一个安全公钥广播加密方案*

谭作文[1,2+], 刘卓军[1,2], 肖红光[3]

[1](中国科学院 数学与系统科学院 系统科学研究所,北京 100080)
[2](信息安全国家重点实验室(中国科学院 研究生院),北京 100049)
[3](长沙理工大学 电子信息工程系,湖南 长沙 410076)

A Fully Public Key Tracing and Revocation Scheme Provably Secure Against Adaptive Adversary

TAN Zuo-Wen[1,2+], LIU Zhuo-Jun[1,2], XIAO Hong-Guang[3]

[1](Institute of Systems Science, AMSS, The Chinese Academy of Sciences, Beijing 100080, China)
[2](State Key Laboratory of Information Security (Graduate School, The Chinese Academy of Sciences), Beijing 100049, China)
[3](The College of Electronics Information Engineering, Changsha University of Science & Technology, Changsha 410076, China)
+ Corresponding author: Phn: +86-10-82682543, E-mail: tanzywl@mail.amss.ac.cn, http://www.amss.ac.cn
Received 2004-04-07; Accepted 2004-07-06

Tan ZW, Liu ZJ, Xiao HG. A fully public key tracing and revocation scheme provably secure against adaptive adversary. *Journal of Software*, 2005,16(7):1333−1343. DOI: 10.1360/jos161333

Abstract: A broadcast encryption allows the sender to securely distribute content to a dynamically changing group of users over a broadcast channel. A public key tracing and revocation scheme can combine the public key encryption with the traitor tracing algorithm. This paper proposes a fully public key tracing and revocation scheme. The salient feature of the scheme is that the secret keys of the users are chosen by the users themselves, while in the previous public key broadcast encryption schemes, the broadcaster publishes the encryption key and distributes the individual secret keys to the users. The scheme deals with the setting of stateless receivers. When the traitors are found, the sender can revoke them without involvement of the remaindering receivers. The encryption algorithm in the scheme is semantically secure against adaptive chosen cipher-text attacks based on the DDH assumption.
Key words: broadcast encryption; provably secure; black-box tracing; adaptive adversary

摘 要: 消息的发送者使用广播加密算法通过广播信道将消息发送给用户.公钥加密算法和追踪算法结合在一起,可构成一个公钥广播加密方案.提出了一个完全式公钥广播加密方案.在以往公钥广播加密方案中,消息发送中心替每个用户选择解密私钥,分配解密私钥.而在完全式公钥广播加密方案中,用户的解密私钥是由用户自己所选择的.用户可以随时加入或退出广播系统.当消息发送者发现非法用户时,不要求合法用户作任何改变,就

* Supported by the National Natural Science Foundation of China under Grant No.10371127 (国家自然科学基金)

TAN Zuo-Wen was born in 1967. He is a Ph.D. candidate at the Institute of Systems Science, the Chinese Academy of Sciences. His current research interests include information security, network security and cryptography. **LIU Zhuo-Jun** was born in 1958. He is a professor and doctoral supervisor at the Institute of Systems Science, the Chinese Academy of Sciences. His research areas are symbolic computation and information security. **XIAO Hong-Guang** was born in 1970. He is a Ph.D. candidate at Changsha University of Science & Technology. His current research interests include information security and network security.

能够很方便地取消这些非法用户.此外,证明了方案中加密算法在DDH假设和适应性选择密文攻击下是安全的.
关键词: 广播加密;可证安全; black-box 追踪;适应性攻击
中图法分类号: TP309 文献标识码: A

1 Introduction

Broadcast encryption. Broadcast encryption involves a sender and a large number of users (receivers). The sender first encrypts digital content, and then transmits it to a dynamically changing set of users via insecure broadcasting channels. The broadcast encryption scheme assures that only privileged receivers can recover the content subscribed and the unauthorized users can learn nothing. Revocation of a user is necessary for broadcast encryption schemes, for a user unsubscribes the programs or leaves the system entirely, or for the user is corrupted to create an illegal decryption key. It is for this reason that broadcast encryption scheme is called revocation scheme. Broadcast encryption schemes have found many applications, including pay-per-view television systems, distribution of copyrighted materials, such as CD/DVD, and many others. The area of broadcast encryption is first formally introduced by Fiat and Naor[1] and has received much attention since then[2,3]. Blundo and Cresti[4] prove the information theoretic low bounds for a model of unconditionally secure broadcast encryption. Some broadcast encryption schemes obtain a trade-off between storage and communication[3,5].

The basic technique of broadcast encryption is that the sender generates a message encryption key S, allocates every privileged user a private key from which the encryption key S can be obtained, and broadcasts ⟨*enabling block*, *cipher block*⟩, where cipher block represents the encryption of the message and the encryption key S is embedded in the enabling block. Thus, key pre-distribution schemes (KPS for short) are related with broadcast encryption schemes. In the broadcast encryption schemes, KPS can be categorized as follows: (1) combinatorial approaches: schemes using combinatorial design[3,6,7]; schemes using tree structure[8,9]; (2) algebraic approaches: schemes using secret share on the exponent[10−12].

