PPDCP-ABE: Privacy-Preserving Decentralized Ciphertext-Policy Attribute-Based Encryption

Jinguang Han [1], Willy Susilo[2], Yi Mu [2], Jianying Zhou [3] and Man Ho Au [2]

[1]Jiangsu Provincial Key Laboratory of E-Business, Nanjing University of Finance and Economics, Nanjing, Jiangsu 210003, China

[2]School of Computer Science and Software Engineering, University of Wollongong, Wollongong, NSW 2522, Australia

[3]Infocomm Security Department, Institute for Infocomm Research, 1 Fusionopolis Way, Singapore 138632, Singapore

jghan22@gmail.com, {wsusilo,ymu,aau}@uow.edu.au, jyzhou@i2r.a-star.edu.sg

The 19th European Symposium on Research in Computer Security - ESORICS 2014
@ Wroclaw, Poland

September 8, 2014

Calendar

I. Introduction

In network society, users can be identified by distinct attributes.

[1] Sahai, A., Waters, B.: Fuzzy identity-based encryption. In EUROCRYPT 2005. LNCS, vol. 3494, pp. 457-473.

In network society, users can be identified by distinct attributes.

For example, European electronic identity cards often contain the attributes: nationality, sex, civil status, hair and eye color, and applicable minority status.

[1] Sahai, A., Waters, B.: Fuzzy identity-based encryption. In EUROCRYPT 2005. LNCS, vol. 3494, pp. 457-473.

In network society, users can be identified by distinct attributes.

For example, European electronic identity cards often contain the attributes: nationality, sex, civil status, hair and eye color, and applicable minority status.

Especially, these attributes are very privacy-sensitive and require a selective disclosure of one while hiding others completely; otherwise, a user can be identified and impersonated by collecting and analyzing his attributes.

[1] Sahai, A., Waters, B.: Fuzzy identity-based encryption. In EUROCRYPT 2005. LNCS, vol. 3494, pp. 457-473.

In network society, users can be identified by distinct attributes.

For example, European electronic identity cards often contain the attributes: nationality, sex, civil status, hair and eye color, and applicable minority status.

Especially, these attributes are very privacy-sensitive and require a selective disclosure of one while hiding others completely; otherwise, a user can be identified and impersonated by collecting and analyzing his attributes.

In practical applications, we often share data with some expressive attributes without knowing who will receive it. To resolve this problem, Sahai and Waters introduced the seminal concept of attribute-based encryption (ABE) [1].

[1] Sahai, A., Waters, B.: Fuzzy identity-based encryption. In EUROCRYPT 2005. LNCS, vol. 3494, pp. 457-473.

MA-ABE: To reduce the trust on the central authority, Chase proposed a multi-authority ABE (MA-ABE) scheme [2].

[2] Chase, M.: Multi-authority attribute based encryption. In TCC 2007. LNCS, vol. 4392, pp. 515-534.

[3] Lewko, A., Waters, B.: Decentralizing attribute-based encryption. In: EUROCRYPT 2011. LNCS, vol. 6632, pp. 568-588.

MA-ABE: To reduce the trust on the central authority, Chase proposed a multi-authority ABE (MA-ABE) scheme [2].

- A central authority is required;
- Authorities cooperatively initial the system.

[2] Chase, M.: Multi-authority attribute based encryption. In TCC 2007. LNCS, vol. 4392, pp. 515-534.

[3] Lewko, A., Waters, B.: Decentralizing attribute-based encryption. In: EUROCRYPT 2011. LNCS, vol. 6632, pp. 568-588.

MA-ABE: To reduce the trust on the central authority, Chase proposed a multi-authority ABE (MA-ABE) scheme [2].

- A central authority is required;
- Authorities cooperatively initial the system.

DCP-ABE: Lewko and Waters proposed a new MA-ABE scheme called decentralized CP-ABE (DCP-ABE)[3].

[2] Chase, M.: Multi-authority attribute based encryption. In TCC 2007. LNCS, vol. 4392, pp. 515-534.

[3] Lewko, A., Waters, B.: Decentralizing attribute-based encryption. In: EUROCRYPT 2011. LNCS, vol. 6632, pp. 568-588.

MA-ABE: To reduce the trust on the central authority, Chase proposed a multi-authority ABE (MA-ABE) scheme [2].

- A central authority is required;
- Authorities cooperatively initial the system.

DCP-ABE: Lewko and Waters proposed a new MA-ABE scheme called decentralized CP-ABE (DCP-ABE)[3].

- A central authority is not required;
- Authorities can work independently.

---

[2] Chase, M.: Multi-authority attribute based encryption. In TCC 2007. LNCS, vol. 4392, pp. 515-534.

