciphertext in [6] is defined as $(M_i, \rho_i)_{i \in I}$. That is to say, to encrypt a message m under attributes monitored by authorities $\{\breve{A}_i\}_{i \in I}$, the encryptor selects an access structure (M_i, ρ_i) for each $\breve{A}_i$ and takes the conjunction of all these (M_i, ρ_i), namely, $\bigcap_{i \in I} (M_i, \rho_i)$, as the policy of the encryption algorithm. Here, we note that, $(M_i, \rho_i)_{i \in I}$ is one kind of restricted policy according to the definition of DCP-ABE. For instance, when $I = \{1, 2, 3\}$, the DCP-ABE scheme in [6] only supports the conjunctive relations between authorities: $(M_1, \rho_1) \cap (M_2, \rho_2) \cap (M_3, \rho_3)$, but cannot describe more general policies, like $(M_1, \rho_1) \cup ((M_2, \rho_2) \cap (M_3, \rho_3))$.

2.3. Privacy-preserving key extract protocol of Han et al.

Intended to provide protection of both user's identifier and attributes, the privacy-preserving key extract protocol is proposed by Han *et al.* to replace the key generation algorithm of basic DCP-ABE scheme. It is claimed to satisfy two properties: leak-freeness and selective-failure

DOI: 10.1002/cpe

blindness. The protocol is executed between an authority $\breve{A}_i$ with PK_i, SK_i and a user U with attribute-set $\tilde{U}$ and GID u. A detailed description follows.

1. User U firstly randomly selects $k_1, k_2, d_1, d_2 \in Z_p$ and sets $d_u = d_1 d_2$. Then computes $\theta_1 = {A_i}^{d_1}$, $\theta_2 = g^{d_u}$, $\theta_3 = h^{k_1} f^u$, $\theta_4 = \theta_3^{k_2}$, $\theta_5 = B_i^{k_2}$, $\theta_6 = f^{\frac{1}{k_2}}$, $\{\psi_x^1 = T_x^{d_u}, \psi_x^2 = Z_x^{d_u}\}$ for each $a_x \in \tilde{U} \cap \tilde{A}_i$ and runs a proof of knowledge $\sum_U = PoK\{(k_1, k_2, d_1, d_2, u, (a_x \in \tilde{U} \cap \tilde{A}_i)) : \theta_1 = {A_i}^{d_1} \wedge \theta_2 = g^{d_u} \wedge \theta_3 = h^{k_1} f^u \wedge \theta_4 = \theta_3^{k_2} \wedge \theta_5 = B_i^{k_2} \wedge (\wedge \frac{e(\Gamma_i^1, \psi_x^1)}{e(\Gamma_i^2, \psi_x^2)} = e(g, \psi_x^1)^{-a_x} e(h, \psi_x^2)^{a_x} e(g, g)^{d_u})_{a_x \in \tilde{U} \cap \tilde{A}_i}\}$.
2. $\breve{A}_i$ checks the proof and aborts if it fails. Otherwise, $\breve{A}_i$ randomly selects $c_u, e_u \in Z_p$ and computes $\Upsilon_1 = g^{c_u}, \Upsilon_2 = g^{\frac{1}{c_u}}, \Upsilon_3 = h^{c_u}, \Upsilon_4 = h^{\frac{1}{c_u}}, \Upsilon_5 = g^{e_u}, \bar{K}_i = g^{\alpha_i} \theta_1^{e_u} \theta_6^{c_u} (\theta_4 \theta_5)^{\frac{1}{c_u}}$, and $\phi_x = (\psi_x^2)^{e_u}$ for each $a_x \in \tilde{U} \cap \tilde{A}_i$, and runs a proof of knowledge $\sum_{A_i} = PoK\{(\alpha_i, c_u, e_u) : e(\Upsilon_1, \Upsilon_2) = e(g, g) \wedge \Upsilon_1 = g^{c_u} \wedge \Upsilon_2 = g^{\frac{1}{c_u}} \wedge \Upsilon_3 = h^{c_u} \wedge \Upsilon_4 = h^{\frac{1}{c_u}} \wedge e(\Upsilon_3, \Upsilon_4) = e(h, h) \wedge \Upsilon_5 = g^{e_u} \wedge \bar{K}_i = g^{\alpha_i} \theta_1^{e_u} \theta_6^{c_u} (\theta_4 \theta_5)^{\frac{1}{c_u}} \wedge (\wedge \phi_x = (\psi_x^2)^{e_u})_{a_x \in \tilde{U} \cap \tilde{A}_i}\}$. Send $\Upsilon_1, \Upsilon_2, \Upsilon_3, \Upsilon_4, \Upsilon_5, \bar{K}_i, \phi_x$ to the user U.
3. User U checks the proof and aborts if it fails. Otherwise, he computes $K_i = \frac{\bar{K}_i}{{\Upsilon_4}^{k_1 k_2}}$, $P_i = \Upsilon_5^{d_1}$, $L_i = \Upsilon_1^{\frac{1}{k_2}}, R_i = \Upsilon_2^{\frac{1}{k_2}}, (F_x = \phi_x^{\frac{1}{d_2}})_{a_x \in \tilde{U} \cap \tilde{A}_i}$ as his secret key.

