Attribute-Based Threshold Key-Insulated Encryption

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; attribute based; encryption; key-exposure.

Abstract. Because of the compromise of the security of the underlying system or machine storing the key, exposure of the private key can be an great attack on a cryptosystem. Key insulation is an important method to protect private keys. To deal with the private key exposure problem in attribute-based encryption systems, we propose an attribute-based threshold key-insulated encryption (ABTKIE) scheme. It strengthens the security and flexibility of existing attribute-based key-insulated encryption schemes.

Introduction

To protect private keys, Dodis et al. [2] gave the mechanism of key insulation in 2002. After that, identity-based parallel key-insulated encryption (IBPKIE) scheme [3] were given for some special situations. In 2007, Weng et al. [5] gave the idea of threshold key-insulation in which for at least k out of n helpers are needed to update the user's temporary private keys. The first attribute-based encryption scheme (ABE) [4] was proposed by Sahai and Waters in 2005. Chen et al. gave attribute-based threshold key-insulated encryption (ABKIE) [1] scheme in 2011. Chen et al. 's scheme is (N-1,N)-key-insulated, i.e. even if temporary private keys for up to N-1 time periods are compromised, an adversary is still unable to get this user's temporary private key from the remaining time period. But there are some scenarios in which helper keys could be harmed. To solve the problem of key exposure in attribute-based encryption system, we give an attribute-based threshold key-insulated encryption (ABTKIE) scheme. In a (k, n) threshold ABTKIE system, at least k out of n helpers are needed to update the user's temporary private keys. Even if up to $k-1$ helpers are compromised and all temporary private keys are exposed, the adversary still can not compromise the security of the non-exposed periods. It strengthens the security and flexibility of Chen et al.'s ABKIE scheme.

Model of ABTKIE

Definition

Throughout this paper, we use bilinear pairings, DBDH assumption, PRF[1] and Lagrange coefficient [5]. 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. An ABTKIE scheme consists of six algorithms:

–Setup(d): Given a threshold value d, the authority runs this algorithm to output a master key MK and a set of public parameters PK.

–KeyGen(w,MK): Given the user's identity w, as a set representing a user's attributes, and the master-key MK, the authority runs this algorithm to output an initial private key $TK_{w,0}$ and n helper keys $\{HK_{w,i'}\}_{1£\ i'\leq n}$ 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.

–HelperUpt(t,w, $HK_{w,i'}$,PK): The helper key-update algorithm takes as input a period index t, an identity w and his i'-th ($1 \leq i' \leq n$) helper key $HK_{w,i'}$. It outputs the i'-th key-update information share $UI_{w,t,i'}$ with respect to identity w and period t.

–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 $S' \subseteq \{1, \dots, n\}$ and $|S'| \geq k$. It returns this user's temporary private key $TK_{w,t}$ for period t, and deletes $TK_{w,t'}$ and $\{UI_{w,t,i'}\}_{i'\in S''}$.

–Encryption(t,M,w,PK): The Encryption algorithm is run by a user to encrypt a message M, with a target identity w', period t and the public parameters PK. It outputs a ciphertext, E encrypted under w' and t.

–Decryption($E,w',w,TK_{w,t},PK$): The Decryption algorithm is run by a user with identity w and the temporary private key $TK_{w,t}$ to attempt to decrypt a ciphertext E under identity w' and period t. If the set overlap $|w\cap w'| \geq d$, the algorithm will output the decrypted message M.

Security notions for ABTKIE

We first consider the basic (i.e., non-strongly) key-insulated security for ABTKIE. For one thing, as standard ABE systems, the key generation queries should be considered. For another, as traditional key-insulated encryption schemes, the temporary private key exposure should be addressed. An ABTKIE 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.

Init. The adversary declares the identity g^* 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 $\langle g\rangle$: The challenger first runs algorithm KeyGen to obtain the initial private key $TK_{g,0}$ and n helper key n helper keys $\{HK_{g,i'}\}_{1£\ i'\leq n}$ corresponding to identity g. It then sends these results to the adversary.

–Helper Key Queries $\langle g,i'\rangle$: The challenger runs KeyGen algorithm to obtain $HK_{g,i'}$ and sends it to the adversary.

–Temporary Private Key Query $\langle g, t\rangle$: The challenger runs algorithm UserUpt to obtain the temporary private key for identity g 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 g^* and t^*. The ciphertext is passed to the adversary.