[3] Lewko, A., Waters, B.: Decentralizing attribute-based encryption. In: EUROCRYPT 2011. LNCS, vol. 6632, pp. 568-588.

Privacy in Multi-Authority ABE

Privacy issues are the primary concerns of users in MA-ABE schemes.
Some privacy-preserving ABE scheme have been proposed, but there are still some disadvantages.

Privacy in Multi-Authority ABE

Privacy issues are the primary concerns of users in MA-ABE schemes.
Some privacy-preserving ABE scheme have been proposed, but there are still some disadvantages.

- Cooperate to initial the system;
- Privacy of attributes is not addressed.

However, a user can be identified by some sensitive attributes.

Privacy in Multi-Authority ABE

Privacy issues are the primary concerns of users in MA-ABE schemes.
Some privacy-preserving ABE scheme have been proposed, but there are still some disadvantages.

- Cooperate to initial the system;
- Privacy of attributes is not addressed.

However, a user can be identified by some sensitive attributes.
Suppose the Head of the school of Computer Science is Bob.

Privacy in Multi-Authority ABE

Privacy issues are the primary concerns of users in MA-ABE schemes.
Some privacy-preserving ABE scheme have been proposed, but there are still some disadvantages.

- Cooperate to initial the system;
- Privacy of attributes is not addressed.

However, a user can be identified by some sensitive attributes.
Suppose the Head of the school of Computer Science is Bob.
Given
$S_1 = \{Position = Header, Department = CS, Sex = Male\}$ and
$S_2 = \{Position = Student, Department = CS, Sex = Male\}$,
we can guess S_1 is the attributes of Bob even if we do not know his global identifier (GID).

Our Contributions

In this paper, we propose a privacy-preserving decentralized CP-ABE (PPDCPABE) scheme with the following features:

- Any authority can dynamically join or leave the system without re-initialing the system;
- There is no any requirement for the central authority or interactions among multiple authorities.
- A user can obtain secret keys for his attributes from multiple authorities without revealing any information about his GID and attributes to the authorities.
- This is the first PPDCP-ABE scheme where both the identifiers and attributes are considered

II. Related Work

Attribute-Based Encryption

Sahai and Waters introduced the conception of attribute-based encryption (ABE).

Currently, ABE schemes can be classified into two types: key-policy ABE (KP-ABE) and cipher-policy ABE (CP-ABE).

- KP-ABE. In these schemes, an access structure is embedded in the secret keys, while the ciphertext is associated with a set of attributes .
- CP-ABE. In these schemes, the secret keys are associated with a set of attributes, while an access structure is embedded in the ciphertext.

Multi-Authority ABE

Chase first proposed an MA-ABE scheme. The technical hurdle in designing an MA-ABE scheme is to resist the collusion attacks. To overcome this hurdle, GID was introduced to tie all the users secret keys together.

Lin et al [4]. proposed an MA-ABE scheme based on the distributed key generation (DKG) protocol [5] and the joint zero secret sharing (JZSS) protocol [6], where the cental authority is not required.

Müller et al. [7] proposed a distributed CP-ABE scheme which was proven to be secure in the generic group.

[4] Lin, H., Cao, Z., Liang, X., Shao, J.: Secure threshold multi authority attribute based encryption without a central authority. In: INDOCRYPT'08. LNCS, vol. 5365, pp. 426-436.

[5] Gennaro, R., Jarecki, S., Krawczyk, H., Rabin, T.: Secure distributed key generation for discrete-log based cryptosystems. In: EUROCRYPT'99. LNCS, vol. 1592, pp. 295-310.

[6] Gennaro, R., Jarecki, S., Krawczyk, H., Rabin, T.: Robust threshold dss signatures. In: EUROCRYPT'96. LNCS, vol. 1070, pp. 354-371.

[7] Müller, S., Katzenbeisser, S., Eckert, C.: Distributed attribute-based encryption. In: ICISC'08. LNCS, vol. 5461, pp. 20-36.

Multi-Authority ABE

Liu et al. [8] proposed a fully secure multi-authority CP-ABE scheme in the standard model. In this scheme, there are multiple central authorities and attribute authorities. The central authorities issue identity-related keys to users, while the attribute authorities issue attribute-related keys to users.

Lekwo and Waters [9] proposed a new MA-ABE scheme named decentralizing CP-ABE (DCP-ABE) scheme. In this scheme, no cooperation between the multiple authorities is required in the setup stage and the key generation stage, and there is no central authority. The scheme was constructed in the composite order ($N = p_1 p_2 p_3$) bilinear group, and achieves full (adaptive) security in the random oracle model.

---

[8] Liu, Z., Cao, Z., Huang, Q., Wong, D.S., Yuen, T.H.: Fully secure multi-authority ciphertext-policy attribute-based encryption without random oracles. In: ESORICS'11. LNCS, vol. 6879, pp. 278-297.