Tracing mechanism. Chor, Fiat and Naor[13] introduced the concept of a traitor tracing scheme to discourage the subscribers from giving away their private keys. A traitor may let its decryption key out for its profits. Tracing mechanism allows the detection of at least one "identity" of the keys that are used to create an illegal decryption key among the collusion users. Traitor tracing includes straight tracing and black box tracing. The straight tracing method can get the traitor's key through cracking the "pirate box", e.g. set-top terminals in Pay-Tv systems, and determine all the traitors. The other deals with the pirate decryption box as an oracle to query on various inputs. The way the black box behaves on different inputs should reveal the information contained[14,15].

Public key tracing and revocation. A broadcast encryption scheme combined with tracing mechanism is called a tracing and revocation scheme[6,10,11,15]. These schemes might adopt symmetric key approach or public key approach. The secret key approach has every user holding a set of keys. Only the trusted designer of the system can broadcast message to the receivers. Generally speaking, as the number of subscribers is large, the schemes become impractical. The public key approach has the size of enabling block independent of the number of qualified receivers, but dependent on the number of revocative users, with each user holding only one key[16,17]. The setting of standard public key broadcast encryption scheme is as follows. The sender generates a single public key and distributes individual secret keys to the receivers of the broadcast. This is a one-to-many map. All the receivers but the specified subset of "revoked" receivers can decrypt the message. Furthermore, if a group of receivers collude to produce an "illegal" decoder, the sender can trace at least one of the "traitors". Differently from the secret key case, its scalability allows any third party (not necessarily trusted one) to use the encryption mechanism and broadcast digital content to the set of privileged receivers. Boneh and Franklin introduced their public key traitor tracing

scheme[16]. Based on the hardness of the discrete logarithm problem, its tracing algorithm is deterministic, and its encryption is semantically secure on the assumption of the decision Diffie-Hellman problem. Graray, Staddon and Wool[2] presented a long-lived public key traitor tracing scheme in which by discarding a part of the keys in the encryption procedure, some users can be excluded from the broadcast system and in a long run, a steady percent of keys of legitimate users need to be refreshed while revoking other users. Tzeng and Tzeng[18] proposed a new public traitor tracing scheme with revocation capability, using the dynamic share and entity revocation techniques. By dynamically assigning shares into the enabling block, the scheme increases the revocation capability. Its traitor tracing is fully k-resilient.

Our result. We concentrate on the revocation and tracing scheme for stateless receivers[2,9,12,16,18]. The distinct feature of the stateless case is that when the traitors are found, we can revoke their private keys without updating others' keys, or when a new user is added, other users' secret keys remain unchanged.

Our scheme is motivated by Ref.[19]. One of its advantages over the previous public key broadcast encryption schemes is that it is a fully public key scheme in which each receiver chooses his or her own private decryption key, while in a general public key broadcast encryption scheme, the sender generates and assigns all the keys. In a fully public key broadcast encryption scheme, the sender can not control all the receivers any longer, but once a coalition of some receivers occurs, the scheme still can trace them. To our best knowledge, of all the existing public key broadcast encryption schemes, those schemes which adopt secret share on the exponent are more efficient. This is that because their enabling block is independent of the number of the receivers, but dependent on the collusion and revocation thresholds. The technique in Ref.[18] can increase the revocation capability, but degrade its efficiency. In our fully public key scheme, the enabling block is independent of both the number of the receivers and the number of the revocation.

Following the idea of Ref.[19], we first introduce carefully a formalized model and present a fully public key broadcast encryption scheme, where an unlimited number of users can be added and removed efficiently from the system. Addition or revocation does not require to rekey other users. Its black-box tracing algorithm can track down all the colluders regardless of their size. We improve the security of the scheme in Ref.[19], which is plain-text secure assuming the hardness of computational Diffie-Hellman and semantically secure assuming the hardness of DDH against a passive generic adversary. Our scheme is semantically secure against adaptive chosen ciphertext attack (CCA2) on the DDH assumption, allowing the adversary to corrupt the users at any point during the execution. We take Cramer-Shoup[20] scheme as the encryption scheme and provide a rigorous proof based on Refs.[20, 21].

The rest of the paper is organized as follows: some preliminaries are introduced in Section 2. In the third section, we propose the model of the fully public key broadcast encryption scheme. In Section 4, we present a novel fully public key broadcast encryption scheme. In Section 5, we investigate the security property of the proposed scheme. Section 6 contains a conclusion.

2 Preliminaries

We first present a number-theoretical result.

Lemma 1.[19] If q, $p=2q+1$ are two large primes, then for any integer a with $0<a<p-1$, $-a^2$ is a primitive root modulo p.

Now, we recall the Decision Diffie-Hellman problem.

Definition 2. Let G be the group of a large order n and let a be a generator of G. Let B be an adversary that takes as input n and three elements (β,γ,δ), and outputs a bit. Let $I=\{n\}$. Consider two experiments.