Phase 2. Phase 1 is repeated.

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

For convenience, we give the definition of a restricted identity as below: the set overlap between a restricted identity and the challenge identity g^* is at least d. 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-ABTKIE-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.

The word "strongly" doesn't mean our strongly key-insulated security is more strong security than our key-insulated security. It means that the cryptosystem should ensure that even if all the n helpers corresponding to an identity w are compromised, it is still impossible for the adversary to derive any of user w's temporary private keys. An ABTKIE 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-ABTKIE-SKI-CPA game. The IND-ABTKIE-SKI-CPA game is almost the same as the IND-ABTKIE-KI-CPA game.

Phase 1. The adversary adaptively issues a set of queries as below:

–Key Generation Query $\langle g\rangle$: the same as the IND-ABTKIE-KI-CPA game.

–Helper Key Queries $\langle g,i'\rangle$: The challenger runs KeyGen algorithm to obtain $HK_{w,i'}$ 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 ABTKIE SCHEME

Description of Our Scheme

Our proposed ABTKIE scheme is based on Sahai-Waters' large universe ABE construction [4]. Let G_1 and G_2 be two groups with prime order p of size k, and let g be a generator of G_1. Additionally, let e: $G_1\times G_1 \rightarrow G_2$ denote the bilinear map. We restrict encryption identities to be of length n for some fixed n. Identities will be sets of n elements of Z_p^*. With some minor modifications to our scheme, which we omit for simplicity, we can encrypt to all identities of size≤n. Note that here we associate each element with a unique integer in Z_p^*, while in practice an attribute will be associated with each element so that identities will have some semantics. We can also describe an identity as a collection of n strings of arbitrary length and hash strings into members of Z_p^* using a collision-resistant hash function, $H:\{0,1\}^* \rightarrow Z_p^*$.

The proposed ABTKIE system includes the following algorithms:

–Setup: The authority picks $y \in_R Z_p$, $g_2, h_1 \in_R G_1$, sets $g_1 = g^y$, picks $v_1, \ldots, v_{n+1} \in_R G_1$, lets N be the set $\{1, \ldots, n+1\}$ and defines a function, V, as $V(x) = g_2^{x^n} \prod_{i=1}^{n+1} v_i^{\Delta_{i,N}(x)}$. We can view V as the function $g_2^{x^n} g^{h(x)}$ for some n degree polynomial h. For clarity, we define $H_w: Z_p^* \rightarrow G_1$ to be the function $H_w(x) = g_1^x h_1$. The public parameters are published as $PK = (g_1, g_2, h_1, v_1, \ldots, v_{n+1})$ and the master secret key is $MK = y$.

–KeyGen: To generate the helper key and the initial private key for identity w, the authority works as follows. For each $i \in w$, pick b_i , $r_i \overset{U}{\leftarrow} Z_p^*$ and set the initial private key for identity w as

$TK_{w,0} = (\{R_i\}_{i \in w}, -, -, -) = (\{g_2^{b_i}\}_{i \in w}, -, -, -)$

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

$$HK_{w,i'} = (\{HK_{i,i'}^{\langle 1 \rangle}\}_{i \in w}, \{HK_{i,i'}^{\langle 2 \rangle}\}_{i \in w}) = (\{g_2^{l_{i,j}} V(i)^{r_{i,i'}}\}_{i \in w}, \{g^{r_{i,i'}}\}_{i \in w}) \qquad (1)$$

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

$$(\{(g_2^{q(i)-b_i} V(i)^{s_i})^{D_{i',S'}(0)} (\prod_{j=1}^{k-1} HK_{i,i'}^{\langle 1 \rangle})^{D_{i',S'}(j)}\}_{i \in w}, \{(g^{s_i})^{D_{i',S'}(0)} (\prod_{j=1}^{k-1} HK_{i,i'}^{\langle 2 \rangle})^{D_{i',S'}(j)}\}_{i \in w}) \qquad (2)$$

Here we claim that the helper keys in Eq. (2) have the same form as those in Eq. (1)[5].