[9] Lewko, A., Waters, B.: Decentralizing attribute-based encryption. In: EUROCRYPT'11. LNCS, vol. 6632, pp. 568-588.

Privacy-Preserving Multi-Authority ABE

Considering the privacy issues in MA-ABE schemes, Chase and Chow [10] proposed a new MA-ABE scheme where an anonymous key issuing protocol for the GID was developed by using the 2-party secure computing technique. As a result, a group of authorities cannot cooperate to pool the users attributes by tracing his.

Li et al. [11] proposed a multi-authority CP-ABE (MACP-ABE) scheme with accountability. In this scheme, a user can be identified when he shared his secret keys with others. Notably, the multiple authorities must initialize the system interactively.

---

[10] Chase, M., Chow, S.S.: Improving privacy and security in multi-authority attributebased encryption. In: CCS 2009. pp. 121-130.

[11] Li, J., Huang, Q., Chen, X., Chow, S.S.M., Wong, D.S., Xie, D.: Multi-authority ciphertext-policy attribute-based encryption with accountability. In: ASIACCS 2011. pp. 386-390.

Multi-Authority ABE

Han et al. [12] proposed a privacy-preserving decentralized KP-ABE (PPDKP-ABE) scheme. In this scheme, multiple authorities can work independently without any cooperation. Especially, the central authority is not required and a user can obtain secret keys from multiple authorities without releasing anything about his GID to them.

Qian et al. [13] proposed a privacy-preserving decentralized CP-ABE (PPDCP-ABE) scheme which can support simple access structures.

Notably, the authorities in these schemes can know the users attributes.

---

[12] Han, J., Susilo, W., Mu, Y., Yan, J.: Privacy-preserving decentralized key-policy attribute-based encryption. IEEE Transactions on Parallel and Distributed Systems 23(11), 21502162 (2012).

[13] Qian, H., Li, J., Zhang, Y.: Privacy-preserving decentralized ciphertext-policy attribute-based encryption with fully hidden access structure. In: ICICS'13. LNCS, vol. 8233, pp. 363-372.

Anonymous Credential

In an anonymous credential system [14], an issuer can issue a credential to a user, which includes the users pseudonym and attributes. By using it, the user can prove in zero knowledge to a third party that he obtains a credential containing the given pseudonym and attributes without releasing any other information.

Therefore, in our construction, we assume that each user has obtained an anonymous credential including his GID and attributes. Then, he can prove in zero knowledge to the multiple authorities that he has a GID and holds the corresponding attributes using the anonymous credential technique.

[14] Camenisch, J., Lysyanskaya, A.: An efficient system for non-transferable anonymous credentials with optional anonymity revocation. In: EUROCRYPT'01. LNCS, vol. 2045, pp. 93-118.

III. Preliminaries

Complexity Assumptions

Let $\mathbb{G}$ and $\mathbb{G}_\tau$ be two cyclic groups with prime order p, and g be a generator of $\mathbb{G}$. A map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_\tau$ is a bilinear group if the following properties can be satisfied:

1. Bilinearity. For all $a, b \in \mathbb{Z}_p$ and $u, v \in \mathbb{G}$, $e(u^a, v^b) = e(u^b, v^a) = e(u, v)^{ab}$.
2. Nondegeneracy. $e(g, g) \neq 1_\tau$ where 1_τ is the identity of the group $\mathbb{G}_\tau$.
3. Computability. For all $u, v \in \mathbb{G}$, there exists an efficient algorithm to compute $e(u, v)$.

Let $\mathcal{GG}(1^\kappa)$ be a bilinear group generator, which takes as input a security parameter 1^κ and outputs a bilinear group $(e, p, \mathbb{G}, \mathbb{G}_\tau)$ with prime order p and a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_\tau$.

Complexity Assumptions

Definition

(q-Strong Diffie-Hellman (q-SDH) Assumption) Let $x \xleftarrow{\$} \mathbb{Z}_p$, $\mathcal{GG}(1^\kappa) \rightarrow (e, p, \mathbb{G}, \mathbb{G}_\tau)$ and g be a generator of $\mathbb{G}$. Given a $(q+1)$-tuple $\overrightarrow{y} = (g, g^x, g^{x^2}, \cdots, g^{x^q})$, we say that the q-SDH assumption holds on $(e, p, \mathbb{G}, \mathbb{G}_\tau)$ if no probabilistic polynomial-time adversary $\mathcal{A}$ can output $(c, g^{\frac{1}{x+c}})$ with the advantage

$$Adv_{\mathcal{A}} = \Pr[\mathcal{A}(\overrightarrow{y}) \rightarrow (c, g^{\frac{1}{x+c}})] \geq \epsilon(k)$$

where $c \in \mathbb{Z}_p$ and the probability is token over the random choices $x \xleftarrow{\$} \mathbb{Z}_p$ and the random bits consumed by $\mathcal{A}$.