Experiment $\mathbf{Exp}_{I,\alpha}^{ddh-real}(B)$

$a \xleftarrow{R} Z_n$; $\beta \leftarrow \alpha^a$;

$b \xleftarrow{R} Z_n$; $\gamma \leftarrow \alpha^b$;

$\delta \leftarrow \alpha^{ab}$

$d \leftarrow B(n,\alpha,\beta,\gamma,\delta)$

Return d

Experiment $\mathbf{Exp}_{I,\alpha}^{ddh-rand}(B)$

$a \xleftarrow{R} Z_n$; $\beta \leftarrow \alpha^a$;

$b \xleftarrow{R} Z_n$; $\gamma \leftarrow \alpha^b$;

$\delta \leftarrow G$

$d \leftarrow B(n,\alpha,\beta,\gamma,\delta)$

Return d

The advantage of B is defined:

$$Adv_{I,\alpha}^{ddh}(B)=\Pr[\mathbf{Exp}_{I,\alpha}^{ddh-real}(B)=1]-\Pr[\mathbf{Exp}_{I,\alpha}^{ddh-rand}(B)=1] \quad (1)$$

For any t, we define the advantage of the *DDH*

$$Adv_{I,\alpha}^{ddh}(t)=\mathrm{Max}\{Adv_{I,\alpha}^{ddh}(B)\}$$

where the maximum is over all B having time-complexity t.

3 Model of the Fully Public Key Broadcast Encryption Scheme

We formalize the fully public key broadcast encryption scheme (FBE) as the following algorithms.

• Key generation algorithm (*KGen*)

The sender publishes some information I including the security parameter 1^{λ}. According to I, the potential receiver U_i randomly chooses his/her own secret key SK_i and computes its public key PK_i. When a user U_i wants to join the system, U_i sends its public key to the sender. On receiving these public keys PK_1, PK_2, …, PK_n , where n is the number of the users, the sender computes the system encryption key.

• Broadcast encryption algorithm (*BEnc*)

The sender randomly chooses a session encryption key s . After that, it encrypts the session key s with PK as the enabling block Γ, and computes the cipher block $C'=E(m,s)$, where m is the message to broadcast and E is a symmetric encryption algorithm, and then broadcasts the ciphertext:

$$C=\langle \Gamma, C' \rangle=\langle BEnc(s, PK), E(m,s) \rangle.$$

• Conversion algorithm (*Con*)

While receiving the broadcast C, every user U_i converts it into the ciphertext C_i pertaining to the user. The conversion algorithm takes as input the public key PK_i and the ciphertext , and outputs $C_i=\mathrm{Con}(PK_i, C)$.

• Decryption algorithm (*Dec*)

Each user U_i obtains the session key s through the decryption algorithm which takes as input the secret key SK_i and the enabling block in the ciphertext C_i , decrypts the ciphertext block, and then gets the message m.

• Add-user algorithm (*Add*)

This is a key generation procedure by the cooperation of the sender and the new user. The new user acts as the one in the key generation algorithm, while the sender produces the new system public key based on the original

system public key PK and the new user's public key PK_{new}.

• Revocation algorithm (*Rev*)

Given the current public key PK and a user's public key PK_i, the algorithm results in a new system public key PK', so that for all the messages m, the cipher-ext $C=\langle BEnc(s', PK), E(m,s')\rangle$ and all the conversion cipher-text $C'_j = Con(PK_j\ C')$ should be "incomprehensible" for the user pertaining to the key PK_i, while the legal users should be capable of decrypting it without any change of their secret keys and public keys.

• Tracing algorithm (*Tr*)

Given a pirate decoder, the algorithm *Tr* outputs its public keys contained in the decoder by querying the decoder and analyzing the queries, and then finds these users who collude to produce the pirate decoder.

4 Our Fully Public Key Broadcast Encryption Scheme

In this section, we present our fully public key broadcast encryption scheme as the following procedures.

Key generation.

The sender chooses randomly two large primes $q, p=2q+1$ and two elements a_1, a_2 in Z_p, such that $1<a_1, a_2<p-1$. We denote the common information by $I=(p,q,\overline{g_1},\ \overline{g_2}\}$, 1^λ where 1^λ is the system security parameter, $\overline{g_1}=a_1^2$, $\overline{g_2}=a_2^2$. Each user U_i chooses two random primes $q_i, p_i=2q_i+1$, where $p_i>p$ and computes $g_{i1}=\overline{g_1}^2 \bmod p_i$, $g_{i2}=\overline{g_2}^2 \bmod p_i$. Note that for $i\neq j$, $p_i\neq p_j$. g_{i1} and g_{i2} have prime order q_i in $Z_{p_i}^*$. Then, U_i chooses x_{i1}, x_{i2}, y_{i1}, y_{i2}, z_{i1}, z_{i2} in Z_{q_i}, and computes

$$c_i=g_{i1}^{x_{i1}}\cdot g_{i2}^{x_{i2}} \bmod p_i, d_i=g_{i1}^{y_{i1}}\cdot g_{i2}^{y_{i2}} \bmod p_i, h_i=g_{i1}^{z_{i1}}\cdot g_{i2}^{z_{i2}} \bmod p_i.$$

If the user U_i subscribes broadcast service, U_i transmits the set p_i, c_i, d_i, h_i to the sender. The set is called the user U_i's public key, denoted by PK_i. On receiving the subscribers' public keys, the sender computes

$$g_1=\overline{g_1}^2 \bmod N,\ g_2=\overline{g_2}^2 \bmod N, \text{ where } N=\prod_{i=1}^n p_i.$$

Note that g_1, g_2 are two generators of the cyclic group consisting of all the quadratic residues in Z_N^*, whose order is $q'=\prod_{i=1}^n q_i$. Through the Chinese Remainder Theorem, the sender computes

$$c=c_i \bmod p_i,\ d=d_i \bmod p_i,\ h=h_i \bmod p_i,$$

where $i=1,2,...,n$. The sender chooses randomly $H(\cdot)$ from the family of universal one-way hash functions that map long bit strings to elements of $Z_{q'}$. The system public key is $PK=\{g_1, g_2, c, d, h, H(\cdot)\}$.

