Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Engineering 29 (2012) 316 – 320

Procedia Engineering

www.elsevier.com/locate/procedia

2012 International Workshop on Information and Electronics Engineering (IWIEE)

Fully Secure Broadcast Encryption for Inner-Product Predicates

SUN Jin [1, 2,*] , HU Yu-pu [2]

1.Department of Application Mathematics in Xi'an University of Technology, Xi'an, 710048，China
2.Key Lab of Computer Network and Information Security, Xidian University, Xi'an, 710071，China

Abstract

According to the broadcast encryption scheme with wide applications in the real world without considering its security and efficiency in the model simultaneously, a fully secure broadcast encryption for inner-product predicates (IPBE) was proposed by combining with Waters dual system encryption methodology and inner-product predicate encryption. Based on the standard model, the scheme can not only achieve constant-size key and ciphertext, but also guarantee the security of the plaintext M as well as the security of the attribute vectors. Furthermore, the scheme is proved by using a non-interactive static assumption and the analysis results indicated that the scheme is fully secure.

Keywords: broadcast encryption; full security; inner-product predicate encryption; provably secure.

1. Introduction

The concept of the broadcast encryption were introduced by Fiat and Naor[1] firstly, which allow a sender, who wants to send a message to a dynamically chosen subset *S* of users, to construct a ciphertext such that only users in *S* can decrypt. It has become a new hot spot of the Cryptology promptly. Many broadcast encryption schemes [2-4] with special purpose were proposed consecutively. However, these schemes had some deficiency obviously, for example, their security was based on the strong assumption or non-standard cryptographic assumption; the scheme only guaranteed chosen plaintext security or selective-ID security; the scheme was designed under the random oracle model, etc.

Predicate encryption is an important cryptographic primitive that has been recently studied [5~8] and that has found wide applications as it allows for fine-grained key management. Roughly speaking, in a predicate encryption scheme, secret keys correspond to predicates in some class $\mathbb{F}$, and ciphertexts correspond to attributes in Σ. Until now, there have been three inner-product predicates encryption （IPE） schemes suggested [6-8]. The scheme [6] shows how inner-product predicates can be used as a

*.Corresponding author. tel.: 0086-0-18629299056. e-mail: oksunjin@xaut.edu.cn.

doi:10.1016/j.proeng.2011.12.714

building block to construct a wide class of predicates and can be realized in composite-order groups. The scheme [8] introduces a new method of using n-dimensional vector spaces in prime order groups, and shows how the delegation functionality is realized in an IPE scheme. Recently, Lewko *et al* [7] gave fully secure implementation for the inner-product predicate. However, these constructions only guaranteed the semantic security and security guarantee for specific predicates just in the selective model.

Our Contribution: In this work, the definition of IPBE and the security model for them were firstly proposed, then by combining with Waters dual system encryption methodology and inner-product predicate encryption, a fully secure broadcast encryption for inner-product predicates was brought forward. Based on the standard model, the scheme can achieve constant-size ciphertext which constrain only two group exponents, and guarantee the security of the plaintext M as well as the security of the attribute vectors.

2. Preliminaries

2.1. Definition of Broadcast Encryption for Inner- Product Predicate (IPBE)

A IPBE scheme consists of four probabilistic polynomial-time algorithms as following semantics:

Setup: takes as input the security parameter 1^{λ} and the attribute length n, outputs the master public key Pk and the master secret key Mk.

KeyGen: takes as input the master secret key Mk and the predicate $\boldsymbol{k}=(k_1,\ldots,k_n)$, outputs the decryption key $Sk_{\boldsymbol{k}}$ associated with $\boldsymbol{k}$.

Encrypt: takes as input the public key Pk, attribute string assemblage $\{\boldsymbol{x}\,|\,\boldsymbol{x}\in\{0,1\}^n\}$ and message M from the associated message space and returns ciphertext C.

Decrypt: takes as input a secret key $Sk_{\boldsymbol{k}}$ and a ciphertext C, outputs the message M or the distinguished symbol $\perp$.