Complexity Assumption

Definition

(Decisional q-Parallel Bilinear Diffie-Hellman Exponent (q-PBDHE) Assumption) Let $a, s, b_1, \cdots, b_q \xleftarrow{\$} \mathbb{Z}_p$, $\mathcal{GG}(1^\kappa) \rightarrow (e, p, \mathbb{G}, \mathbb{G}_\tau)$ and g be a generator of $\mathbb{G}$. Given a tuple $\overrightarrow{y} =$

$$g, g^s, g^a, \cdots, g^{(a^q)}, g^{(a^{q+2})}, \cdots, g^{(a^{2q})}$$

$$\forall_{1 \le j \le q} \quad g^{s \cdot b_j}, g^{\frac{a}{b_j}}, \cdots, g^{(\frac{a^q}{b_j})}, g^{(\frac{a^{q+2}}{b_j})}, \cdots, g^{(\frac{a^{2q}}{b_j})}$$

$$\forall_{1 \le j,k \le q, k \ne j} \quad g^{\frac{a \cdot s \cdot b_k}{b_j}}, \cdots, g^{(\frac{a^q \cdot s \cdot b_k}{b_j})},$$

we say that the decisional q-PBDHE assumption holds if

$$Adv_{\mathcal{A}} = \left| \Pr[\mathcal{A}(\overrightarrow{y}, e(g,g)^{a^{q+1}s}) = 1] - \Pr[\mathcal{A}(\overrightarrow{y}, R) = 1] \right| \ge \epsilon(k).$$

Building Blocks

Definition

(Access Structure) Let $\mathcal{P} = (P_1, P_2, \cdots, P_n)$ be n parties. A collection $\mathbb{A} \subseteq 2^{\{P_1, P_2, \cdots, P_n\}}$ is monotonic if $B \in \mathbb{A}$ and $B \subseteq C$, then $C \in \mathbb{A}$. An access structure (respectively monotonic access structure) is a collection (respectively monotonic collection) $\mathbb{A}$ of the non-empty subset of $(P_1, P_2, \cdots, P_n)$, i.e., $\mathbb{A} \subseteq 2^{\{P_1, P_2, \cdots, P_n\}} \setminus \{\phi\}$.

Definition

(Linear Secret Sharing Schemes) A secret sharing scheme $\prod$ over a set of parties $\mathcal{P}$ is called linear (over $\mathbb{Z}_p$) if :
(1) The shares for each party form a vector over $\mathbb{Z}_p$.
(2) For $\prod$, there is a matrix M with ℓ rows and n columns called the share-generating matrix. For $x = 1, 2, \cdots, \ell$, the *ith* row is labeled by a party $\rho(i)$ where $\rho : \{1, 2, \cdots, \ell\} \rightarrow \mathbb{Z}_p$. When we consider the vector $\overrightarrow{v} = (s, v_2, \cdots, v_n)$, where $s \in \mathbb{Z}_p$ is the secret to be shared and $v_2, \cdots, v_n \in \mathbb{Z}_p$ are randomly selected, then $M\overrightarrow{v}$ is the vector of the ℓ shares according to $\prod$. The share $M_i\overrightarrow{v}$ belongs to the party $\rho(i)$, where M_i is the ith row of M.

Commitment Schemes. A commitment scheme consists of the following algorithms.

- Setup$(1^\kappa) \rightarrow$ *params*. This algorithm takes as input a security parameter 1^κ, and outputs the public parameters *params*.
- Commit(*params*, *m*) $\rightarrow$ (*com*, *decom*). This algorithm takes as input the public parameters *params* and a message *m*, and outputs a commitment *com* and a decommitment *decom*. *decom* can be used to decommit *com* to *m*.
- Decommit(*params*, *m*, *com*, *decom*) $\rightarrow \{0, 1\}$. This algorithm takes as input the public parameters *params*, the message *m*, the commitment *com* and the decommitment *decom*, and outputs 1 if *decom* can decommit *com* to *m*; otherwise, it outputs 0.

Building Blocks

Proof of Knowledge. [15] By

$$\text{PoK}\left\{(\alpha,\beta,\gamma) : y = g^{\alpha}h^{\beta} \wedge \tilde{y} = \tilde{g}^{\alpha}\tilde{h}^{\gamma}\right\},$$

we denote a zero knowledge proof of knowledge of integers α, β and γ such that $y = g^{\alpha}h^{\beta}$ and $\tilde{y} = \tilde{g}^{\alpha}\tilde{h}^{\gamma}$ hold on the group $\mathbb{G} = \langle g \rangle = \langle h \rangle$ and $\tilde{\mathbb{G}} = \langle g \rangle = \langle h \rangle$, respectively.