Broadcast Encryption.

The sender selects a random number a_0, such that $1<a_0<\sqrt{p}$, and computes $s=a_0^2$ as the session key. The sender encrypts *s* with the Cramer-Shoup scheme. That is, the sender chooses $r\in Z_q$, and computes

$$u_1=g_1^r,\ u_2=g_2^r,\ e=h^r\cdot s,\ \alpha=H(u_1,u_2,e),\ v=c^r\cdot d^{\alpha r}.$$

Then the enabling block is $BEnc(s,PK)=(u_1, u_2, e, v)$. To broadcast message m, the sender broadcasts

$$C=\langle BEnc(s,PK), E(m,s)\rangle=\langle \Gamma, C'\rangle.$$

Decryption.

When receiving the broadcast $\langle \Gamma, C'\rangle$, the user U_i takes the conversion algorithm and obtains the associated

cipher-text $C=\langle Con(\Gamma), C'\rangle=\langle \Gamma_i, C'\rangle$. Here, the conversion algorithm is to only compute the remainder modulo prime p_i: $\Gamma_i=(u_{i1}=u_1,u_{i2}=u_2,e_i=e,v_i=v)$. Then, the user U_i computes $\alpha=H(u_1,u_2,e)$ and checks if

$$v_i=u_{i1}^{x_{i1}+y_{i1}\cdot\alpha}\cdot u_{i2}^{x_{i2}+y_{i2}\cdot\alpha} \bmod p_i.$$

If the equation holds, U_i computes $s=e_i/h_i^r=e_i/(u_{i1}^{z_{i1}}\cdot u_{i2}^{z_{i2}}) \bmod p_i$ and uses s to decrypt $E(m,s)$.

Remark. For i, the hash value α is computed from (u_1,u_2,e), not from (u_{i1},u_{i2},e_i).

Traitor tracing.

Our traitor tracing algorithm can be classified into straight traitor tracing and black box tracing, which is similar to algorithms in Ref.[19]. The black box tracing is somewhat different. For completeness, we list its steps.

Step 1. Compute $g_1=\overline{g_1}^2 \bmod N/p_i$, $g_2=\overline{g_2}^2 \bmod N/p_i$, and for all $j\neq i$, compute $c=c_j \bmod p_j$, $d=d_j \bmod p_j$, $h=h_j \bmod p_j$.

Step 2. Choose a quadratic residue s as in Key Generation procedure and compute the enabling block Γ with the new system public key $(g_1,g_2,c,d,h,H(\cdot))$.

Step 3. Given $\Gamma_i=Con(\Gamma)$, if the black box decoder outputs s' and $s'\neq s$, then the user U_i is a traitor.

Thus, the tracing algorithm can track down all and only traitors.

Long-Livedness.

When some users are removed or some new users join the system, the system can assure that only the legitimate receivers can receive the service without any change on the remaindering or existing users' secret keys. The end can be obtained by modifying the system public key. Assume that $(g_1,g_2,c,d,h,H(\cdot))$ is the original system key. Suppose that the user U_i is compromised, since U_i is a traitor or U_i unsubscribes the broadcast encryption subsequent service, then the new system public key is

$$(g_1 \bmod N/p_i, g_2 \bmod N/p_i, c', d', h', H(\cdot)),$$

where for all $j\neq i$, c',d',h' satisfy the following:

$$c'=c_j \bmod p_j,\quad d'=d_j \bmod p_j,\quad h'=h_j \bmod p_j.$$

If a new user U_{n+1} subscribes the service, the user randomly chooses primes p_{n+1}, q_{n+1} such that $p_{n+1}=2q_{n+1}+1$, $q_{n+1}>q$. The sender computes w_1, w_2, c',d',h' from the following

$$p_{n+1}\cdot w_1=1 \bmod N,\quad N\cdot w_2=1 \bmod p_{n+1},$$
$$c'=c\cdot p_{n+1}\cdot w_1+c_{n+1}\cdot N\cdot w_2 \bmod N\cdot p_{n+1},$$
$$d'=d\cdot p_{n+1}\cdot w_1+d_{n+1}\cdot N\cdot w_2 \bmod N\cdot p_{n+1},$$
$$h'=h\cdot p_{n+1}\cdot w_1+h_{n+1}\cdot N\cdot w_2 \bmod N\cdot p_{n+1}.$$

then, the new system public key is $(g_1 \bmod N\cdot p_{n+1}, g_2 \bmod N\cdot p_{n+1}, c',d',h', H(\cdot))$.

As shown above, a removed user can not decrypt the broadcast using its secret key and a new subscriber cannot decrypt the broadcast before the subscriber joins the system. The correctness of the above methods is easily verified.

