ATLANTIS PRESS

Advances in Engineering Research, volume 170

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

Fuzzy Identity-Based Key-Insulated Encryption with AND Gates on Attributes

Jianhong Chen [1, a]

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

[a]1395996433@qq.com

Keywords: key-insulated; fuzzy identity based; encryption; key-exposure.

Abstract. To deal with the signing key exposure problem in fuzzy identity-based encryption systems with AND gates on attributes, we propose a fuzzy identity-based key-insulated encryption scheme with AND gates on attributes (FIBKIE-AGA). Our scheme is provably secure. Our scheme is (N-1,N)- 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 derive this user's temporary private key from the remaining time period. Even if the adversary exposes the secrets stored in the helper, there is still no security compromise.

Introduction

Security is often been violated by inadvertent loss of private keys. In 2002, Dodis et al. [3] introduced a key insulation mechanism, which can protect private keys in public key cryptosystems. In PKC'06, Hanaoka et al. [5] introduced a novel method named parallel key-insulation. In their parallel key-insulated cypto system, two distinct helpers are alternately used to update the private keys. In 2007, Weng et al [7] proposed the mechanism of threshold key-insulation in which for at least k out of n helpers are needed to update the user's temporary private keys. There are two variants of FIBE, i.e. key policy FIBE[4] and ciphertext policy FIBE[2]. In a key policy FIBE system, every ciphertext is associated with a set of attributes, and every user secret key is associated with a threshold access structure on attributes. In a ciphertext policy FIBE 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 key-insulated encryption (FIBKIE) [1] scheme. In Chen et al. 's scheme, decryption is enabled if and only if the ciphertext and secret key attribute sets overlap by at least a fixed threshold value d. But there are some scenarios in which attributes are associated with user secret keys and access structures with ciphertext. To solve the problem of key exposure in fuzzy identity-based encryption system with access structures for ciphertext, we give a fuzzy identity-based key-Insulated encryption scheme with AND gates on attributes (FIBKIE-AGA) in which access structures are AND gates on positive and negative attributes.

Model of FIBKIE-AGA

Definition

Throughout this paper, we use bilinear pairings, DBDH assumption and PRF[1]. We let Z_p^* denote the set {0,1,2,…,p-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 FIBKIE-AGA scheme consists of six algorithms:

-Setup(k): Given a security parameter k, the authority runs this algorithm to output a master secret key msk and a public key pk.

-KeyGen(S,msk): Given the user's identity S, as a set representing a user's attributes, and the master-key msk, the authority runs this algorithm to output an initial private key $TK_{S,0}$ and a helper key HK_S corresponding to S. The helper key is kept by the helper and the user with identity S keeps the initial private key.

-HelperUpt(t,t',S,HK_S,pk): Given period indices t and t', an identity S, its helper key HK_S and the public parameters pk, the helper runs this algorithm to output the key-update information $UI_{S,t',t}$ for S from period t' to period t.

-UserUpt($t,t',S,TK_{S,t'}, UI_{S,t',t},pk$): Given period indices t and t', an identity S, the temporary private key $TK_{S,t'}$ corresponding to S and t', the key-update information $UI_{S,t',t}$ for S from period t' to period t and the public parameters PK, the user with identity S runs this algorithm to output the temporary private key $TK_{S,t}$ corresponding to S and t.

-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 S for period t can be used decrypt (t,E) if and only if $S \models W$.

-Decryption($t,E,S,TK_{S,t},pk$): The Decryption algorithm takes as input a ciphertext (t,E) and a temporary private key $TK_{S,t}$. It returns the message M if S satisfies W, where S and t are the identity (attribute set) and the time period index respectively used to generate $TK_{S,t}$.

Security notions for FIBKIE-AGA

A FIBKIE-AGA 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:

-Key Generation Query $\langle S\rangle$: The challenger first runs algorithm KeyGen to obtain the initial private key $TK_{S,0}$ and the helper key HK_S corresponding to identity S. It then sends these results to the adversary.

-Temporary Private Key Query $\langle S, t\rangle$: The challenger runs algorithm UserUpt to obtain the temporary private key for identity S and period index t. It then sends this result 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-FI&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^*.

FIBKIE-AGA 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-FI&SKI-CPA game. The IND-FI&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:

-Key Generation Query $\langle S\rangle$: the same as the IND-FI&KI-CPA game.