–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 $(\{HK_{i,i'}^{\langle 1 \rangle}\}_{i \in w}, \{HK_{i,i'}^{\langle 2 \rangle}\})$. 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

$$UI_{w,t,i'} = (\{HK_{i,i'}^{\langle 1 \rangle} H_w(t)^{u_{i'}}\}_{i \in w}, \{HK_{i,i'}^{\langle 2 \rangle}\}_{i \in w}, g^{u_{i'}})$$

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

–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 $(\{R_i\}_{i \in w}, \{D_{i,t'}^{\langle 2 \rangle}\}_{i \in w}, D_{w,t'}^{\langle 3 \rangle}, \{d_i\}_{i \in w})$;

Parse $UI_{w,t,i'}$ as $(\{UI_{i,t,i'}^{\langle 1 \rangle}\}_{i \in w}, \{UI_{i,t,i'}^{\langle 2 \rangle}\}_{i \in w}, UI_{w,t,i'}^{\langle 3 \rangle})$; Set user w's temporary private key $TK_{w,t}$ for period t to be $(\{R_i\}_{i \in w}, \{(\prod_{i'} UI_{i,t,i'}^{\langle 1 \rangle})^{D_{i',S'}(0)}\}_{i \in w}, (\prod_{i'} UI_{w,t,i'}^{\langle 3 \rangle})^{D_{i',S'}(0)}, \{(\prod_{i'} UI_{i,t,i'}^{\langle 2 \rangle})^{D_{i',S'}(0)}\}_{i \in w})$

Note that in time period t, if let $r_i = \sum_{i' \in S''} \Delta_{0,S''}(i') \cdot r_{i,i'}$ and $u = \sum_{i' \in S''} \Delta_{0,S''}(i') \cdot u_{i'}$,then $TK_{w,t}$ is always set to be

$$(\{R_i\}_{i \in w}, \{D_{i,t}^{\langle 2 \rangle}\}_{i \in w}, D_{w,t}^{\langle 3 \rangle}, \{d_i\}_{i \in w}) = (\{g_2^{b_i}\}_{i \in w}, \ \{g_2^{q(i)-b_i} V(i)^{r_i} H_w(t)^u\}_{i \in w}, g^u, \{g^{r_i}\}_{i \in w}).$$

–Encryption: In time period t, to encrypt a message $M \in G_2$ with the public key w', a user picks $s \in_R Z_p$ and publishes the ciphertext as $E = (t, w', E' = Me(g_1, g_2)^s, E'' = g^s, E''' = H_w(t)^s, \{E_i = V(i)^s\}_{i \in w'})$.

–Decryption: Suppose that a ciphertext, *E*, is encrypted with identity *w′* and period index *t* while we have a temporary private key for identity *w* and period index *t*, where $|w\cap w'| \geq d$. Choose an arbitrary *d*-element subset, *S*, of $w\cap w'$. Then, the ciphertext can be decrypted as

$$M = E'\prod_{i\in S}(\frac{e(d_i, E_i)e(D_{w,t}^{\langle 3\rangle}, E''')}{e(R_iD_{i,t}^{\langle 2\rangle}, E'')})^{\Delta_{i,S}(0)}$$

$$= Me(g_1, g_2)^s\prod_{i\in S}(\frac{e(g^{r_i}, V(i)^s)e(g^u, H_w(t)^s)}{e(g_2^{b_i}g_2^{q(i)-b_i}V(i)^{r_i}H_w(t)^u, g^s)})^{\Delta_{i,S}(0)}$$

$$= Me(g_1, g_2)^s\prod_{i\in S}(\frac{e(g^{r_i}, V(i)^s)e(g^{k_{w,t}}, H_w(t)^s)}{e(g_2^{q(i)}V(i)^{r_i}H_w(t)^{k_{w,t}}, g^s)})^{\Delta_{i,S}(0)}$$

$$= Me(g_1, g_2)^s\prod_{i\in S}(\frac{e(g^{r_i}, V(i)^s)e(g^u, H_w(t)^s)}{e(g_2^{q(i)}, g^s)e(V(i)^{r_i}, g^s)e(H_w(t)^u, g^s)})^{\Delta_{i,S}(0)}$$

$$= Me(g, g_2)^{ys}\prod_{i\in S}\frac{1}{e(g, g_2)^{q(i)s\Delta_{i,S}(0)}}$$

$$=M.$$

Security

The proof of our proposed ABTKIE scheme is similar with that of Chen et al.'s ABKIE[1].

Conclusions

We introduce the notion of attribute-based threshold key-insulated encryption (ABTKIE) and describe a construction that is based on attribute-based encryption (ABE) 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] 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

[3] 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

[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