5 Analysis of the Proposed Scheme

Before we proceed to discuss the security of our scheme, we formalize the model of the adaptive adversary in the adaptively chosen cipher-text attack (CCA2). It comprises three stages. In the first stage, (PK, PK_i, SK_i) $(i = 1,2,...,n) \leftarrow KGen(I,1^{\lambda})$ is run and the adversary A is given the public keys (PK, PK_i). Then A enters the corruption stage. Suppose that A is given a user corruption oracle Cor. This oracle takes as input the index i of the user U_i to be corrupted and returns $SK_i \leftarrow Cor(U_i)$. Let R be the set of the compromised users at the end of the stage.

In the Find stage, A finds a pair of session key s_0, s_1, and then queries the encryption Oracle $BEnc_{PK,R,\sigma}$ on it, where the bit σ is randomly chosen by the oracle. $BEnc_{PK,R,\sigma}$ returns the challenge enabling block Γ^*. At the end of this stage, A outputs a bit σ^8. In the second and third stages, A is equipped with some Decryption Oracles, with the same number as the number of the remaindering users. When A calls any of them at any point during the two stages, the Decryption Oracle is given an enabling block of A's choice and returns the session key contained in the enabling block. The enabling block Γ queried is only restricted that it is not equivalent with the challenge Γ^*. Specifically speaking, there does not exist i in the index set of legal users, such that $\Gamma_i = \Gamma_i^*$.

Now we give the definitions of the advantage of A and the advantage of FES.

As usual, we consider the Experiments.

Experiment $\mathbf{Exp}_{FBE,I}^{cca2}(A, \sigma)$

For $i = 1,2,...,n$,

do (PK, PK_i, SK_i) $(i = 1,2,...,n) \leftarrow KGen(I,1^{\lambda})$ Endfor

$\sigma^* \leftarrow A^{BEnc_{PK,R,\sigma}, Dec_1, Dec_2, ..., Dec_n}(I, PK, PK_1, ..., PK_n)$

Return σ^*.

Definition 3. The advantage of the adversary A in CCA2 is defined as follows

$$Adv_{FBE,I}^{cca2}(A) = Pr[\mathbf{Exp}_{FBE,I}^{cca2}(A,0) = 0] - Pr[\mathbf{Exp}_{FBE,I}^{cca2}(A,1) = 0] \quad (2)$$

Define the advantage of our fully public encryption as follows

$$Adv_{FBE,I}^{cca2}(t, q_e, q_d) = \mathrm{Max}\{Adv_{FBE,I}^{cca2}(A)\} \quad (3)$$

where the maximum is over all A with time-complexity t, at most q_e queries to the encryption oracle and at most q_d queries to each decryption oracle.

The encryption algorithm of the fully public key broadcast encryption scheme is semantically secure against the adaptive chosen cipher-text attack. We will prove the result using the similar technique to that in Ref.[18].

Theorem 4. Assume that the DDH problem is hard, the encryption algorithm of our fully public key broadcast encryption scheme is semantically secure against the adaptive chosen cipher-text attack.

Proof. Let A be a probabilistic polynomial-time adversary attacking our fully public key broadcast encryption scheme. Assume that A makes at most q_d queries to each of its n decryption oracles. By the adversary A, we construct a probabilistic polynomial-time algorithm B that tries to solve DDH problem. We will reduce the advantage of B into the advantage of the adversary A.

Let I denote the prescribed information including $\{p,q,p_1,q_1,...,p_n,q_n\}$, where n is the number of legal users and all p_i,q_i have the same property as in our scheme. The adversary B is given the set (I,g_1,g_2,u_1,u_2), where g_1, g_2 are the generators of the quadratic residue group of Z_M^*, the quadruple (g_1,g_2,u_1,u_2) has the form (g,g^x,g^y,g^{xy}) or (g,g^x,g^y,g^z), $x,y\in_R Z_q$ and $z\neq xy \pmod q$. B will run the adversary A as a subroutine. On basis of B, we design a simulator that can simulate A's view during its attack.

1) Key generation

(a) Compute the quadratic $(g_{i1},g_{i2},u_{i1},u_{i2.})$, $i=1,2,...,n$

$$g_{i1}=g_1 \mod p_i,\ g_{i2}=g_2 \mod p_i,\ u_{i1}=u_1 \mod p_i,\ u_{i2}=u_2 \mod p_i \tag{4}$$

(b) Randomly select x_{i1}, x_{i2}, y_{i1}, y_{i2}, z_{i1}, z_{i2} in Z_{q_i} as the user U_i's secret key, and computes

$$c_i=g_{i1}^{x_{i1}}\cdot g_{i2}^{x_{i2}} \mod p_i,\ d_i=g_{i1}^{y_{i1}}\cdot g_{i2}^{y_{i2}} \mod p_i,\ h_i=g_{i1}^{z_{i1}}\cdot g_{i2}^{z_{i2}} \mod p_i \tag{5}$$

as U_i's public key, and computes

$$c=c_j \mod p_j,\ d=d_i \mod p_j,\ h=h_i \mod p_j \tag{6}$$

Then the system public key is $(g_1,g_2,c,d,h,H(\cdot))$, where $H(\cdot)$ is randomly chosen from the family of universal one-way functions with any long bit string mapped into Z_q.

2) Challenge

The adversary A finds two secret keys s_0 and s_1, which are quadratic residue module all the Z_{p_i}.

