

Pairing-Based Multi-Recipient Public Key Encryption

Li Lu Lei Hu

State Key Laboratory of Information Security
Graduate School of Chinese Academy of Sciences
Beijing 100049, PR China
{luli,hu}@is.ac.cn

Abstract

The growth of the Internet has triggered tremendous opportunities for broadcast service. However, the security issue of the broadcast has not been properly addressed. In this paper, we propose a new multi-recipient public key encryption scheme called "Pairing-Based Multi-Recipient Encryption" (PBMRE) to achieve a secure broadcast transmission. In PBMRE, a ciphertext encrypted by an encryption key can be decrypted by a number of decryption keys. Therefore, PBMRE can be applied to broadcast sensitive information in a unsafe distributed environment. The proposed scheme is novelly constructed on weil pairing on elliptic curve and the Shamir's secrets sharing scheme [2]. We also proved that the security strength of our scheme is relative to "Gap Bilinear Diffie-Hellman Assumption" (Gap-BDH), which is extremely difficult to compromise.

Keywords: Multi-Recipient, Pairing, Public Key Encryption, Gap-BDH

1 Introduction

The proliferation of the Internet has motivated tremendous approaches for broadcast transmissions. An example of these approaches is pay TV service, which occurs between multiple customers and a centralized company. An overt issue in this scenario is that the company wants to provide the service to only authorized users. On the other hand, users may never be willing to expose the content they retrieve from the company. The problem is known as how to conduct secure and trusted broadcast transmission. To address this problem, most traditional cryptographic schemes are implemented as follows. Assume that there are n receivers, numbered $1, \dots, n$, and each of them has a pair of private and public keys, (sk_i, pk_i) . A sender encrypts a plaintext M_i to a receiver i using pk_i for $i = 1, \dots, n$ and sends C_1, \dots, C_n as ciphertexts. Upon the ciphertexts, the

receiver i extracts C_i and decrypts it using its private key sk_i . Such a public key encryption is called "multi-recipient public key encryption" in the literature [5, 6, 10].

There is a natural construction of a broadcast encryption scheme derived from the multi-recipient public key encryption. That is, a single message M is encrypted n times using different public key pk_i for $i = 1, \dots, n$ and the ciphertexts (C_1, \dots, C_n) are sent to receivers, respectively [4, 5]. However, such a scheme needs at least n encryption operations for delivering each M , which is overtly inefficient.

In this paper, we present a novel multi-recipient public key encryption scheme based on weil pairing, called "Pairing Based Multi-Recipient Encryption" (PBMRE). The key idea of PBMRE is that we split a single decrypting key into a number of private key subsets, each for an individual decrypter. We use Shamir's secret sharing [2] to achieve this key distribution. Different decrypters have their decryption key components.

We prove our scheme is semantically secure (IND-CPA, [14]) in a standard model assuming that the Bilinear Decisional Diffie-Hellman problem (BDDH) is intractable. We also enhance PBMRE to a slightly modified variant which is equipped with IND-CCA security [14], under the random oracle model assuming the Gap Bilinear Diffie-Hellman problem (Gap-BDH) is computational infeasible [15]. Our schemes are also resistant to colluding attacks. Even all decrypters collude, they can not combine their decryption components to recover the master key.

RELATED WORK. The concept of multi-recipient public key encryption was proposed by Bellare, Boldyreva, and Micali [5], and Baudron, Pointcheval, and Stern [4]. Their results state that the security of public key encryption in the single-recipient setting implies the security in the multi-recipient setting. Therefore, a semantically secure multi-recipient public key encryption scheme can be constructed by simply encrypting a plaintext using n different public keys in a semantically secure single-recipient public key

encryption scheme. Later, a technique called Randomness Re-use was proposed by Kurosawa [10] to improve the efficiency and save the bandwidth via an ElGamal [9] based multi-recipient public key encryption scheme. Bellare, Boldyreva and Pointcheval refined Kurosawa's work [6] and proposed a general test method to determine whether or not a single-recipient public key encryption scheme is proper to construct an efficient multi-recipient encryption scheme with the randomness re-use technique.