-Helper Key Query $\langle S\rangle$: The challenger runs algorithm KeyGen to generate HK_S and sends it to the adversary.

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.

OUR PROPOSED FIBKIE-AGA SCHEME

Description of Our Scheme

Our proposed FIBKIE-AGA 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 $S \models W$) 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 $\neg i$ 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 $\neg i$).

The proposed FIBKIE-AGA system includes the following algorithms:

-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 $i \in N$. Then, compute the initial private key $TK_{S,0} = (\hat{D}'_{S,0}, \hat{D}''_{S,0}, \{D_i\}_{i \in N}, \{F_i\}_{i \in N})$. The helper key is kept by the helper and the user with identity S keeps the initial private key.

–HelperUpt: This algorithm first computes $k_{S,t} = F_{HK_S}(t)$.and$k_{S,t'} = F_{HK_S}(t')$. Then it defines and returns the key-update information for identity S from period t' to period t as

$$UI_{S,t',t} = (UI^{\langle 1 \rangle}_{S,t',t}, UI^{\langle 2 \rangle}_{S,t',t}) = \left(\frac{H_w(t)^{k_{S,t}}}{H_w(t')^{k_{S,t'}}}, g^{k_{S,t}}\right).$$

–UserUpt: Given a period index t, an update key $UI_{S,t',t}$ and a temporary private key $TK_{S,t'}$, user S works as follows:

This algorithm first parses the temporary private key for identity S and period t' as $TK_{S,t'} = (\hat{D}'_{S,t}, \hat{D}''_{S,t'}, \{D_i\}_{i \in N}, \{F_i\}_{i \in N})$ and parses the key-update information for identity S from period t' to period t as $UI_{S,t',t} = (UI^{\langle 1 \rangle}_{S,t',t}, UI^{\langle 2 \rangle}_{S,t',t})$. Then it sets the temporary private key for identity S and period t as

$$TK_{S,t} = (\hat{D}'_{S,t}, \hat{D}''_{S,t'}, \{D_i\}_{i \in N}, \{F_i\}_{i \in N}) = (\hat{D}'_{S,t} UI^{\langle 1 \rangle}_{S,t',t}, UI^{\langle 2 \rangle}_{S,t',t}, \{D_i\}_{i \in N}, \{F_i\}_{i \in N})$$

Delete $TK_{S,t'}$and $UI_{S,t',t}$, and return $TK_{S,t}$. Note that in time period t, $TK_{S,t}$ is always set to be

$$(g^{y-r}H_w(t')^{k_{S,t'}}\frac{H_w(t)^{k_{S,t}}}{H_w(t')^{k_{S,t'}}},\ g^{k_{S,t}},\{D_i\}_{i\in N},\{F_i\}_{i\in N}) = (g^{y-r}H_w(t)^{k_{S,t}},\ g^{k_{S,t}},\{D_i\}_{i\in N},\{F_i\}_{i\in N})$$

–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 $(t,E)=(t,(W,E'=M\cdot Y^s,E''=g^s,E'''=H_w(t)^s,\{E_i\}_{i\in N}))$

-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 S denote the identity used to generate the input secret key $TK_{S,t}=(g^{y-r}H_w(t)^{k_{S,t}},\ g^{k_{S,t}},\{D_i\}_{i\in N},\{F_i\}_{i\in N})$. For each $i\in I$, this algorithm computes the pairing $e(C_i,D_i)$. If $\underline{i}=i$ and $i\in S$, 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 $i\in S$, 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

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

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

Security

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

Conclusions

We introduce the notion of fuzzy identity-based key-insulated encryption with an access structure on attributes (FIBKIE-AGA) and describe a construction that is based on a fuzzy ciphertext policy identity-based encryption (CPFIBE) scheme.

References

[1] J. Chen, Y. Wang and K. Chen: Attribute-Based Key-Insulated Encryption. in: Journal of Information Science & Engineering, Vol. 27, No. 2, (2011), p. 437-449

[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] V. Goyal, O. Pandey, A. Sahai, and B. Waters: Attribute-Based Key-Insulated Encryption. in: Proceedings of ACM Computer and communications security (CCS), (2006), p. 89-98

[5] G. Hanaoka, Y. Hanaoka and H. Imai: Parallel key-insulated public key encryption. in: Proceedings of International Conference on Practice and Theory in Public Key Cryptography (PKC), (2006), p. 105-122

[6] 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

[7] 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