3) Broadcast encryption

Randomly picks σ and computes

$$e_i=s_\sigma\cdot u_{i1}^{z_{i1}}\cdot u_{i2}^{z_{i2}} \mod p_j,\ e=e_i \mod p_j,\ \alpha=H(u_1,u_2,e) \tag{7}$$

$$v_i=u_{i1}^{x_{i1}+y_{i1}\cdot\alpha}\cdot u_{i2}^{x_{i2}+y_{i2}\cdot\alpha} \mod p_j,\ v=v_i \mod p_j \tag{8}$$

The cipher-text of s_σ is $\Gamma^*=(u_1,\ u_2,e,v)$.

4) Decryption

Given the enabling block Γ and i, the decryption oracle Dec_i first computes $\alpha=H(u_1,u_2,e)$, then checks the validity by verifying

$$v_i=u_{i1}^{x_{i1}+y_{i1}\cdot\alpha}\cdot u_{i2}^{x_{i2}+y_{i2}\cdot\alpha} \mod p_i \tag{9}$$

If it is not valid, the oracle rejects it; otherwise, the oracle returns

$$s=e_i/(u_{i1}^{z_{i1}}\cdot u_{i2}^{z_{i2}}) \mod p_i \tag{10}$$

Since the secret keys are all known to the simulator, the simulator can answer the queries to the encryption oracles and the decryption oracles. The simulation above is feasible. Thus, we complete the description of the simulator. The adversary B_A takes as input (I,g_1,g_2,u_1,u_2) and output 1 if and only if $\sigma=A(\Gamma)$, where Γ is the enabling block of the challenge session key s_σ.

Now we analyze the advantage of the adversary B.

When B_A's quadratic input has the form (g,g^x,g^y,g^{xy}). In other words, $g_1=g,g_2=g^x,u_1=g^y,u_2=g^{xy}$ (mod N). Then for all $i\in\{1,2,...,n\}$, $(g_{i1},g_{i2},u_{i1},u_{i2})$ has the same property. As Lemma 1 in Ref.[20] states, the

simulator outputs a perfectly legitimate cipher-text and the joint distribution of the adversary A's view and the hidden bit σ is statistically indistinguishable from that in the actual attack except with negligible probability.

In this case, the success probability of any adversary for the DDH problem is

$$\Pr[\mathbf{Exp}_{I,g_1}^{ddh-real}(B)=1] \geq \Pr[\mathbf{Exp}_{I,g_1}^{ddh-real}(B_A)=1]$$

$$\geq \frac{1}{2}\Pr([\mathbf{Exp}_{FBE,I}^{cca2}(A,0)=0])+\frac{1}{2}\Pr([\mathbf{Exp}_{FBE,I}^{cca2}(A,1)=1])-\sum_{i=1}^{n}\sum_{j=1}^{q_{d_i}}1/(q_i-j+1)$$

$$\geq \frac{1}{2}+\frac{1}{2}Adv_{FBE,I}^{cca2}(A)-\sum_{i=1}^{n}\sum_{j=1}^{q_{d_i}}1/(q_i-q_j+1) \quad (11)$$

The second sum of the last terms in the third and last rows above refers to the probability with which the decryption oracle Dec_i accepts the invalid enabling block. q_{di} denotes the number of queries to the decryption oracle Dec_i.

When B_A's input has the form (g,g^x,g^y,g^z), $x,y,z \in_R Z_q$, and $z \neq xy \bmod q$, we will show that the distribution of the hidden bit σ is independent of the adversary' view. This can be proved through the following analogue of the proof in Lemma 2[20].

Claim 1: If the decryption oracle rejects all invalid enabling blocks, then the distribution of the challenge bit σ is independent of the adversary's view.

Note that when the input value u_1,u_2 are random, so are u_{i1},u_{i2}. Consider the point

$$Q=(z_{11},z_{12},z_{21},z_{22},\ldots,z_{n1},z_{n2}) \in Z_{q_1}\times Z_{q_2}\times\ldots\times Z_{q_n}\times Z_{q_n}.$$

Let $w_i=\log_{g_{i1}} g_{i2} \bmod q_i$ and $u_{i1}=g_{i1}^{r_{i1}} \bmod p_i$, $u_{i2}=g_{i1}^{w_i r_{i2}} \bmod p_i$. From each user's public key, the equations hold

$$z_{i1}+z_{i2}\cdot w_i=\log_{g_i} h_i \bmod q_i \quad (12)$$

Every decryption oracle can not contribute a little. Consider the output (u_{i1},u_{i2},e_i,v_i) of the encryption oracle for (i,s_σ). We have $e_i=s_\sigma\cdot u_{i1}^{z_{i1}}\cdot u_{i2}^{z_{i2}}$. Let $e'_\sigma=u_{i1}^{z_{i1}}\cdot u_{i2}^{z_{i2}} \bmod p_i$. Thus, the adversary can obtain the equation

$$r_{i1}z_{i1}+w_i\cdot r_{i2}\cdot z_{i2}=\log_{g_{i1}} e'_\sigma \bmod q_i \quad (13)$$

Observing the simulation, we can find that for all i, r_{i1} is the same, and r_{i2} is also the same. It is enough to consider the claim for i. Equations (12) and (13) are linearly independent. It follows that σ is independent of the adversary's view, even B_A queries every decryption oracle.