In 2001, Boneh and Franklin constructed an practical identity-based encryption scheme taking advantage of the weil pairing [7]. Later, several identity-based multi-recipient encryption schemes were proposed. Chen, Harrison, Soldera, and Smart [8] and Smart [12] gave an identity-based multi-recipient public key encryption scheme established from Boneh and Franklin's IBE scheme. However, one drawback of this work [8], [12] is that their schemes are not supported by appropriate formal security model and proofs. Some outstanding schemes with formal secure proofs were proposed by Mu, Susilo, and Lin [21], and Baek, Safavi-Naini and Susilo [1].

ORGANIZATIONS. The rest of this paper is organized as follows. Section 2 gives preliminaries on complexity assumptions and Lagrange interpolation. Section 3 describes the schemes, and Section 4 discusses their efficiency. In section 5 we present security proofs. Section 5 is the conclusion.

2 Preliminaries

The following computational problem and complexity assumption are used in the security analysis of our schemes.

Definition 1 [Bilinear Decisional Diffie-Hellman (BDDH) Assumption] Let \mathbb{G}_1 and \mathbb{G}_2 be two groups of prime order p , and with addition and multiplication as group operations, respectively. Let P be a generator of \mathbb{G}_1 .

Assume $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is a bilinear map, namely $e(aQ, bR) = e(Q, R)^{ab}$ holds for any $Q, R \in \mathbb{G}_1$ and for any $a, b \in \mathbb{Z}_p$, and $e(P, P) \neq 1$ (see [7]). Suppose a challenger chooses $a, b, c, z \in \mathbb{Z}_p$ at random. If there exists no polynomial-time adversary who can distinguish the 4-tuple $(aP, bP, cP, e(P, P)^{abc})$ from the tuple $(aP, bP, cP, e(P, P)^z)$ with a non-negligible advantage, then the BDDH assumption holds for $(\mathbb{G}_1, \mathbb{G}_2, e)$.

Definition 2 [Gap-BDH Problem] Let $\mathbb{G}_1, \mathbb{G}_2$ and e be as in Definition 1. The Gap-BDH problem is that given (P, aP, bP, cP) , compute $e(P, P)^{abc}$ with the help of the Bilinear Decisional Diffie-Hellman (BDDH) oracle, which, given (P, aP, bP, cP, κ) , outputs 1 if $\kappa = e(P, P)^{abc}$ and 0 otherwise.

Let \mathcal{A} be an attacker. \mathcal{A} 's advantage to solve the Gap-BDH problem is defined as

$$\text{Adv}_{\mathcal{A}}^{\text{Gap-BDH}} = \Pr[\mathcal{A}^{\text{OBDDH}}(P, aP, bP, cP) = e(P, P)^{abc}].$$

\mathcal{A} is a (t, q_o, ε) -solver to the Gap-BDH problem if the advantage of \mathcal{A} is not less than ε when \mathcal{A} makes q_o BDDH-oracle queries and \mathcal{A} run its attack within time t . The Gap-BDDH problem is (t, q_o, ε) -intractable if there is no (t, q_o, ε) -solver to the Gap-BDH problem.

Another tool used in our schemes is Shamir's secret sharing. It is a mechanism to distribute shares of a master secret to several participants, and some of the participants can use their shares to recover the master secret. Let Γ be a finite subset of \mathbb{Z}_p^* , where p is a prime. The Lagrange interpolation polynomial $\Delta_{i, \Gamma}$ for $i \in \Gamma$ is

$$\Delta_{i, \Gamma}(x) = \prod_{j \in \Gamma, j \neq i} \frac{x - j}{i - j}.$$

Let $|\Gamma| = m$. A polynomial $q(x) \in \mathbb{Z}_p[x]$ of degree $m - 1$ can be expressed as

$$q(x) = \sum_{i \in \Gamma} q(i) \Delta_{i, \Gamma}(x).$$

Obviously, $q(0) = \sum_{i \in \Gamma} q(i) \Delta_{i, \Gamma}(0)$. In our schemes, we will let $q(0)$ denote the master secret.

3 Schemes

We first propose an IND-CPA secure scheme PBMRE-CPA, then employ the technique used in [11] to extend it to an IND-CCA secure scheme PBMRE-CCA.