3. ANALYSIS OF BASIC DECENTRALIZED CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTION SCHEME OF HAN *ET AL.*

In a DCP-ABE system, any user can encrypt messages under a specific policy over attributes managed by multiple authorities, and a user is permissible to decrypt if and only if his attributes (maybe monitored by different authorities) satisfy the policy in the ciphertext. Because multiple authorities work independently, malicious users may combine their secret keys to create a new key for decryption. Therefore, the basic security requirement for multi-authority ABE is collusion resistance, namely, any group of users holding secret keys for different attributes learns nothing about the plaintext if none of them is individually authorized to decrypt the ciphertext. To that end, the concept of GID was introduced to tie a user's secret key components obtained from different authorities as an integrality, for example, [2, 5].

Unfortunately, we find that the basic DCP-ABE scheme of Han *et al.* [6] is not secure against collusion attacks. We will show a collusion attack where several unauthorized users combine their secret keys together and then decrypt the ciphertext successfully, yet each user's attribute-set does not satisfy the policy attached to the ciphertext.

3.1. Collusion attack on decentralized ciphertext-policy attribute-based encryption scheme

Without loss of generality, assume $I = \{1, 2\}$. Then, according to the *Encrypt* algorithm, the ciphertexts $\mathbf{C}$ associated with policy $(M_1, \rho_1) \cap (M_2, \rho_2)$ is computed as follows:

$$C_0 = m \cdot \prod_{j=1,2} e(g, g)^{\alpha_j s_j} = m e(g, g)^{\alpha_1 s_1 + \alpha_2 s_2},$$

$$\left\{X_j = g^{s_j}, Y_j = f^{s_j}, E_j = B_j^{s_j}\right\}_{j=1,2}$$

$$\left\{\left(C_{j,i} = g^{x_j \lambda_{j,i}} Z_{\rho_j(i)}^{-r_{j,i}}, D_{j,i} = g^{r_{j,i}}\right)_{i=1,\ldots,l_j}\right\}_{j=1,2}$$

Assume there are two users $U1$, $U2$ with identifier u_1 and u_2, respectively. In addition, user $U1$ owns attribute-set S_1 whose elements are monitored by authority $\breve{A}_1$, and S_1 only satisfies the access structure (M_1, ρ_1) but not (M_2, ρ_2); similarly, User U_2 owns attribute-set S_2 whose elements are