Claim 2: The decryption oracles will reject all invalid ciphertexts except with negligible probability.

We investigate the distribution of the point

$$P=\{x_{11},x_{12},y_{11},y_{12},\ldots,x_{n1},x_{n2},y_{n1},y_{n2}\}.$$

According to all the users' public keys, there are the following equations

$$x_{i1}+x_{i2}\cdot w_i=\log_{g_i} c_i \bmod q_i,\quad y_{i1}+y_{i2}\cdot w_i=\log_{g_i} d_i \bmod q_i \quad (14)$$

From the output of the encryption oracles and conversion algorithm, the equations hold.

$$r_1\cdot x_{i1}+w_i\cdot r_2\cdot x_{i2}+\alpha\cdot r_1\cdot y_{i1}+\alpha\cdot w_i\cdot r_2\cdot y_{i2}=\log_{g_{i1}} v_i \bmod q_i \quad (15)$$

Now assume that the adversary submits an invalid enabling block (u'_1,u'_2,e',v') to all of its decryption oracles. Here, the invalid enabling block satisfies

$$(u'_{i1},u'_{i2},e'_i,v'_i)\neq(u_{i1},u_{i2},e_i,v_i), \text{ for all } i \quad (16)$$

Let $\log_{g_{i1}} u'_{i1}=r'_{i1}$, $\log_{g_{i2}} u'_{i2}=r'_{i2}$, and $r'_{i1}\neq r'_{i2}$, $\alpha'=H(u'_1,u'_2,e')$.

Case 1. $(u_1', u_2', e')=(u_1, u_2, e)$ but for all i, $v_i' \neq v_i$, which implies the decryption oracle will reject.

Case 2. $(u_1', u_2', e') \neq (u_1, u_2, e)$ and $\alpha = \alpha'$. In the case, we can draw a contradiction that $H(\cdot)$ comes from the family of a universal one-way hash function.

Case 3. $(u_{i1}', u_{i2}', e_i') \neq (u_{i1}, u_{i2}, e_i)$ and $\alpha \neq \alpha'$.

In this case, the decryption oracles will reject unless the point P satisfies the equation.

$$r_{i1}' \cdot x_{i1} + w_i \cdot r_{i2}' \cdot x_{i2} + \alpha \cdot r_{i1}' \cdot y_{i1} + \alpha' \cdot w_i \cdot r_{i2}' \cdot y_{i2} = \log_{g_{i1}} v_i' \mod q_i \tag{17}$$

For every i, the coefficient determinant of (14), (15), and (17) is as follows

$$\det \begin{pmatrix} 1 & w_i & 0 & 0 \\ 0 & 0 & 1 & w_i \\ r_1 & w_i \cdot r_2 & \alpha \cdot r_1 & \alpha \cdot w_i \cdot r_2 \\ r_{i1}' & w_i \cdot r_{i2}' & \alpha' \cdot r_{i1}' & \alpha' \cdot w_i \cdot r_{i2}' \end{pmatrix} = w_i^2 (r_2 - r_1)(r_{i2}' - r_{i1}')(\alpha - \alpha') \neq 0 \bmod q_i .$$

This shows that the distribution of the hidden bit σ is independent of A's view except that two events happen: a collision of hash function $H(\cdot)$ occurs, or a decryption oracle accepts an invalid ciphertext. Suppose the first occurs with the probability ε. We have

$$\begin{aligned} \Pr[\mathbf{Exp}_{I,g_1}^{ddh-rand}(B)=1] &\leq 1/2 + \varepsilon + \sum_{i=1}^{n} \sum_{j=1}^{q_{d_i}} 1/(q_i - q_j + 1) \\ &\leq 1/2 + \varepsilon + n \cdot q_d / q \end{aligned} \tag{18}$$

where $q_d \leq q/2$.

Subtracting Equations (11) and (18), we get

$$Adv_{FBE,I}^{cca2}(A) \leq 2 Adv_{I,g_1}^{ddh}(B) + 2\varepsilon + 4n \cdot q_d / q \tag{19}$$

For a general case, when the encryption oracles are queried q_e, by using the hybrid argument, we have

$$Adv_{FBE,I}^{cca2}(A) \leq 2q_e \cdot Adv_{I,g_1}^{ddh}(B) + 2q_e \cdot \varepsilon + 4q_e \cdot n \cdot q_d / q \tag{20}$$

Thus, we have completed the proof of the theorem.

6 Conclusions

We formalize the model of a fully public key broadcast encryption scheme in which each user can choose its private decryption key without others learning the key. We propose a fully public key tracing and revocation scheme provably adaptive secure against the chosen cipher-text attack assuming that the DDH problem is hard. In our scheme, the system can be dynamically updated by the broadcaster without any involvement of any other users. Our updating algorithm is simple and efficient. The tracing algorithm is fully n-resilient and can capture all and only traitors.

Acknowledgement The authors are most grateful to the anonymous referees for pointing out some errors in the earlier version of the paper and providing some methods to correct them. The authors wish to thank Yuh-Dauh Lyuu and Ming-Luen Wu for their helpful discussions about this work.

References:

[1] Fiat A, Naor M. Broadcast encryption. In: Stinson DR, ed. Advances in Cryptology-CRYPT0'93. LNCS 773, Berlin, Heidelberg: Springer-Verlag, 1994. 480–491.