(1) PBMRE-CPA

Key Generation: Select two groups \mathbb{G}_1 and \mathbb{G}_2 of prime order p , such that there exists an admissible bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ and the Computational Diffie-Hellman problem on \mathbb{G}_1 is intractable [7]. Let P be a generator of \mathbb{G}_1 . Choose two elements $Q, R \in \mathbb{G}_1$ at random.

Assume E is the message encrypter (sender) and there exist d message decrypters (receivers), D_1, D_2, \dots, D_d . Let a and b be two positive integers. Select $a + bd$ pairwise different elements in \mathbb{Z}_p randomly, $t_{0,1}, \dots, t_{0,a}, t_{1,1}, \dots, t_{1,b}, \dots, t_{d,1}, \dots, t_{d,b}$, and let

$$EC = \{t_{0,1}, \dots, t_{0,a}\}, \quad DC_j = \{t_{j,1}, \dots, t_{j,b}\}.$$

Let $m = a + b$. An element $s \in \mathbb{Z}_p$ is picked randomly as the master secret. Select at random a polynomial $q(x) \in \mathbb{Z}_p[x]$ of degree $m - 1$ and with constant term s , namely $q(0) = s$. Compute

$$EK = \{q(t_{0,1})P, \dots, q(t_{0,a})P\}$$

$$DK_j = \{q(t_{j,1})(R + Q), \dots, q(t_{j,b})(R + Q)\}.$$

Finally compute $P_0 = sP$ and output the common parameter $(p, \mathbb{G}_1, \mathbb{G}_2, e, P, Q, R, P_0, EC)$. Receiver D_j keeps DC_j secretly.

Encryption: Choose $r \in \mathbb{Z}_p^*$ uniformly at random and compute the ciphertext

$$(U, V, W, X) = (rP, rQ, e(P_0, R)^r \cdot M, r \cdot EK),$$

where $r \cdot EK = \{rq(t_{0,1})P, \dots, rq(t_{0,a})P\}$.

Decryption: For every receiver D_j , he knows $\Gamma = EC \cup DC_j$, and from it he computes $\Delta_{i,\Gamma}(0)$ for each $i \in \Gamma$. Then D_j computes

$$M_1 = \prod_{i=1}^a e(R + Q, rq(t_{0,i})P)^{\Delta_{t_{0,i},\Gamma}(0)},$$

$$M_2 = \prod_{k=1}^b e(q(t_{j,k})(R + Q), U)^{\Delta_{t_{j,k},\Gamma}(0)}$$

$$M = \frac{e(V, P_0) \cdot W}{M_1 \cdot M_2}$$

By the bilinearity of e and Lagrange interpolation, it is easy to check that this quantity is equal to

$$\begin{aligned} W \cdot \frac{e(V, P_0)}{e(R + Q, sP)^r} &= W \cdot \frac{e(Q, P_0)^r}{e(R, P_0)^r \cdot e(Q, P_0)^r} \\ &= W \cdot \frac{1}{e(R, P_0)^r} \\ &= e(R, P_0)^r \cdot M \cdot \frac{1}{e(R, P_0)^r} \\ &= M. \end{aligned}$$

(II) PBMRE-CCA

Key Generation: Same as in the PBMRE-CPA. In addition, we select two hash functions $H_1 : \mathbb{G}_2 \rightarrow \{0, 1\}^{l_1}$ and $H_2 : \{0, 1\}^* \rightarrow \{0, 1\}^{l_2}$. The common parameter is

$$(p, \mathbb{G}_1, \mathbb{G}_2, e, P, Q, R, P_0, EC, H_1, H_2)$$

Encryption: Choose $S \in \mathbb{G}_2$ and $r \in \mathbb{Z}_p^*$ at random respectively. Compute

$$\begin{aligned} C &= (U, V, W_1, W_2, \sigma, X) \\ &= (rP, rQ, e(P_0, R)^r \cdot S, M \oplus H_1(S), \\ &\quad H_2(S, M, U, V, W_1, W_2), r \cdot EK) \end{aligned}$$

Decryption: From $\Gamma = EC \cup DC_j$, D_j computes $\Delta_{i,\Gamma}(0)$ for each $i \in \Gamma$. Parsing the ciphertext into $(U, V, W_1, W_2, \sigma, X)$, D_j computes

$$S'_1 = \prod_{i=1}^a e(R + Q, rq(t_{0,i})P)^{\Delta_{t_{0,i},\Gamma}(0)}$$

$$S'_2 = \prod_{k=1}^b e(q(t_{j,k})(R + Q), U)^{\Delta_{t_{j,k},\Gamma}(0)}$$

$$S' = \frac{e(V, P_0) \cdot W_1}{S'_1 \cdot S'_2}$$

$$M' = W_2 \oplus H_1(S')$$

$$\sigma' = H_2(S', M', U, V, W_1, W_2)$$

Checks whether $\sigma' = \sigma$. If it holds, return M' , otherwise output "Reject".