2.2. Security Definition for Fully Secure Inner-Product Predicate Broadcast Encryption

We start by defining the security game $Game_{real}$ between an adversary A and a challenger $\Re$ for IPBE. $Game_{real}$ consist of a *Setup* phase and a *Query Answering* phase. More precisely, we have the following description.

Setup: $\Re$ inputs the security parameter λ and the length parameter n to generate public parameters pk and master secret key mk.

Key Query Answering: Upon receiving a query for predicate vector $\boldsymbol{y}$, $\Re$ returns $KeyGen(mk,\boldsymbol{y})$.

Challenge: Upon receiving the pair $(\boldsymbol{x}_0,\boldsymbol{x}_1)$, and challenge plaintexts (m_0,m_1), $\Re$ picks random $\eta\in\{0,1\}$ and returns $Encrypt(pk,\boldsymbol{x}_\eta)$. A outputs a guess η' for η at the end of the game. We define that A wins the game if $\eta=\eta'$ and if for all $\boldsymbol{y}$ for which A has issued a *Key Query*, it holds $f_{\boldsymbol{k}}(\boldsymbol{x})=1$.

2.3. Complexity Assumptions

Assumption (n-extended decisional Diffie-Hellman assumption (n-eDDH)): The n-eDDH problem is given $(param_G,g,g^k,\{g^{\omega+\gamma_i h_i},g^{\gamma_i},g^{h_i}\}_{1\le i\le n},\{g^{\gamma_i h_j}\}_{1\le i\ne j\le n},Y_b)\longleftarrow\aleph_b^{n-eDDH}(1^{\lambda})$, to guess $b\in\{0,1\}$, where $\aleph_b^{n-eDDH}(1^{\lambda}):param_G=(q,G,G_T,g,e)\leftarrow\aleph(1^{\lambda})$. Uniformly select $\omega,h_i,\gamma_i\in F_q$ for $i=1,\ldots,n$,

$k \in F_q^*$ and $Y_2 \in G$, sets $Y_0 = g^{k\omega}$, then return $(param_G, g, g^k, \{g^{\omega+\gamma_i h_i}, g^{\gamma_i}, g^{h_i}\}_{1\le i\le n}, \{g^{\gamma_i h_j}\}_{1\le i\ne j\le n}, Y_b)$. For a probabilistic machine A, the advantage of A for the n-eDDH problem is defined as: $Adv_A^{n-eDDH}(\lambda) := \left|\Pr\left[A(1^\lambda, \rho) \to 1 \middle| \rho \leftarrow \aleph_0^{n-eDDH}(1^\lambda)\right] - \Pr\left[A(1^\lambda, \rho) \to 1 \middle| \rho \leftarrow \aleph_1^{n-eDDH}(1^\lambda)\right]\right|$.

Definition1: For any polynomial time adversary A, the advantage $Adv_A^{n-eDDH}(\lambda)$ is negligible.

3. Our IPBE Scheme

3.1. Construction

In this section, we describe our construction for a broadcast encryption for inner-product predicates.

Setup $(1^\lambda, n)$**:** The algorithm chooses a description of a bilinear group $(param_{R^n}, \boldsymbol{B}, \boldsymbol{B}^*) \leftarrow \aleph(1^\lambda, 2n+3)$, and $\hat{\boldsymbol{B}} = (\beta_1, \ldots, \beta_n, \beta_{2n+1}, \beta_{2n+3})$, the public parameters are $pk = (1^\lambda, param_{R^n}, \hat{\boldsymbol{B}})$ and the master secret key is $mk = \mathbf{B}^*$, then return mk and pk.

KeyGen($mk, \mathbf{k}_l := (k_{l_1}, k_{l_2}, \cdots, k_{l_n})$ **):** Every user in the system with identity l ($l = 1, \cdots, m$), which m is the maximal number of user. The key generation algorithm chooses random $\sigma_l, \eta_l \in F_q$, and sets $sk_{\boldsymbol{k}_l} = \sigma_l(\sum_{i=1}^{n} k_{l_i} \cdot \beta_i^*) + \beta_{2n+1}^* + \eta_l \beta_{2n+2}^*$, then return $sk_{\boldsymbol{k}_l}$.