Set-Membership Proof. Camenisch *et al.* [16] proposed a set membership proof scheme.

Theorem

This protocol is a zero-knowledge argument of set-membership proof for a set Φ if the $|\Phi|$-SDH assumption holds on the bilinear group $(e, p, \mathbb{G}, \mathbb{G}_{\tau})$.

[15] Camenisch, J., Stadler, M.: Efficient group signature schemes for large groups. In: CRYPTO'97. LNCS, vol. 1294, pp. 410-424.

[16] Camenisch, J., Chaabouni, R., Shelat, A.: Efficient protocols for set membership and range proofs. In: ASIACRYPT'08. LNCS, vol. 5350, pp. 234-252.

Formal Definition

A DCP-ABE scheme consists of the following five algorithms.

- **Global Setup**$(1^\kappa) \rightarrow params$;
- **Authority Setup**$(1^\kappa) \rightarrow (SK_i, PK_i)$;
- **Encrypt**$(params, \mathcal{M}, (M_i, \rho_i, PK_i)_{i\in\mathcal{I}}) \rightarrow CT$;
- **KeyGen**$(params, SK_i, GID_U, \tilde{U} \bigcap \tilde{A}_i) \rightarrow SK_U^i$;
- **Decrypt**$(params, GID, (SK_U^i)_{i\in\mathcal{I}}, CT) \rightarrow \mathcal{M}$.

Definition

A DCP-ABE is correct if

$$\Pr\left[\begin{array}{l|l} \textbf{Decrypt}(params, GID, (SK_U^i)_{i\in\mathcal{I}}, CT) \rightarrow \mathcal{M} & \begin{array}{l}\textbf{Global Setup}(1^\kappa) \rightarrow params; \\ \textbf{Authority Setup}(1^\kappa) \rightarrow (SK_i, Pk_i); \\ \textbf{Encrypt}(params, \mathcal{M}, (M_i, \rho_i, PK_i)_{i\in\mathcal{I}}) \\ \rightarrow CT; \\ \textbf{KeyGen}(params, SK_i, GID_U, \tilde{U} \bigcap \tilde{A}_i) \\ \rightarrow SK_U^i \end{array} \end{array}\right] = 1$$

Security Model of DCP-ABE

Initialization. The adversary $\mathcal{A}$ submits a list of corrupted authorities $\mathfrak{A} = \{\breve{A}_i\}_{i\in\mathcal{I}}$ and a set of access structures $\mathbb{A} = \{M_i^*, \rho_i^*\}_{i\in\mathcal{I}^*}$, where $\mathcal{I} \subseteq \{1, 2, \cdots, N\}$ and $\mathcal{I}^* \subseteq \{1, 2, \cdots, N\}$. There should be at lease an access structure $(M^*, \rho^*) \in \mathbb{A}$ which cannot be satisfied by the attributes monitored by the authorities in $\mathfrak{A}$ and the attributes selected by $\mathcal{A}$ to query secrete keys.

Global Setup. The challenger $\mathcal{C}$ runs the **Global Setup** algorithm to generate the public parameters *params*, and sends them to $\mathcal{A}$.

Authority Setup. There are two cases.

1. For the authority $\breve{A}_i \subseteq \mathfrak{A}$, the challenger runs the Authority Setup algorithm to generate the secret-public key pair (SK_i, PK_i), and sends them to $\mathcal{A}$.
2. For the authority $\breve{A}_i \nsubseteq \mathfrak{A}$, the challenger runs the Authority Setup algorithm to generate the secret-public key pair (SK_i, PK_i), and sends the public key PK_i to $\mathcal{A}$.

Security Model of DCP-ABE

Phase 1. $\mathcal{A}$ can query secret key for a user U with an identifier GID_U and a set of attributes $\tilde{U}$. The challenger runs the **KeyGen** algorithm to generate a secret key SK_U, and sends it to $\mathcal{A}$. This query can be made adaptively and repeatedly.

Challenge. $\mathcal{A}$ submits two messages $\mathcal{M}_0$ and $\mathcal{M}_1$ with the same length. The challenger flips an unbiased coin with $\{0, 1\}$, and obtains a bit $b \in \{0, 1\}$. Then, $\mathcal{C}$ runs **Encrypt**$(parmas, \mathcal{M}_b, (M_i^*, \rho^*, PK_i)_{i \in \mathcal{I}^*})$ to generate CT^*, and sends CT^* to $\mathcal{A}$.

Phase 2. Phase 1 is repeated.

Guess. $\mathcal{A}$ outputs his guess b' on b. $\mathcal{A}$ wins the game if $b' = b$.