4 Discussions

KEY GENERATION: As mentioned above, the degree $m - 1$ polynomial $q(x) \in \mathbb{Z}_p[x]$ is used to hide the master secret s in $a + bd$ shares. According to the secret sharing, we can recover the master secret from m of $a + bd$ shares, but from less than m shares. Naturally, any decrypter D_j can not recover s since $b < m$. Further, letting $bd < m$, we can make even all colluding decrypters can not recover the master secret.

From $bd < m$ and $a + b = m$, we get $a > b(d - 1)$. If $b = 1$, then $a = d = m - 1$ is a minimal number of shares the encrypter shall keep. We can build a valid scheme for any other parameters (a, b, d) with $b > 1$ and $a > b(d - 1)$, however, the efficiency will degrade.

COMPUTATIONAL EFFICIENCY: To encrypt a plaintext M , our scheme needs one pairing computation (none if $e(P_0, R)$ is precomputed), $a + 2$ scalar multiplications with elements from \mathbb{G}_1 to compute $rP, rQ, rq(t_{0,1})P, \dots, rq(t_{0,a})P$, and 1 exponentiation in group \mathbb{G}_2 to compute $e(P_0, R)^r$.

For decryption, it looks like the cost will be dominated by $m = a + b$ pairing computations. But, we can decrypt as follows:

Let

$$M_1 = e(R + Q, \sum_{i=1}^a \Delta_{t_{0,i},\Gamma}(0) \cdot rq(t_{0,i})P)$$

$$M_2 = e(\sum_{k=1}^b \Delta_{t_{j,k},\Gamma}(0) \cdot q(t_{j,k})(R + Q), U)$$

Therefore

$$M = \frac{e(V, P_0) \cdot W}{M_1 \cdot M_2}$$

(We show this for PBMRE-CPA. A similar fact holds for PBMRE-CCA). Hence, the decryption algorithm in our scheme only needs three pairing computations, and $a + b$ scalar multiplications (for $\Delta_{t_{0,i},\Gamma}(0) \cdot rq(t_{0,i})P$, $1 \leq i \leq a$ and $\Delta_{t_{j,k},\Gamma}(0) \cdot q(t_{j,k}) \cdot (R + Q)$, $1 \leq k \leq b$) and three operations in \mathbb{G}_2 (two multiplications and an inversing).

5 Security Analysis

We first prove that the hardness of the BDDH problem (Definition 1) is sufficient for PBMRE-CPA scheme to be IND-CPA secure in the standard model.

Theorem 1: If there exists an IND-CPA adversary \mathcal{A} to break PBMRE-CPA scheme with advantage ε in polynomial time t , we can use \mathcal{A} as a black box to construct an algorithm solving BDDH problem with advantage $\frac{1}{2}\varepsilon$ in time t' , where $t' = O(t)$.

Proof: We use \mathcal{A} to construct an algorithm \mathcal{B} solving the BDDH problem.

Suppose \mathcal{B} is given $(P, \mathbb{G}_1, \mathbb{G}_2, e, aP, bP, cP, Z_0, Z_1)$ as an instance of the BDDH problem, in this tuple, $Z_0 = e(P, P)^{abc}$, and $Z_1 = e(P, P)^z$, where z is uniformly distributed in \mathbb{Z}_p^* . By ε' , we denote \mathcal{B} 's advantage on distinguishing (P, aP, bP, cP, Z_0) and (P, aP, bP, cP, Z_1) . Suppose the running time of \mathcal{B} is t' . \mathcal{B} generates an instance of PBMRE-CPA scheme as follows.

\mathcal{B} selects some proper parameters \hat{a} , \hat{b} , d and m , such that $\hat{b} < m$, $\hat{b}d < m$, and $\hat{a} + \hat{b} = m$. Where d states the number of decipherer.