DOI: 10.1002/cpe

monitored by authority $\breve{A}_2$, and S_2 only satisfies the access structure (M_2, ρ_2) but not (M_1, ρ_1). Two users can get their secret keys from $\breve{A}_1$, $\breve{A}_2$, respectively:

$$U1: K_1 = g^{\alpha_1} g^{x_1 w_{U,1}} f^{t_{U,1}} f^{\frac{\beta_1+u_1}{t_{U,1}}}, P_1 = g^{w_{U,1}}, L_1 = g^{t_{U,1}}, R_1 = g^{\frac{1}{t_{U,1}}}, \left(F_x = Z_x^{w_{U,1}}\right)_{a_x \in S_1}$$

$$U2: K_2 = g^{\alpha_2} g^{x_2 w_{U,2}} f^{t_{U,2}} f^{\frac{\beta_2+u_2}{t_{U,2}}}, P_2 = g^{w_{U,2}}, L_2 = g^{t_{U,2}}, R_2 = g^{\frac{1}{t_{U,2}}}, \left(F_y = Z_y^{w_{U,2}}\right)_{a_y \in S_2}$$

Note that, because the policy $(M_1, \rho_1) \cap (M_2, \rho_2)$ for the aforementioned encryption is not satisfied by S_i for $i = 1, 2$, neither $U1$ nor $U2$ can decrypt the target ciphertext $\mathbf{C}$ alone. However, $U1$ and $U2$ are capable of recovering the message m collaboratively through the following computation based on the respective match between S_i and (M_i, ρ_i) for $i = 1, 2$:

$$U1: \frac{e(L_1, Y_1)e(R_1, E_1)e(R_1, Y_1)^{u_1} \prod_{i=1}^{l_1} \left(e(C_{1,i}, P_1)e(D_{1,i}, F_{\rho_1(i)})\right)^{\omega_{1,i}}}{e(K_1, X_1)} = e(g, g)^{\alpha_1 s_1}$$

$$U2: \frac{e(L_2, Y_2)e(R_2, E_2)e(R_2, Y_2)^{u_2} \prod_{i=1}^{l_2} \left(e(C_{2,i}, P_2)e(D_{2,i}, F_{\rho_2(i)})\right)^{\omega_{2,i}}}{e(K_2, X_2)} = e(g, g)^{\alpha_2 s_2}.$$

Therefore,

$$\frac{C_0 \cdot \prod_{j=1,2} e(L_j, Y_j)e(R_j, E_j)e(R_j, Y_j)^{u_j} \prod_{j=1,2} \prod_{i=1}^{l_j} (e(C_{j,i}, P_j)e(D_{j,i}, F_{\rho_j(i)}))^{\omega_{j,i}}}{\prod_{j=1,2} e(K_j, X_j)} = m,$$

where $\{\omega_{j,i} \in Z_p\}_{i=1}^{l_j}$ is a set of constants such that $\sum_{i=1}^{l_j} \omega_{j,i} \lambda_{j,i} = s_j$ if $\{\lambda_{j,i}\}_{i=1}^{l_j}$ are valid shares of the secret value s_j according to the access structure (M_j, ρ_j).

As shown previously, an encrypted data with policy $(M_1, \rho_1) \cap (M_2, \rho_2)$ is accessible to a pair of unauthorized users $U1$ and $U2$, while each user's attribute-set S_i only matches the access structure (M_i, ρ_i), which is assigned to authority $\tilde{A}_i$ and acts as a part of the encryption policy.

3.2. Discussion

As can be seen, the scheme of Han *et al.* [6] followed the concept of GID to resist collusion attacks among users with different GIDs. Unfortunately, their way of using GID cannot provide the intended security.