[2] Graray JA, Staddon J, Wool A. Longlived broadcast encryption. In: Bellare M, ed. Advances in Cryptology-CRYPTO 2000. LNCS 1880, Berlin, Heidelberg: Springer-Verlag, 2000. 333−352.

[3] Luby M, Staddon J. Combinatorial bounds for broadcast encryption. In: Nyberg K, ed. Advances in Cryptology-EUROCRYPT'98. LNCS 1403, Berlin, Heidelberg: Springer-Verlag, 1998. 512−526.

[4] Blundo C, Cresti A. Space requirements for broadcast encryption. In: De Santis A, ed. Advances in Cryptology-EUROCRYPT'94. LNCS 950, Berlin, Heidelberg: Springer-Verlag, 1995. 287−298.

[5] Blundo C, Mattos LAF, Stinson DR. Trade-Offs between communication and storage in unconditionally secure scheme for broadcast encryption and interactive key distribution. In: Koblitz N, ed. Advances in Cryptology-CRYPTO'96. LNCS 1109, Berlin, Heidelberg: Springer-Verlag, 1996. 387−400.

[6] Gafni E, Staddon J, Yin YL. Efficient methods for integrating traceability and broadcast encryption. In: Wiener M, ed. Advances in Cryptology-CRYPTO'99. LNCS 1606, Berlin, Heidelberg: Springer-Verlag, 1999. 372−387.

[7] Kurosawa K, Yoshida T, Desmedt Y, Burmester M. Some bounds and a construction for secure broadcast encryption. In: Ohta K, Pei D, eds. ASIACRYPT'98. LNCS 1514, Berlin, Heidelberg: Springer-Verlag, 1998. 420−433.

[8] Halevi D, Shamir A. The LSD broadcast encryption scheme. In: Yung M, ed. Advances in Cryptology-CRYPTO 2002. LNCS 2442, Berlin, Heidelberg: Springer-Verlag, 2002. 47−60.

[9] Naor D, Naor M, Lotspiech J. Revocation and tracing schemes for stateless receivers. In: Kilian J, ed. Advances in Cryptology-CRYPTO'2001. LNCS 2139, Berlin, Heidelberg: Springer-Verlag, 2001. 41−62.

[10] Nao M, Pinkas B. Efficient trace and revoke schemes. In: Frankel Y, ed. Financial Cryptography FC'2000, LNCS 1962, Berlin, Heidelberg: Springer-Verlag, 2000. 1−20.

[11] Anzai J, Matsuzaki N, Matsumoto T. A quick group key distribution scheme with entity revocation. In: Lam KY, Okamoto E, Xing C, eds. Advances in Cryptology-Asiacrypt'99. LNCS 1716, Berlin, Heidelberg: Springer-Verlag, 1999. 333−347.

[12] Dodis Y, Fazio N. Public key broadcast encryption secure against adaptive chosen ciphertext attack. In: Desmedt YG, ed. Proc. of the PKC'03. LNCS 2567, 2003. 100−115.

[13] Chor B, Fiat A, Naor M. Tracing traitors. In: Desmedt YG, ed. Advances in Cryptology-CRYPTO'94. LNCS 839, Berlin Heidelberg: Springer -Verlag, 1994. 257−270.

[14] Kiayias A, Yung M. Self protecting pirates and black-box traitor tracing. In: Kilian J, ed. Advances in Cryptology-CRYPTO 2001. LNCS 2139, Berlin, Heidelberg: Springer-Verlag, 2001. 63−79.

[15] Stinson DR, Wei R. Key preassigned traceability schemes for broadcast encryption. In: Tavares S, Meijer J, eds. Proc. of the 5th Annual Workshop on Selected Areas in Cryptography. LNCS 1556, Berlin, Heidelberg: Springer-Verlag, 1999. 144−156.

[16] Boneh D, Franklin M. An efficient public traitor tracing scheme. In: Wiener M, ed. Advances in Cryptology-CRYPTO'99. LNCS 1666, Berlin, Heidelberg: Springer-Verlag, 1999. 338−353.

[17] Kuroisawa K, Desmedt Y. Optimum traitor tracing and asymmetric schemes. In: Nyberg K, ed. Advances in Cryptology-EUROCRYPT'98. LNCS 1403, Berlin, Heidelberg: Springer-Verlag, 1998. 145−157.

[18] Tzeng WG. A public key traitor tracing scheme with revocation using dynamic schemes. In: Kim K, ed. PKC 2001. LNCS 1992, Berlin, Heidelberg: Springer-Verlag, 2001. 207−224.

[19] Lyuu YD, Wu ML. A fully public key traitor tracing scheme. WSEA Trans. on Circuits 1, 2002,(1):88−93.

[20] Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. In: Krawczyk H, ed. Advances in Cryptology-CRYPTO'98. LNCS 1460, Berlin, Heidelberg: Springer-Verlag, 1998. 13−25.

[21] Bellare M, Boldyreva A, Micali S. Public key encryption in a multi-user setting: security proofs and improvements. In: Preneel B, ed. Advances in Cryptology-EUROCRYPT 2000. LNCS 1807, Berlin, Heidelberg: Springer-Verlag, 2000. 259−274.