Phase 1: \mathcal{B} sets $P_0 = aP$ and $R = bP$. Chooses $\beta \in \mathbb{Z}_p^*$ and degree $m - 1$ polynomial $q(x) \in \mathbb{Z}_p[x]$ at random respectively. Besides, \mathcal{B} selects a proper subset of \mathbb{Z}_p^* of size \hat{a} , denoted by EC , at random. Then \mathcal{B} computes $Q = \beta P$. Output $(p, Q, R, P, P_0, \mathbb{G}_1, \mathbb{G}_2, e, EC)$ to \mathcal{A} .

Challenge Phase: On receiving two messages M_0 and M_1 with same length from \mathcal{A} , \mathcal{B} creates a target ciphertext C^* :

- Choose $u, v \in \{0, 1\}$ at random respectively.
- Return $C^* = (cP, \beta cP, Z_v \cdot M_u, \{q(i) \cdot cP | i \in EC\})$.

For Z_v , if $v = 0$, C^* encrypts M_u , since $Z_v \cdot M_b = e(P, P)^{abc} \cdot M_b = e(aP, bP)^c \cdot M_b = e(P_0, R)^r \cdot M_u$. If $v = 1$, $Z_v \cdot M_u = e(P, P)^z \cdot M_u$. Due to the randomness of z , \mathcal{A} cannot earn any information about u .

Guess: On receiving \mathcal{A} 's guess u' , \mathcal{B} outputs (P, aP, bP, cP, Z_v) if $u' = u$, otherwise output

$$(P, aP, bP, cP, Z_{1-v})$$

We analyze the advantage of \mathcal{B} . If $v = 1$, the adversary \mathcal{A} cannot get any information about u . So $\Pr[u' = u | v = 1] = \Pr[u' \neq u | v = 1] = \frac{1}{2}$, and the probability of \mathcal{B} guessing the BDDH tuple correctly is $\Pr[\mathcal{B} \text{ success} | v = 1] = \frac{1}{2}$.

Otherwise if $v = 0$, \mathcal{B} returns the valid ciphertext of M_u . As the notation in theorem, the advantage of \mathcal{A} breaking PBMRE-CPA is ε . Hence, $\Pr[u' = u | v = 0] = \frac{1}{2} + \varepsilon$, and

the probability of \mathcal{B} guessing the BDDH tuple successfully is $\Pr[\mathcal{B} \text{ success} | v = 0] = \frac{1}{2} + \varepsilon$.

In summary, the advantage of \mathcal{B} distinguishing the BDDH tuple is

$$\begin{aligned} \Pr[\mathcal{B} \text{ success}] - \frac{1}{2} &= \Pr[\mathcal{B} \text{ success} \wedge v = 0] \\ &+ \Pr[\mathcal{B} \text{ success} \wedge v = 1] - \frac{1}{2} \\ &= \frac{1}{2} \cdot \Pr[\mathcal{B} \text{ success} | v = 0] \\ &+ \frac{1}{2} \cdot \Pr[\mathcal{B} \text{ success} | v = 1] - \frac{1}{2} \\ &= \frac{1}{2} \cdot \left(\frac{1}{2} + \varepsilon\right) + \frac{1}{2} \cdot \frac{1}{2} - \frac{1}{2} \\ &= \frac{1}{2}\varepsilon \end{aligned}$$

□

We prove that the hardness of the Gap-BDH problem is sufficient for the PBMRE-CCA scheme to be IND-CCA secure in the random oracle model.

Theorem 2: Suppose there exists an IND-CCA adversary \mathcal{A} to break the PBMRE-CCA scheme with advantage ε within polynomial time t . Let \mathcal{A} make at most q_{H_1} , q_{H_2} and q_d queries to H_1 , H_2 and decryption oracle respectively. We can use \mathcal{A} as a subroutine to construct an algorithm \mathcal{B} solving Gap-BDH problem with advantage ε' in polynomial time t' . Where $t' = O(t)$, and $\varepsilon' \geq \frac{1}{q_{H_2}}(\varepsilon - \frac{q_d}{2^{l_2}})(1 - \frac{q_{H_1}}{2^{l_1}} - \frac{q_{H_2}}{2^{l_2}})$. Let l_1 and l_2 be the length of hash value of H_1 and H_2 respectively.