Now, we try to make clear the reason why the basic DCP-ABE scheme of Han *et al.* cannot prevent users from implementing collusion attacks. Firstly, we present three useful observations about the scheme itself:

- *Observation1* : Let $s = \sum_{j \in I} \alpha_j s_j$. In the ciphertext, the element $e(g, g)^s = e(g, g)^{\sum_{j \in I} \alpha_j s_j} = \prod_{j \in I} e(g, g)^{\alpha_j s_j}$ is used to blind the message m. Moreover, the aforementioned equation can be regarded as an implement of secret sharing: each $\alpha_j s_j$ in exponent is a secret share of the main secret s.
- *Observation2* : For each $j \in I$, a user with GID u and attribute-set S is able to recover a target element $e(g, g)^{\alpha_j s_j}$ (with secret share $\alpha_j s_j$ in the exponent), as long as S satisfies the single access structure (M_j, ρ_j), which is assigned to the authority $\breve{A}_j$:

$$\frac{e\left(L_j, Y_j\right) e\left(R_j, E_j\right) e\left(R_j, Y_j\right)^u \prod_{i=1}^{l_j} \left(e\left(C_{j,i}, P_j\right) e\left(D_{j,i}, F_{\rho_j(i)}\right)\right)^{\omega_{j,i}}}{e\left(K_j, X_j\right)} = e(g, g)^{\alpha_j s_j}.$$

DOI: 10.1002/cpe

- *Observation3* : The identifier GID is not needed in the course of combining secret shares $\{\alpha_j s_j\}_{j\in I}$ to recover the main secret s. Once $e(g,g)^{\alpha_j s_j}$ for all $j \in I$ is obtained, the blindness element $e(g,g)^s = e(g,g)^{\sum_{j\in I}\alpha_j s_j}$ is easily computed to retrieve the message m. (Our collusion attack is exactly based on this weakness.)

Informally, the flaw in constructing the DCP-ABE scheme of [6] lies in that the binding of GID seems not to be kept all long the decryption. More precisely, GID is utilized in the computing of the corresponding secret share for each authority, that is, $e(g,g)^{\alpha_j s_j}$, but the consistency of GID makes no influence on the final step of combining $e(g,g)^{\alpha_j s_j}$ for all $j \in I$ to recover $e(g,g)^s$ $(= e(g,g)^{\sum_{j\in I}\alpha_j s_j})$.

As a consequence, the collusion attack can be generalized as the following: Suppose the ciphertext is associated with policy $(M_i, \rho_i)_{i\in I}$, a group of unauthorized users (none of their attribute-set satisfies policy $(M_i, \rho_i)_{i\in I}$) is able to access the encrypted data successfully, as long as they could individually obtain shares $e(g,g)^{\alpha_j s_j}$ under authority $\breve{A}_i$ for all $j \in I$ and then collude to compute $e(g,g)^{\sum_{j\in I}\alpha_j s_j}$. Thus, the basic DCP-ABE scheme of Han *et al.* [6] fails to meet the security requirement of collusion resistance.

4. ANALYSIS OF PRIVACY-PRESERVING KEY EXTRACT PROTOCOL OF HAN *ET AL.*

Motivated by a blind IBE scheme [7], the privacy-preserving extract protocol in the scheme of Han *et al.* [6] is designed to prevent the authorities from knowing both user's identifier and his attributes. The basic idea underlying is that, user U firstly makes commitments to identifier GID and each attribute and then authority $\breve{A}_i$ and user U cooperatively compute the secret key by executing a two-party secure computing protocol. Indeed, the privacy of GID in [6] can be obtained. However, we will show that it fails to provide the privacy protection of attributes. Precisely, the values user sending in the protocol allow the authority $\breve{A}_i$ to figure out the attributes information.