Definition

A DCP-ABE scheme is $(T, q, \epsilon(\kappa))$ secure in the selective-access structure model if no PPT adversary $\mathcal{A}$ making q secret key queries can win the above game with the advantage

$$Adv_{\mathcal{A}}^{DCP-ABE} = \left| \Pr[b' = b] - \frac{1}{2} \right| > \epsilon(\kappa).$$

Privacy-Preserving DCP-ABE

The main difference is that we replace the **KeyGen** algorithm in a DCP-ABE scheme with a privacy-preserving key generation algorithm **PPKeyGen**.

PPKeyGen$(U(params, GID_U, \tilde{U}, PK_i, decom_i, (decom_{i,j})_{a_{i,j} \in \tilde{U} \bigcap \tilde{A}_i}) \leftrightarrow \check{A}_i(params, SK_i, PK_i, com_i, (com_{i,j})_{a_{i,j} \in \bigcap \tilde{A}_i})) \rightarrow (SK_U^i, \text{empty})$.

This is an interactive algorithm executed between a user U and an authority $\check{A}_i$.

PPKeyGen should satisfy the following two properties [17][18]:

- leak-freeness
- selective-failure blindness

[17] Camenisch, J., Kohlweiss, M., Rial, A., Sheedy, C.: Blind and anonymous identitybased encryption and authorised private searches on public key encrypted data. In: PKC'09. LNCS, vol. 5443, pp. 196-214.

[18] Green, M., Hohenberger, S.: Blind identity-based encryption and simulatable oblivious transfer. In: ASIACRYPT'07. LNCS, vol. 4833, pp. 265-282.

Security Model of **PPKeyGen**

Leak-freeness requires that by executing the algorithm **PPKeyGen** with honest authorities, the malicious user cannot know anything which it cannot know by executing the algorithm **KeyGen** with the authorities.

Selective-failure blindness requires that malicious authorities cannot know anything about the user's identifier and his attributes, and cause the **PPKeyGen** algorithm to selectively fail depending on the user's identifier and his attributes.

Definition

A PPDCP-ABE scheme $\tilde{\prod} = (\textbf{Global Setup}, \textbf{Authority Setup}, \textbf{Encrypt}, \textbf{PPKeyGen}, \textbf{Decrypt})$ is secure if:

1. $\prod = (\textbf{Global Setup}, \textbf{Authority Setup}, \textbf{Encrypt}, \textbf{KeyGen}, \textbf{Decrypt})$ is a secure DCP-ABE in the selective-access structures model;
2. **PPKeyGen** is both leak-free and selective-failure blind.

IV. Our Construction

Our Construction

Global Setup. Let g, h and $\mathfrak{g}$ be generators of the group $\mathbb{G}$. Suppose that there are N authorities $\{\breve{A}_1, \breve{A}_2, \cdots, \breve{A}_N\}$, and $\breve{A}_i$ monitors a set of attributes $\tilde{A}_i = \{a_{i,1}, a_{i,2}, \cdots, a_{i,q_i}\}$ where $a_{i,j} \in \mathbb{Z}_p$ for $i = 1, 2, \cdots, N$ and $j = 1, 2, \cdots, q_i$. The public parameters are $PP = (g, h, \mathfrak{g}, e, p, \mathbb{G}, \mathbb{G}_\tau)$.

Authorities Setup. Each authority $\breve{A}_i$ selects $\alpha_i, x_i, \beta_i, \gamma_i \xleftarrow{\$} \mathbb{Z}_p$, and computes $H_i = e(g,g)^{\alpha_i}$, $A_i = g^{x_i}$, $B_i = \mathfrak{g}^{\beta_i}$, $\Gamma_i^1 = g^{\gamma_i}$ and $\Gamma_i^2 = h^{\gamma_i}$, where $i = 1, 2, \cdots, N$. For each attribute $a_{i,j} \in \tilde{A}_i$, $\breve{A}$ chooses $z_{i,j} \xleftarrow{\$} \mathbb{Z}_p$, and computes $Z_{i,j} = g^{z_{i,j}}$ and $T_{i,j} = h^{z_{i,j}} g^{\frac{1}{\gamma_i + a_{i,j}}}$. Then, $\breve{A}$ publishes the public key $PK_i = \left\{H_i, A_i, B_i, (\Gamma_i^1, \Gamma_i^2), (T_{i,j}, Z_{i,j})_{a_{i,j} \in \tilde{A}_i}\right\}$, and keeps the master secrete key as $SK_i = (\alpha_i, a_i, \beta_i, \gamma_i, (z_{i,j})_{a_{i,j} \in \tilde{A}_i})$.

