ATLANTIS PRESS

Advances in Engineering Research, volume 170

7th International Conference on Energy and Environmental Protection (ICEEP 2018)

Fuzzy Identity-Based Threshold Key-Insulated Encryption with Ciphertext Policy

Jianhong Chen [1, a]

[1] Faculty of Computer and Software Engineering, Huaiyin Institute of Technology, Huaian 223003, China

[a] 1395996433@qq.com

Keywords: Threshold key-insulated; fuzzy identity based; encryption; ciphertext policy.

Abstract. To solve the signing key exposure problem in fuzzy identity-based encryption systems with ciphertext policy, we propose a fuzzy identity-based threshold key-insulated encryption scheme with ciphertext policy (FIBTKIE-CP) which is provably secure. Our scheme is key-insulated and strongly key-insulated. Even if temporary private keys for up to N-1 time periods are compromised, an adversary is still unable to obtain this user's temporary private key from the remaining time period. Even if up to $k-1$ helpers are exposed and all temporary private keys are compromised, the adversary still can not harm the security of the non-exposed periods..

Introduction

Security is harmed by inadvertent loss of private keys. In 2002, Dodis et al. [3] introduced a key insulation mechanism, which can protect secret keys in public key cryptosystems. Weng et al. [5] proposed the threshold key-insulation in which for at least k out of n helpers are used to refresh the user's temporary private keys. Ciphertext policy FIBE (FIBIE-CP) [2] is a variant of FIBE [4]. In a FIBIE-CP system, attributes are associated with user secret keys and access structures with ciphertexts. To deal with the key exposure problem in FIBE systems, Chen et al. gave a fuzzy identity-based parallel key-insulated encryption (FIBPKIE-CP) [1] scheme. But Chen et al. used two different helpers to refresh the private keys. There are some scenarios in which at least k out of n helpers are needed to update the user's temporary private keys. To strengthens the security and flexibility of Chen et al.'s scheme, we give a fuzzy identity-based threshold key-Insulated encryption scheme with ciphertext policy (FIBTKIE-CP) in which decryption is enabled if and only if the user's identity (attribute set) satisfies the access structure.

Model of FIBTKIE-CP

Definition

Throughout this paper, we use bilinear pairings, DBDH assumption and PRF[1]. We let Z_p^* denote the set $\{0,1,2,\ldots,p\text{-}1\}$ and denote Z_p /0. For a finite set S, $x \in_R S$ means choosing an element x from S with a uniform distribution. A FIBTKIE-CP scheme consists of six algorithms:(1)Setup(k): Given a security parameter k, the authority runs this algorithm to output a master secret key msk and a public key pk; (2)KeyGen(w,msk): Given the user's identity w, as a set representing a user's attributes, and the master-key msk, the authority runs this algorithm to output an initial private key $TK_{w,0}$ and n helper keys $\{HK_{w,i'}\}_{1 \le i' \le n}$ corresponding to w. Each helper key $HK_{w,i'}$ is kept by the i'-th helper and the user with identity w keeps the initial private key. (3)HelperUpt(t,w,HK_w,pk): The helper key-update algorithm takes as input a period index t, an identity w and his i'-th ($1 \le i' \le n$) helper key $HK_{w,i'}$. It outputs the i'-th key-update information share $UI_{w,t,i'}$ with respect to identity i' and period t. (4) UserUpt(t,w,$TK_{w,t'}$,$UI_{w,t',t}$,PK): The user key-update algorithm takes as input an identity w, his temporary private key $TK_{w,t'}$ for period t', and a set $\{UI_{w,t,i'}\}_{i' \in S''}$ of key-update information shares, where $S \subseteq \{1, \ldots, n\}$ and $|S'| \ge k$. It returns this user's temporary private key $TK_{w,t}$ for period t, and deletes $TK_{w,t'}$ and $\{UI_{w,t,i'}\}_{i' \in S''}$;(5)Encryption($t$,$M$,$W$,$pk$): The Encryption algorithm takes as input the public key pk, the time period index t, a message M and an access structure W. It returns a ciphertext

(t,E) such that a temporary private key generated from attribute set w for period t can be used decrypt (t,E) if and only if $w|= W$;(6)Decryption($t,E,w,TK_{w,t},pk$): The Decryption algorithm takes as input a ciphertext (t,E) and a temporary private key $TK_{w,t}$. It returns the message M if w satisfies W, where S and t are the identity (attribute set) and the time period index respectively used to generate $TK_{w,t}$.