Proof: In [11], a security notion for public key encryption called "Oneway-ness under Plaintext Checking Attack (OW-PCA)" is defined. Informally, a public key encryption scheme is (t', q_o, ε') -OW-PCA secure if for any t' -time attacker \mathcal{B} making q_o queries to the *Plaintext Checking (PC) oracle*, which, given a ciphertext-plaintext message pair (C, M) , outputs 1 if C encrypts M and 0 otherwise, \mathcal{B} 's probability of finding a pre-image of a given ciphertext is less than ε' .

It is easy to find that the PBMRE-CPA is OW-PCA secure assuming that the Gap-BDH problem is intractable: Taking a common parameter (P, R, P_0) , a ciphertext $(U, V, W, r \cdot EK)$, and a certain plaintext M' as input, the PC oracle checks whether $(P, U, R, P_0, W/M')$ is a Bilinear Diffie-Hellman tuple. Hence, the running time and advantage of the OW-PCA attacker is exactly the same as the Gap-BDH attacker.

Assume that an IND-CCA adversary \mathcal{A} breaks the PBMRE-CCA scheme with advantage greater than ε within

time t , and makes at most q_{H_1} , q_{H_2} and q_d random oracle and decryption queries respectively. We can construct an OW-PCA attacker \mathcal{B} for the PBMRE-CPA scheme.

Suppose that \mathcal{B} is given $(p, Q, P, P_0, R, \mathbb{G}_1, \mathbb{G}_2, e, EC)$ and

$$(U^*, V^*, W^*, X^*) = (r^*P, r^*Q, e(P_0, R)^{r^*} \cdot S^*, r^* \cdot EK)$$

as a target ciphertext of the PBMRE-CPA scheme, and makes at most q_o queries to the PC oracle of the PBMRE-CPA scheme within time t' . We denote \mathcal{B} 's winning probability by ε' , \mathcal{B} plays an IND-CCA game with \mathcal{A} as follows.

Phase 1: \mathcal{B} gives \mathcal{A}

$$(p, P, Q, P_0, R, \mathbb{G}_1, \mathbb{G}_2, e, EC, H_1, H_2)$$

as the common parameter. Where the H_1 and H_2 are the random oracles controlled by \mathcal{B} as below.

H_1 : On receiving a query S_j for a query $j \in [1, q_{H_1}]$:

- If (S_j, K_j) exists in the H_1 list, return K_j .
- Else check whether (U^*, V^*, W^*, X^*) encrypts S_j using the PC oracle.
 - * If it holds, return S_j and terminate the game (i.e. \mathcal{B} has found the pre-image of $(r^*P, r^*Q, e(P_0, R)^{r^*} S^*, r^* \cdot EK)$).
 - * Otherwise, do:
 - ★ Choose $K_j \in \{0, 1\}^{l_1}$ uniformly at random.
 - ★ Put (S_j, K_j) into the H_1 list and return K_j .

H_2 : On receiving a query $(S_j, M_j, U_j, V_j, W_{j1}, W_{j2})$ for some query $j \in [1, q_{H_2}]$:

- If $((S_j, M_j, U_j, V_j, W_{j1}, W_{j2}), \sigma_j)$ exists in H_2 list, return σ_j .
- Else check whether $(r^*P, r^*Q, e(P_0, R)^{r^*} S^*, r^* \cdot EK)$ encrypts S_j using PC oracle.
 - * If it holds, return S_j and terminate the game (i.e. \mathcal{B} has found the pre-image of $(r^*P, r^*Q, e(P_0, R)^{r^*} S^*, r^* \cdot EK)$).
 - * Otherwise:
 - ★ Choose $\sigma_j \in \{0, 1\}^{l_2}$ uniformly at random.
 - ★ Put $((S_j, M_j, U_j, V_j, W_{j1}, W_{j2}), \sigma_j)$ into the H_2 list and return σ_j .

Phase 2: \mathcal{B} answers \mathcal{A} 's decryption queries as follows.