Our Construction

Encryption. Let $\mathcal{I}$ be a set which consists of the indexes of the authorities whose attributes are selected to encrypt $\mathcal{M}$. For each $j \in \mathcal{I}$, this algorithm first selects an access structures (M_j, ρ_j) and a vector $\overrightarrow{v_j} = (s_j, v_{j,2}, \cdots, v_{j,n_j})$, where $s_j, v_{j,2}, \cdots, v_{j,n_j} \xleftarrow{\$} \mathbb{Z}_p$ and M_j is an $\ell_j \times n_j$ 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 $r_{j,1}, r_{j,2}, \cdots, r_{j,\ell_j} \xleftarrow{\$} \mathbb{Z}_p$, and computes

$$C_0 = \mathcal{M} \cdot \prod_{j \in \mathcal{I}} e(g,g)^{\alpha_j s_j}, \ \{X_j = g^{s_j}, \ Y_j = \mathfrak{g}^{s_j}, \ E_j = B_j^{s_j}\}_{j \in \mathcal{I}}$$

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

The ciphertext is

$$CT = \left\{ C_0, \ \left(X_j, \ Y_j, \ E_j, \ (C_{j,1}, \ D_{j,1}), \ \cdots, \ (C_{j,\ell_j}, \ D_{j,\ell_j}) \right)_{j \in \mathcal{I}} \right\}.$$

Our Construction

KeyGen. To generate secret keys for a user U with GID μ and a set of attributes $\tilde{U} \bigcap \tilde{A}_i$, $\check{A}_i$ selects $t_{U,i}, w_{U,i} \xleftarrow{\$} \mathbb{Z}_p$, and computes

$K_i = g^{\alpha_i} g^{x_i w_{U,i}} \mathfrak{g}^{t_{U,i}} \mathfrak{g}^{\frac{\beta_i+\mu}{t_{U,i}}}$, $P_i = g^{w_{U,i}}$, $L_i = g^{t_{U,i}}$,
$L'_i = h^{t_{U,i}}$, $R_i = g^{\frac{1}{t_{U,i}}}$, $R'_i = h^{\frac{1}{t_{U,i}}}$ and $(F_x = Z_x^{w_{U,i}})_{a_x \in \tilde{U} \bigcap \tilde{A}_i}$.
The secret keys for U are $SK_U^i = \left\{K_i, P_i, L_i, L'_i, R_i, R'_i, (F_x)_{a_x \in \tilde{U} \bigcap \tilde{A}_i}\right\}$.

Decryption. To decrypt a ciphertext CT, this algorithm computes

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

$$= \mathcal{M}$$

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

Privacy-Preserving Key Extract Protocol

Overview. In the proposed DCP-ABE scheme, to generate a secret key for a user U, the authority $\breve{A}_i$ selects two random numbers $(t_{U,i}, w_{U,i})$, and uses them to tie the user's secret keys to his GID. If $\breve{A}_i$ records $(t_{U,i}, w_{U,i})$, he can compute

$$\boxed{\mathfrak{g}^{\mu} = \left(\frac{K_i}{g^{\alpha_i} g^{x_i w_{U,i}} \mathfrak{g}^{t_{U,i}}}\right)^{t_{U,i}} \mathfrak{g}^{-\beta_i}} \tag{1}$$

and

$$\boxed{\left(Z_x = F_x^{\frac{1}{w_{U,i}}}\right)_{a_x \in \tilde{U} \bigcap \tilde{A}_i}.} \tag{2}$$

Hence, he can know the user's GID and attributes. Therefore, in order to protect the privacy of the user's GID and attributes, $(t_{U,i}, w_{U,i})$ should be computed using the 2-party secure computing technique.

Privacy-Preserving Key Extract Protocol

$U(PP, PK_i, \mu, a_x \in \tilde{U} \bigcap \tilde{A}_i)$

$w_{U,i} = e_u d_1$, $t_{U,i} = \frac{c_u}{d_2}$

$\breve{A}_i(PP, PK_i, SK_i)$

1. Selects $k_1, k_2, d_1, d_2 \xleftarrow{\$} \mathbb{Z}_p$ and sets $d_u = d_1 d_2$. Computes

$\Theta_1 = A_i^{d_1}$, $\Theta_2 = g^{d_u}$, $\Theta_3 = h^{k_1} \mathfrak{g}^{\mu}$,

$\Theta_4 = \Theta_3^{k_2}$, $\Theta_5 = B_i^{k_2}$, $\Theta_6 = \mathfrak{g}^{\frac{1}{k_2}}$,