Security notions for FIBTKIE-CP

A FIBTKIE-CP scheme is said to be secure against chosen plaintext attacks (CPA) in the sense of key-insulation if no probabilistic polynomial-time adversaries have non-negligible advantage in the following game. For convenience, we give the definition of a restricted identity as below: the attribute set of the restricted identity satisfies challenge access structure W^*.

Init. The adversary declares the access structure W^* and the time period index t^* that he wishes to be challenged upon.

Setup. The challenger runs the setup phase of the algorithm and tells the adversary the public parameters.

Phase 1. The adversary adaptively issues a set of queries as below:(1)Key Generation Query $\langle g \rangle$: The challenger first runs algorithm KeyGen to obtain the initial private key $TK_{g,0}$ and n helper keys $\{HK_{g,i'}\}_{1£ \ i'\leq n}$. It then sends these results to the adversary; (2) Helper Key Query $\langle g,i' \rangle$: The challenger responds by running algorithm KeyGen to generate $HK_{g,i'}$ and sends it to the adversary; (3)Temporary Private Key Query $\langle g, t \rangle$: The challenger responds by running algorithms HelperUpt and UserUpt to generate $TK_{g,t}$. It then returns it to the adversary.

Challenge. The adversary submits two equal length messages M_0, M_1. The challenger flips a random coin, b, and encrypts M_b with $W^*$and t^*. The ciphertext is passed to the adversary.

Phase 2. Phase 1 is repeated.

Guess. The adversary outputs a guess $b'$of b.

The advantage of an adversary A in this game is defined as $\Pr[b'= b] - 1/2$. We refer to the above game as an IND-FIBTKIE-CP-KI-CPA game. In the above game, it is mandated that the following conditions are simultaneously satisfied: (1) A is disallowed to issue key generation queries for the restricted identities; (2) A is disallowed to issue temporary private key queries for the restricted identities and the challenged time period t^*; (3) A can only corrupt up to $k-1$ helper keys with respect to the restricted identities.

FIBTKIE-CP scheme is said to be secure against chosen plaintext attacks (CPA) in the sense of strong key-insulation if no probabilistic polynomial-time adversaries have non-negligible advantage in an IND-FIBTKIE-CP-SKI-CPA game. The IND-FIBTKIE-CP-SKI-CPA game is almost the same as the IND-FI&KI-CPA game except Phase 1.

Phase 1. The adversary adaptively issues a set of queries as below:(1) Key Generation Query $\langle g \rangle$: the same as the IND-FIBTKIE-CP-KI-CPA game; (2) Helper Key Query $\langle g,i' \rangle$: T the same as the IND-FIBTKIE-CP-KI-CPA game.

The advantage of an adversary A in this game is defined as $\Pr[b'=b] - 1/2$. In the above game, it is mandated that the following condition is satisfied: A is disallowed to issue key generation queries for the restricted identities.

Model of FIBTKIE-CP

Description of Our Scheme

Our proposed FIBTKIE-CP scheme is based on Cheung-Newport's construction [2]. Let G_1 and G_2 be two groups with prime order q of size k, g be a random generator of G_1, and e be a bilinear map such that $e : G_1 \times G_1 \rightarrow G_2$. Let H be a collision-resistant hash function such that H: $\{0, 1\}^* \rightarrow \{0, 1\}^{n_u}$. We use a PRF family F such that given a k-bit seed (index) s and a k-bit argument (input) x, it outputs a k-bit string $F_s(x)$. An access structure on attributes is a rule W that returns either 0 or 1 given an identity S (a set of attributes). We say that S satisfies W (written $S |= W$) if and only if W answers 1 on S. Let the set of attributes be $N = \{1,\ldots,n\}$ for some natural number n. We regard attributes i and their negations ¬*i* as literals. We consider access structures that consist of a single AND gate whose inputs are literals. Let $W = \wedge_{i\in I}\underline{i}$ where $I \subseteq N$ and every $\underline{i}$ is a literal (i.e., *i* or ¬*i*).

-Setup: The authority picks $y, t_1, \ldots, t_{3n} \in_R Z_p$, $g_2, h_1 \in_R G_1$, sets $Y=e(g, g)^y$ and $T_k = g^{t_k}$ for each $k \in \{1, \ldots, 3n\}$. We define H_w: $Z_p \rightarrow G_1$ to be the function $H_w(x) = g_1^x h_1$. The public key is $pk=(G_1, G_2, e, g, g_1, Y, h_1, T_1, \ldots, T_{3n}, H_w)$. The master secret key is $msk = (y, t_1, \ldots, t_{3n})$. As illustrated in Table 1, the public key elements T_i, T_{n+i} and T_{2n+i} correspond to the three types of occurrences of *i*: positive, negative and *don't care*.