Encrypt: $(pk, m, \{\boldsymbol{x}_l \mid \boldsymbol{x}_l = (x_{l_1}, x_{l_2}, \ldots, x_{l_n}), l = 1, \ldots, h\})$**:** In order to send a message $m \in G_T$ to the receiver collection $\{\boldsymbol{x}_l \mid \boldsymbol{x}_l = (x_{l_1}, x_{l_2}, \ldots, x_{l_n}), l = 1, \ldots, h\}$ under the constraint that $(\sum_{l=1}^{h} \boldsymbol{x}_l) \cdot \boldsymbol{k}_l = 0$, the encryption algorithm chooses randomly $\delta_1, \delta_2, \xi \in F_q$, and return the ciphertext $C = (C_1, C_2)$, where $C_1 = \sum_{l=1}^{h}\left[\delta_1(\sum_{i=1}^{n} x_{l_i}\beta_i) + \xi\beta_{2n+1} + \delta_2\beta_{2n+3}\right]$, $C_2 = g_T^{h\xi} \cdot m$.

Decrypt ($pk, sk_{\boldsymbol{k}_l}, (C_1, C_2)$ **):** Upon receiving a ciphertext $C = (C_1, C_2)$, the legitimate user l computes and return message $m = \dfrac{C_2}{e(C_1, sk_{\boldsymbol{k}_l})}$.

3.2. Correctness

Let $C = (C_1, C_2)$ is legitimate ciphertext, then the correctness can be easily described by the following qualities $sk_{\boldsymbol{k}_l} = \{\sigma_l \boldsymbol{k}_l, 0, \ldots 0, 1, \eta_l, 0\}\boldsymbol{B}^*$, $C_1 = \{\sum_{l=1}^{h} \delta_1 \boldsymbol{x}_l, 0, \ldots, 0, l\xi, 0, l\delta_2\}\boldsymbol{B}$ and, $e(C_1, sk_{\boldsymbol{k}_l}) = g_T^{\{\sum_{l=1}^{h} \delta_1 \boldsymbol{x}_l, 0, \ldots, 0, l\xi, 0, l\delta_2\}\{\sigma_l \boldsymbol{k}_l, 0, \ldots 0, 1, \eta_l, 0\}}$

$= g_T^{\delta_1\xi_1(\sum_{l=1}^{h} \boldsymbol{x}_l)\boldsymbol{k}_l + h\xi}$, $e(C_1, sk_{\boldsymbol{k}_l}) = g_T^{h\xi}$ if $(\sum_{l=1}^{h} \boldsymbol{x}_l) \cdot \boldsymbol{k}_l = 0$, then $\dfrac{C_2}{e(C_1, sk_{\boldsymbol{k}_l})} = \dfrac{g_T^{h\xi} \cdot m}{g_T^{h\xi}} = m$.

3.3. Efficiency

Comparing with the current broadcast encryption, the novel scheme based on the standard model, can achieve constant-size ciphertext constrained two group exponents. Furthermore, *Encryption* algorithm does not require the bilinear pair computation and *Decryption* algorithm only need one. The scheme has been proved by using a non-interactive static assumption to guarantee the security of the plaintext m as well as the security of the attribute vectors. In addition, the analysis results indicated that the new scheme is fully secure and is better than other IPE schemes in the selective model.

4. Security Analysis

From Lemma 22 in literature [9], we can obtain: for any adversary A, there is a probabilistic machine $\Re$, whose running time is essentially the same as that of A, such that for any security parameter λ, $Adv_{\Re}^{n-eDDH}(\lambda) = Adv_{A}^{P_2}(\lambda)$.

Theorem For any adversary A and any security parameter λ, there exist probabilistic machines $C_k (k = 1,\ldots,t)$, who running the same times as that of A, such that $Adv_A^{PBE}(\lambda) \le \sum_{k=0}^{t} Adv_{C_k}^{n-eDDH}(\lambda) + \frac{t}{q}$. where t is the maximum number of adversary A's key queries. Thus, the proposed IPBE scheme shows adaptively attribute-hiding against chosen plaintext attacks security under the n-eDDH assumption.