Now, we present the concrete attack:

Considering a protocol executed between an authority $\breve{A}_i$ and a user U with attribute-set $\tilde{U}$ and GID u. Authority $\breve{A}_i$ is in possession of all $\{Z_{i,j} = g^{z_{i,j}}\}$, each corresponding to an attribute $a_{i,j}$ he monitored. After executing the first move of the protocol, authority $\breve{A}_i$ becomes to know these values (We only list the components related to attributes.): $\theta_2 = g^{d_u}$ and $\{\psi_x^1 = T_x^{d_u}, \psi_x^2 = Z_x^{d_u}\}_{a_x\in\tilde{U}\cap\tilde{A}_i}$. Given all these values, authority $\breve{A}_i$ can perform the following operations: For each ψ_x^2 he received, $\breve{A}_i$ checks whether Equation (1) holds for all $\{Z_{i,j}\}$ he has.

$$e(\theta_2, Z_x) = e\left(\psi_x^2, g\right) \tag{1}$$

If the equation holds for some $Z_{i,j}$, authority $\breve{A}_i$ can conclude to some extent that attribute $a_{i,j}$ corresponded with this $Z_{i,j}$ is exactly what the user owns. After the checks of all $\{Z_{i,j}\}$, the credentials of the user under authority $\breve{A}_i$ will be revealed.

To explain the reason why privacy-preserving protocol of [6] is vulnerable to such attack, we start from the intuition behind the protocol design. The authors of [6] mentioned that d_u is used to commit user's attributes and the corresponding authentication tags $\{T_{i,j}\}$, and then user U can proceed a zero-knowledge proof to demonstrate to $\breve{A}_i$ that he knows these attributes for which he is obtaining secret keys are monitored by $\breve{A}_i$. Nevertheless, we observe that the actual dispose of an attribute in their protocol looks more like a randomization using d_u: $\{\psi_x^1 = T_x^{d_u}, \psi_x^2 = Z_x^{d_u}\}$, rather than a commitment. More seriously, the element $\theta_2 = g^{d_u}$ corresponding to d_u is also given out, which makes the checks performed by authority $\breve{A}_i$ described previously unavoidable. Therefore, authority $\breve{A}_i$ is able to identify user's credentials and the privacy protection of attributes in [6] can hardly achieve.

5. CONCLUSION

Recently, in ESORICS 2014, a PPDCP-ABE scheme is proposed by Han *et al.* [6], and it was claimed to realize a stronger privacy of both user's identifier and attributes. In this paper, we gave

DOI: 10.1002/cpe

a security analysis and discussed two vulnerabilities of the scheme of Han *et al.* by presenting two attacks. The first is a collusion attack on their basic decentralized ciphertext-policy ABE schemes, and the second is an attack that allows the authority to recognize user's credentials, thus negating the protection of attributes. Consequently, it is still an interesting issue to construct a privacy-preserving decentralized attribute-based encryption scheme.

APPENDIX A. DEFINITIONS OF DECENTRALIZED CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTION

A decentralized ciphertext-policy attribute-based encryption scheme is composed of the following five algorithms:

Global setup $(\lambda) \rightarrow GP$ The global setup algorithm takes in the security parameter λ and outputs global parameters GP for the system.

Authority setup $(GP) \rightarrow SK, PK$ Each authority runs the authority setup algorithm with GP as input to produce its own secret key and public key pair SK, PK.

Encrypt $(M, (A, \rho), GP, \{PK\}) \rightarrow CT$ The encryption algorithm takes in a message M, an access structure (A, ρ), the set of public keys for relevant authorities $\{PK\}$, and the global parameters GP. It outputs a ciphertext CT.

KeyGen$(GID, GP, i, SK) \rightarrow K_{i,GID}$ The key generation algorithm takes in an identity GID, the global parameters GP, an attribute i belonging to some authority, and the secret key SK for this authority. It produces a key $K_{i,GID}$ for this attribute, identity pair.

Decrypt$(CT, GP, \{K_{i,GID}\}) \rightarrow M$ The decryption algorithm takes in the global parameters GP, the ciphertext CT, and a collection of keys corresponding to attributes, identity pairs all with the same fixed identity GID. It outputs either the message M when the collection of attributes i satisfies the access structure corresponding to the ciphertext. Otherwise, decryption fails.