$(\Psi_x^1 = T_x^{d_u}, \Psi_x^2 = Z_x^{d_u})_{a_x \in \tilde{U} \bigcap \tilde{A}_i}$

and $\Sigma_U = \mathrm{PoK}\{(k_1, k_2, d_1, d_u, \mu,$

$(a_x \in \tilde{U} \bigcap \tilde{A}_i)) : \Theta_1 = A_i^{d_1} \wedge$

$\Theta_2 = g^{d_u} \wedge \Theta_3 = h^{k_1} \mathfrak{g}^{\mu}, \wedge$

$\Theta_4 = \Theta_3^{k_2} \wedge \Theta_5 = B_i^{k_2} \wedge$

$e(\Theta_5, \Theta_6) = e(B_i, \mathfrak{g}) \wedge$

$(\wedge \frac{e(\Gamma_i^1, \Psi_x^1)}{e(\Gamma_i^2, \Psi_x^2)} = e(g, \Psi_x^1)^{-a_x} \cdot$

$\wedge e(h, \Psi_x^2)^{a_x} \cdot e(g, g)^{d_u})_{a_x \in \tilde{U} \bigcap \tilde{A}_i}\}$

$\xrightarrow[\Theta_5, \Psi_x^1, \Psi_x^2, \Sigma_U]{\Theta_1, \Theta_2, \Theta_3, \Theta_4}$

2. Selects $c_u, e_u \xleftarrow{\$} \mathbb{Z}_p$ and computes

$\Upsilon_1 = g^{c_u}$, $\Upsilon_2 = g^{\frac{1}{c_u}}$,

$\Upsilon_3 = h^{c_u}$, $\Upsilon_4 = h^{\frac{1}{c_u}}$, $\Upsilon_5 = g^{e_u}$,

$K_i' = g^{\alpha_i} \Theta_1^{e_u} \Theta_6^{c_u} (\Theta_4 \Theta_5)^{\frac{1}{c_u}}$,

$(\Phi_x = (\Psi_x^2)^{e_u})_{a_x \in \tilde{U} \bigcap \tilde{A}_i}$ and

$\Sigma_{A_i} = \mathrm{PoK}\{(\alpha_i, c_u, e_u) :$

$e(\Upsilon_1, \Upsilon_2) = e(g, g) \wedge \Upsilon_1 = g^{c_u} \wedge$

$\Upsilon_2 = g^{\frac{1}{c_u}} \wedge \Upsilon_3 = h^{c_u} \wedge \Upsilon_4 = h^{\frac{1}{c_u}}$

$e(\Upsilon_3, \Upsilon_4) = e(h, h) \wedge \Upsilon_5 = g^{e_u} \wedge$

$K_i' = g^{\alpha_i} \Theta_1^{e_u} \Theta_6^{c_u} (\Theta_4 \Theta_5)^{\frac{1}{c_u}}$

$\wedge (\wedge (\Phi_x = (\Psi_x^2)^{e_u})_{a_x \in \tilde{U} \bigcap \tilde{A}_i}\}.$

$\xleftarrow[\Upsilon_5, K_i', \Phi_x, \Sigma_{A_i}]{\Upsilon_1, \Upsilon_2, \Upsilon_3, \Upsilon_4}$

3. Computes $K_i = \frac{K_i'}{\Upsilon_4^{k_1 k_2}}$, $P_i = \Upsilon_5^{d_1}$,

$L_i = \Upsilon_1^{\frac{1}{k_2}}$, $R_i = \Upsilon_2^{k_2}$, $R_i' = \Upsilon_4^{k_2}$ and

$\left(F_x = \Phi_x^{\frac{1}{d_2}}\right)_{a_x \in \tilde{U} \bigcap \tilde{A}_i}$

Security Analysis

Theorem

Our DCP-ABE is $(T, q, \epsilon(k))$ *secure in the selective-access structure model if the* $(T', \epsilon'(k))$*-decisional q-PBDHE assumption holds on* $(e, p.\mathbb{G}, \mathbb{G}_\tau)$*, where* $T' = T + \mathcal{O}(T)$ *and* $\epsilon'(\kappa) = \frac{1}{2}\epsilon(\kappa)$.

Theorem

The **PPKeyGen** *algorithm is both leak-free and selective-failure blind under the q-SDH assumption, where* $q = max\{q_1, q_2, \cdots, q_N\}$.

Theorem

Our PPDCP-ABE scheme $\tilde{\prod} = ($**Global Setup**, **Authority Setup**, **Encrypt**, **PPKeyGen**, **Decrypt**$)$ *is secure in the selective-access structure model under the decisional q-PBDHE assumption and q-SDH assumption.*

V. Conclusion

Conclusion

Decentralized ABE scheme is more efficient and flexible encryption system as it dose not require a central authority nor the cooperation among multiple authorities. In this paper, the following work was finished:

- We proposed a DCP-ABE scheme where multiple authorities can work independently;
- We proposed a privacy-preserving key generation algorithm for the proposed DCP-ABE scheme;
- We proved the security of the proposed DCP-ABE and privacy-preserving key generation algorithm.

Questions

Thank You For Your Attentions!