Proof: To prove **Theorem**, we consider a sequence of $t+3$ games between A and a challenger $\Re$ for a probabilistic polynomial-time adversary A which makes t queries for $KeyGen$.

$Game_0$: The real security game described in the previous section.

$Game_1$: Same as $Game_0$ except that $\Re$ uses $C_1 = \sum_{l=1}^{h} [\delta_1(\sum_{i=1}^{n} x_{l_i}^{(b)} b_i) + \sum_{i=1}^{n} \omega_i b_{n+i} + \xi b_{2n+1} + \delta_2 b_{2n+3}]$ and $C_2 = g_T^{h\xi} m^{(b)}$ instead of the target ciphertext for challenge plaintexts $(m^{(0)}, m^{(1)})$ and challenge attributes $(\boldsymbol{x}^{(0)}, \boldsymbol{x}^{(1)})$, where $\delta_1, \delta_2, \xi \in F_q$, $b \in \{0,1\}$, $(x_1^{(b)},\ldots,x_n^{(b)}) = \boldsymbol{x}^{(b)}$, and $(\omega_1,\ldots,\omega_n) \in F_q^n \setminus \{\boldsymbol{0}\}$ are uniformly selected.

$Game_{2\to k}$ $(k = 1,\ldots,t)$: $Game_{2\to 0}$ is $Game_1$. $Game_{2\to k}$ is the same as $Game_{2\to(k-1)}$ except the reply to the k-th key query for $\boldsymbol{k} = (k_1,\ldots,k_n)$ is: $sk^* := \sigma(\sum_{i=1}^{n} k_i \beta_i^*) + \sum_{i=1}^{n} r_i \beta_{n+i}^* + \beta_{2n+1}^* + \eta \beta_{2n+2}^*$, where $\sigma, \eta \in F_q$ and $\boldsymbol{r} = (r_1,\ldots,r_n) \in F_q^n$.

$Game_3$: Same as $Game_{2\to t}$ except that the target ciphertext (C_1, C_2) for challenge plaintexts $(m^{(0)}, m^{(1)})$ and challenge attributes $(\boldsymbol{x}^{(0)}, \boldsymbol{x}^{(1)})$ is $C_1' = \sum_{l=1}^{h} [\sum_{i=1}^{n} x_{l_i}' \beta_i + \sum_{i=1}^{n} \omega_i \beta_{n+i} + \xi' \beta_{2n+1} + \delta_2 \beta_{2n+3}]$, $C_2' = g_T^{h\xi} m^{(b)}$, where $x_1',\ldots,x_n', \delta_2, \xi, \xi' \in F_q$, $b \in \{0,1\}$, and $(\omega_1,\ldots,\omega_n) \in F_q^n \setminus \{\boldsymbol{0}\}$ are uniformly selected. In particular, $(x_1',\ldots,x_n')$ and ξ' are chosen uniformly and independently from $(\boldsymbol{x}^{(0)}, \boldsymbol{x}^{(1)})$ and ξ.

Let $Adv_A^0(\lambda)$, $Adv_A^1(\lambda)$, $Adv_A^{2\to k}(\lambda)$, $Adv_A^3(\lambda)$ denote the advantage $Adv_A^{IPBE}(\lambda)$ of A in $Game_0$, $Game_1$, $Game_{2\to k}$, $Game_3$ respectively. It is clear that $Adv_A^3(\lambda) = 0$ because the value of b is independent from the adversary's view in $Game_3$.