Definition 1

A DCP-ABE system is said to be correct if whenever GP is obtained from the global setup algorithm, CT is obtained from the encryption algorithm on the message M, and $\{K_{i,GID}\}$ is a set of keys obtained from the key generation algorithm for the same identity GID and for a set of attributes satisfying the access structure of the ciphertext, $Decrypt(CT, GP, \{K_{i,GID}\}) = M$.

We now describe the security model for decentralized attribute-based encryption. Assume that adversary can statically corrupt some authorities, but make adaptive key queries. Let S denotes authorities set, and U denotes the universe of attributes.

Setup The global setup algorithm is run. The attacker specifies a set $S' \subseteq S$ of corrupt authorities. For non-corrupt authorities in $S - S'$, the challenger obtain public key, private key pairs by running the authority setup algorithm, and gives the public keys to the attacker.

KeyQuery Phase 1 The attacker makes key queries by submitting pairs (i, GID) to the challenger, where i is an attribute belonging to a non-corrupt authority. The challenger responds by giving the attacker the corresponding key $\{K_{i,GID}\}$.

Challenge Phase The attacker specifies two message M_0, M_1 and an access structure (A, ρ). The access matrix must satisfy the following constraint. We let V denote the subset of rows of A labeled by attributes controlled by corrupt authorities. For each identity GID, let V_{GID} denote the subset of rows of A labeled by attribute i for which the attacker has queried (i, GID). For each GID, the subspace spanned by $V \cup V_{GID}$ is not include $(1, 0, \ldots, 0)$. The challenger flips a random coin $\beta \in \{0, 1\}$ and sends the attacker an encryption of M_β under access matrix (A, ρ).

KeyQuery Phase2 The attacker may submit additional key queries (i, GID), as long as they meet the requirement described previously.

Guess The attacker submit a guess β' for β. The attacker wins if $\beta = \beta'$. The attacker's advantage in this game is defined to be $Pr[\beta = \beta'] - \frac{1}{2}$.

Definition 2

A DCP-ABE system is adaptively secure if all polynomial time attackers have at most a negligible advantage in this security game.

DOI: 10.1002/cpe

Selective security is defined by adding an initialization phase where the attacker is asked to declare the challenge access structure before seeing the public parameters.

APPENDIX B. CORRECTNESS OF DECENTRALIZED CIPHERTEXT-POLICY ATTRIBUTE-BASED ENCRYPTION SCHEME OF HAN *ET AL.*

The decryption algorithm of DCP-ABE of Han *et al.* is

$$\frac{C_0 \cdot \prod_{j\in I} e\left(L_j, Y_j\right) e\left(R_j, E_j\right) e\left(R_j, Y_j\right)^u \prod_{j\in I} \prod_{i=1}^{l_j} \left(e\left(C_{j,i}, P_j\right) e\left(D_{j,i}, F_{\rho_j(i)}\right)\right)^{\omega_{j,i}}}{\prod_{j\in I} e(K_j, X_j)} = m,$$

where $\{\omega_{j,i} \in Z_p\}_{i=1}^{l_j}$ is a set of constants such that $\sum_{i=1}^{l_j} \omega_{j,i}\lambda_{j,i} = s_j$, if $\{\lambda_{j,i}\}_{i=1}^{l_j}$ are valid shares of the secret value s_j according to the access structure (M_j, ρ_j).

Correctness:

$$\begin{aligned}\prod_{j\in I} e\left(L_j, Y_j\right) e\left(R_j, E_j\right) e\left(R_j, Y_j\right)^u &= \prod_{j\in I} e\left(g^{t_{U,j}}, f^{s_j}\right) e\left(g^{\frac{1}{t_{U,j}}}, f^{\beta_j s_j}\right) e\left(g^{\frac{1}{t_{U,j}}}, f^{s_j}\right)^u \\ &= \prod_{j\in I} e(g, f)^{t_{U,j} s_j} e(g, f)^{\frac{\beta_j s_j}{t_{U,j}}} e(g, f)^{\frac{u s_j}{t_{U,j}}}\end{aligned}$$