Table 1.Common Parameters

	1	2	3	…	*n*
positive	T_1	T_2	T_3	…	T_n
negative	T_{n+1}	T_{n+1}	T_{n+3}	…	T_{2n}
Don't Care	T_{2n+1}	T_{2n+1}	T_{2n+3}	…	T_{3n}

–KeyGen: To generate the helper key and the initial private key for identity *S*, the authority does as follows. Let *S* denote the input identity (attribute set). Every $i \in S$ is implictly considered a negative attribute. Pick $r_i \in_R Z_p$ for every $i \in N$ and set $r = \sum_{i=1}^{n} r_i$. Randomly choose a helper key $HK_S \in_R \{0,1\}^k$, compute $k_{S,0} = F_{HK_S}$ (0). Note that if the length of the input for *F* is less than *k*, we can add some "0"s as the prefix to meet the length requirement. Let $\hat{D}'_{S,0} = g^{y-r} H_w(0)^{k_{S,0}}$, $\hat{D}''_{S,0} = g^{k_{S,0}}$. For each $i \in N$, let D_i= if $i \in S$; otherwise, let $D_i = g^{\frac{r_i}{t_{n+i}}}$. Let $F_i = g^{\frac{r_i}{t_{2n+i}}}$ for every $i \in N$. Pick $b \in_R Z_p^*$ and set $R=g^b$, compute the initial private key $TK_{S,0} = (R, -,-, \{D_i\}_{i\in N}, \{F_i\}_{i\in N})$.

For each $i \in w$ and each index $i' \in \{1, \ldots, k-1\}$, pick $l_{i,\underline{i}'} \in_R Z_p^*$ and set the *i′*-th helper key to be

$HK_{w,i'} = (\{ HK_{i,i'} \}_{i\in w}) = (\{ g_2^{l_{i,j}} \}_{i\in w})$ (1)

Let $S' = \{0, 1, \ldots, k-1\}$. For each $i \in w$ pick $s_i \in_R Z_p^*$. For each remaining index $i' \in \{k, \ldots, n\}$, set the *i′*-th helper key to be

$(\{ (g_2^{y-r-b})^{D_{i',S'}(0)} (\prod_{j=1}^{k-1} HK_{i,i'})^{D_{i',S'}(j)} \}_{i\in w})$ (2)

–HelperUpt: Given a period index *t*, an identity *w* and his *i′*-th ($1 \le i' \le n$) helper key $HK_{w,i'}$, this algorithm works as follows. Parse $HK_{w,i'}$ as $(\{ HK_{i,i'}^{\langle 1\rangle} \}_{i\in w})$. For each index $i' \in \{1, \ldots, n\}$, pick $u_{i'} \in_R Z_p^*$ and output user *w*'s *i′*-th key-update information share $UI_{w,t,i'}$ for period *t* as

$UI_{w,t,i'} = (\{ HK_{i,i'} H_w(t)^{u_{i'}} \}_{i\in w}, g^{u_{i'}})$

$= (\{ g_2^{l_{i,j}} V(i)^{r_{i,i'}} H_w(t)^{u_{i'}} \}_{i\in w}, g^{u_{i'}})$

–UserUpt: Given an identity *w*, a temporary private key $TK_{w,t'}$ for period *t′*, and a set $\{ UI_{w,t,i'} \}_{i'\in S}$ of key-update information shares for period *t*, where $S'' \subseteq \{1, \ldots, n\}$ and $|S''| \ge k$ (for convenience, we assume $|S''| = k$), this algorithm works as follows. Parse $TK_{w,t'}$ as $(R, \hat{D}'_{S,t'}, \hat{D}''_{S,t'}, \{D_i\}_{i\in N}, \{F_i\}_{i\in N})$;Parse $UI_{w,t,i'}$ as $(UI_{i,t,i'}^{\langle 1\rangle}, UI_{i,t,i'}^{\langle 2\rangle})$; Set user *w*'s temporary private key $TK_{w,t}$ for period *t* to be $(R, (\prod_{i'} UI_{i,t,i'}^{\langle 1\rangle})^{D_{i',S'}(0)}, (\prod_{i'} UI_{w,t,i'}^{\langle 2\rangle})^{D_{i',S'}(0)}, \{D_i\}_{i\in N}, \{F_i\}_{i\in N})$. Note that in time period *t*, if let $u = \sum_{i'\in S''} \Delta_{0,S''}(i') \cdot u_{i'}$,then $TK_{w,t}$ is always set to be

$$(R, \hat{D}'_{S,t}, \hat{D}''_{S,t'}, \{D_i\}_{i\in N}, \{F_i\}_{i\in N}) = (g^b, \{ g^{y-r-b} H_w(t)^u \}_{i\in w}, g^u, \{D_i\}_{i\in N}, \{F_i\}_{i\in N}).$$