From three lemmas(lemmas24-lemmas26) has been proved in paper [9], we can evaluate the gaps with pairs of $Adv_A^0(\lambda)$, $Adv_A^1(\lambda)$, $Adv_A^{2-k}(\lambda)$ ($k=1,..,v$), $Adv_A^3(\lambda)$ and obtain

$Adv_A^{IPBE}(\lambda) = Adv_A^0(\lambda) \le \left|Adv_A^0(\lambda) - Adv_A^1(\lambda)\right| + \sum_{k=1}^{v}\left|Adv_A^{2\to(k-1)}(\lambda) - Adv_A^{2\to k}(\lambda)\right| + \left|Adv_A^{2\to t}(\lambda) - Adv_A^3(\lambda)\right|$
$+ Adv_A^3(\lambda) \le Adv_{B_0}^{P_1}(\lambda) + \sum_{k=1}^{v} Adv_{B_k}^{P_2}(\lambda) + \frac{t}{q}$.

Thus, there exist probabilistic machines $C_k(k=1,\ldots,v)$, whose running times are essentially the same as those of B_k, respectively, such that $Adv_{C_0}^{n-eDDH}(\lambda) = Adv_{B_0}^{P_2}(\lambda)$ and $Adv_{C_k}^{n-eDDH}(\lambda) = Adv_{B_k}^{P_2}(\lambda)$. Hence $Adv_A^{IPBE}(\lambda) \le Adv_{B_0}^{P_1}(\lambda) + \sum_{k=1}^{v} Adv_{B_k}^{P_2}(\lambda) + \frac{t}{q} \le \sum_{k=0}^{t} Adv_{C_k}^{n-eDDH}(\lambda) + \frac{t}{q}$.

5. Conclusions

In view of no general constructions for specific predicates which guarantee the security of the attribute vectors, the new scheme was proposed to enjoy flexibility of expressive access policy and efficiency of small ciphertext and public key. Moreover, any group member can encrypt/decrypt the message simultaneously to satisfy the many-to-many secure group communication requirements. The scheme is proved by using a non-interactive static assumption, the analysis results indicated that the scheme is fully secure and can satisfy the higher efficiency and practice requirement.

Acknowledgements

This research was financed by the National Natural Science Foundation of China under Grants 61173192 and 60833008, and the Scientific Research Foundation of Education Department of Shaanxi Provincial Government of China (Grant No. 11JK0505).

References

[1] Fiat A, Naor M. Broadcast encryption// CRYPTO'93, 1993, LNCS, vol.773: 480-491.

[2] Hu L, Liu Z L，Cheng X H. Efficient identity-based broadcast encryption with- out random oracles. JOURNAL OF COMPUTERS, vol. 5(3), 2010: 331-336.

[3] Yu G, Ma X, Shen Y, *et al*. Provable secure identity based generalized signcryption scheme . Available at arXiv: 1004.1304v1, 2010.

[4] Zhang L Y, Hu Y P, Mu N B. Identity-based Broadcast Encryption Protocol for Ad Hoc Networks . IEEE Computer Society, 2009:1619-1623.

[5] Dan B, Brent W. Conjunctive, subset and range queries on encrypted data. In Salil P. Vadhan, editor, TCC 2007: 4th Theory of Cryptography Conference, LNCS, vol.4392:535-554, Amsterdam, The Netherlands, 2007:21-24. Springer-Verlag, Berlin, Germany.

[6] Jonathan K, Amit S, Brent W. Predicate Encryption Supporting Disjunction, Polynomial Equations, and Inner Products.//In Nigel Smart, editor, Advances in Cryptology-EUROCRYPT 2008, LNCS, vol. 4965 :146-162, Istanbul, Turkey, April 13-17, 2008. Springer-Verlag, Berlin, Germany.

[7] Allison L, Tatsuaki O, Amit S, *et al*.Fully secure functional encryption: Attribute-based encryption and (hierarchical) inner product encryption//In Henri Gilbert, editor, Advances in Cryptology -EUROCRYPT 2010, pages62-91.

[8]Okamoto T, Takashima K. Hierarchical predicate encryption for inner-products. Advances in Cryptlogy-ASIACRYPT2009, LNCS2009, vol. 5912: 214-231.

[9]Lewko A, Okamoto T, Waters B. Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption. Advances in Cryptlogy-EUROCRYPT2010, LNCS2010, vol.6110:62-91.