$$\begin{aligned}\prod_{j\in I} \prod_{i=1}^{l_j} \left(e\left(C_{j,i}, P_j\right) e\left(D_{j,i}, F_{\rho_j(i)}\right)\right)^{\omega_{j,i}} &= \prod_{j\in I} \prod_{i=1}^{l_j} \left(e\left(g^{x_j \lambda_{j,i}} Z_{\rho_j(i)}^{-r_{j,i}}, g^{w_{U,j}}\right) e\left(g^{r_{j,i}}, Z_{\rho_j(i)}^{w_{U,j}}\right)\right)^{\omega_{j,i}} \\ &= \prod_{j\in I} \prod_{i=1}^{l_j} e(g, g)^{x_j w_{U,j} \lambda_{j,i}\, \omega_{j,i}} \\ &= \prod_{j\in I} e(g, g)^{x_j w_{U,j} s_j}\end{aligned}$$

$$\begin{aligned}\prod_{j\in I} e(K_j, X_j) &= \prod_{j\in I} e\left(g^{\alpha_j} g^{x_j w_{U,j}} f^{t_{U,j}} f^{\frac{\beta_j + u}{t_{U,j}}}, g^{s_j}\right) \\ &= \prod_{j\in I} e(g, g)^{\alpha_j s_j} e(g, g)^{x_j w_{U,j} s_j} e(g, f)^{t_{U,j} s_j} e(g, f)^{\frac{\beta_j s_j}{t_{U,j}}} e(g, f)^{\frac{u s_j}{t_{U,j}}}\end{aligned}$$

Therefore,

$$\frac{C_0 \cdot \prod_{j\in I} e(L_j, Y_j) e(R_j, E_j) e(R_j, Y_j)^u \prod_{j\in I} \prod_{i=1}^{l_j} \left(e\left(C_{j,i}, P_j\right) e\left(D_{j,i}, F_{\rho_j(i)}\right)\right)^{\omega_{j,i}}}{\prod_{j\in I} e(K_j, X_j)} = m$$

ACKNOWLEDGEMENTS

The authors would like to thank the editor and anonymous referees for valuable comments. This work is supported by the National Basic Research Program of China (no. 2013CB338003), the National Natural Science Foundation of China (no. 61170278), and the 863 project (no. 2012AA01A403).

DOI: 10.1002/cpe

REFERENCES

1. Chase M. Multi-authority attribute based encryption. In *Theory of Cryptography*. Springer: Berlin, Heidelberg, 2007; 515–534.
2. Lewko A, Waters B. Decentralizing attribute-based encryption. In *Advances in Cryptology-EUROCRYPT 2011*. Springer: Berlin, Heidelberg, 2011; 568–588.
3. Chase M, Chow SSM. *Improving Privacy and Security in Multi-authority Attribute-based Encryption*. ACM, 2009.
4. Ge A, Zhang J, Zhang R. Security analysis of a privacy-preserving decentralized key-policy attribute-based encryption scheme. *Parallel and Distributed Systems, IEEE Transactions on 2013* 2013; **24**(11):2319–2321.
5. Han J, Susilo W, Mu Y. Privacy-preserving decentralized key-policy attribute-based encryption. *Parallel and Distributed Systems, IEEE Transactions on 2012* 2012; **23**(11):2150–2162.
6. Han J, Susilo W, Mu Y. PPDCP-ABE: privacy-preserving decentralized ciphertext-policy attribute-based encryption. In *Computer Security-ESORICS 2014*. Springer International Publishing: Cham, Switzerland, 2014; 73–90.
7. Green M, Hohenberger S. Blind identity-based encryption and simulatable oblivious transfer. In *Advances in Cryptology-ASIACRYPT 2007*. Springer: Berlin, Heidelberg, 2007; 265–282.

DOI: 10.1002/cpe