–Encryption: Given time period index t, a message $M\in G_1$ and an AND gate $W=\wedge_{i\in I}\underline{i}$, this algorithm does as follows. Pick $s\in_R Z_p$; For each $i\in I$, let $E_i=T_i^s$ if $\underline{i}=i$ and T_{n+i}^s if $\underline{i}=\neg i$; for each $i\in N\setminus I$, let $E_i=T_{2n+i}^s$. The ciphertext is $(t,E)=(t,(W,E'=M\cdot Y^s,E''=g^u,E'''=H_w(t)^u,\{E_i\}_{i\in N}))$

-Decryption: Suppose the input ciphertext is of the form $(t,E)=(t,(W,E',E'',E''',\{E_i\}_{i\in N}))$, where $W=\wedge_{i\in I}\underline{i}$. Also, let w denote the identity used to generate the input secret key $TK_{w,t}=(g^b,\{g^{y-r-b}H_w(t)^u\}_{i\in w},g^u,\{D_i\}_{i\in N},\{F_i\}_{i\in N})$. For each $i\in I$, this algorithm computes the pairing $e(C_i,D_i)$. If $\underline{i}=i$ and $i\in w$, then $e(E_i,D_i)=e(g^{t_i\cdot s},g^{\frac{r_i}{t_i}})=e(g,g)^{r_i\cdot s}$; If $\underline{i}=\neg i$ and $i\in w$, then $e(E_i,D_i)=e(g^{t_{n+i}\cdot s},g^{\frac{r_i}{t_{n+i}}})=e(g,g)^{r_i\cdot s}$; for each $i\in I$, this algorithm computes the pairing $e(E_i,F_i)=e(g^{t_{2n+i}\cdot s},g^{\frac{r_i}{t_{2n+i}}})=e(g,g)^{r_i\cdot s}$. Then, the ciphertext can be decrypted as

$$M=\frac{E'e(E''',\hat{D}''_{S,t})}{e(E'',R\cdot\hat{D}'_{S,t})\prod_{i=1}^{n}e(g,g)^{r_i\cdot s}}=\frac{M\cdot Y^s e(H_w(t)^s,g^u)}{e(g^s,g^b g^{y-r-b}H_w(t)^u)e(g,g)^{r\cdot s}}$$

$$=\frac{M\cdot Y^s e(H_w(t)^s,g^u)}{e(g^s,g^{y-r})e(g^s,H_w(t)^u)e(g,g)^{r\cdot s}}=\frac{M\cdot Y^s}{e(g,g)^{y\cdot s}}=\frac{M\cdot Y^s}{Y^s}$$

Security

The proof of our proposed FIBTKIE-CP scheme is similar with that of Chen et al.'s FIBPKIE-CP[1].

Conclusions

We introduce the notion of fuzzy identity-based key-insulated encryption with ciphertext policy (FIBTKIE-CP) and describe a construction that is provably secure.

References

[1] J. Chen, K. Chen, Y. Long , Z. Wan , K. Yu, C. Sun and L. Chen: Ciphertext Policy Attribute-Based Parallel Key-Insulated Encryption. in: Journal of Software, Vol. 23, No. 10, (2012), p. 2795-2804

[2] L. Cheung and L. Newport: Provably Secure Ciphertext Policy ABE. in: Proceedings of ACM Computer and Communications Security (CCS), (2007), p. 456-465

[3] Y.Dodis, J. Katz, S. Xu and M. Yun: Key-Insulated Public-Key Cryptosystem. in: Proceedings of International Conference on Theory and Applications of Cryptographic Techniques (Eurocrypt), (2002), p. 65-82

[4] A. Sahai and B. Waters: Fuzzy Identity-Based Encryption. in: Proceedings of International Conference on Theory and Applications of Cryptographic Techniques (Eurocrypt), (2005), p. 457-473

[5] J. Weng, X. Li, K. Chen and S. Liu: Identity-Based Threshold Key-Insulated Encryption without Random Oracles. in: Proceedings of International Conference on the Cryptographers' Track at the RSA (CT-RSA), (2008), p. 203-220