On receiving a decryption query C_j for some $j \in [1, q_d]$. Where $C_j = (U_j, V_j, W_{j1}, W_{j2}, r_j \cdot EK, \sigma_j)$:

- If $((S_j, M_j, U_j, V_j, W_{j1}, W_{j2}), \sigma_j)$ exists in H_2 list:
 - * Compute the $H_1(S_j)$ using the H_1 oracle and check whether $H_1(S_j) \oplus M_j = W_{j2}$.
 - ★ If not, return "Reject".
 - ★ Otherwise, check whether $(U_j, V_j, W_{j1}, r_j \cdot EK)$ encrypts S_j using the PC oracle.
 - If it holds, return M_j .
 - output "Reject" otherwise.
- Otherwise return "Reject".

Phase 3 Challenge: \mathcal{B} uses the target ciphertext

$$(U^*, V^*, W^*, r^* \cdot EK) = (r^*P, r^*Q, e(P_0, R)^{r^*} S^*, r^* \cdot EK)$$

of PBMRE-CPA to create a target ciphertext C^*

Upon receiving (M_0, M_1) :

- Choose $b \in \{0, 1\}$ at random.
- Choose $K^* \in \{0, 1\}^{l_1}$ uniformly at random and set $H_1(S^*) = K^*$.
- Choose $\sigma^* \in \{0, 1\}^{l_2}$ uniformly at random and set $H_2(S^*, M_b, U^*, V^*, W_{j1}^*, W_{j2}^*) = \sigma^*$.
- Return $C^* = (U^*, V^*, W_{j1}^*, K^* \oplus M_b, \sigma^*, r^* \cdot EK)$ as a target ciphertext.

Phase 4: \mathcal{B} answers \mathcal{A} 's queries as in Phase 1 and 2.

Phase 5 Guess: On receiving \mathcal{A} 's output b' , \mathcal{B} outputs a S chosen uniformly at random from H_2 list, if $b' = b$, otherwise \perp .

The simulation of the decryption oracle is nearly perfect, except that a valid ciphertext is rejected since the adversary \mathcal{A} has guessed a right value for the output of H_2 without querying it. It happens with probability $1/2^{l_2}$.

Following the simulation of \mathcal{A} 's challenger, \mathcal{B} will give a correct result which decrypts $(r^*P, r^*Q, e(P_0, R)^{r^*} S^*, r^* \cdot EK)$ in the following cases.

1. When \mathcal{A} query H_1 with a S_j , \mathcal{B} finds that $(r^*P, r^*Q, e(P_0, R)^{r^*} S^*, r^* \cdot EK)$ encrypts S_j . This case happens with probability $\frac{q_{H_1}}{2^{l_1}}$.
2. When \mathcal{A} query H_2 with a $(S_j, M_j, U_j, V_j, W_{j1}, W_{j2})$, \mathcal{B} finds that $(r^*P, r^*Q, e(P_0, R)^{r^*} S^*, r^* \cdot EK)$ encrypts S_j . This case happens with probability $\frac{q_{H_2}}{2^{l_2}}$.
3. At the end of \mathcal{A} 's attack, if \mathcal{A} didn't correctly guess the output of H_2 without querying it, \mathcal{B} picks a random tuple in H_2 list. We denote $Guess_{H_2}$ as the event that \mathcal{A} correctly guessing the output of H_2 .

We denote E_1 , E_2 and E_3 as the events listed above respectively. Then

$$\begin{aligned}
\Pr[\mathcal{B} \text{ success}] &= \Pr[E_1]\Pr[\mathcal{B} \text{ success}|E_1] \\
&+ \Pr[E_2]\Pr[\mathcal{B} \text{ success}|E_2] \\
&+ \Pr[E_3]\Pr[\mathcal{B} \text{ success}|E_3] \\
&\geq (1 - \Pr[E_1] - \Pr[E_2]) \cdot \\
&\quad \Pr[\mathcal{B} \text{ success}|E_3] \\
&\geq \frac{1}{q_{H_2}} \left(1 - \frac{q_{H_1}}{2^{l_1}} - \frac{q_{H_2}}{2^{l_2}}\right) \cdot \\
&\quad \left(\Pr[b' = b | \neg \text{Guess}H_2] - \frac{1}{2}\right) \\
&\geq \frac{1}{q_{H_2}} \left(1 - \frac{q_{H_1}}{2^{l_1}} - \frac{q_{H_2}}{2^{l_2}}\right) \cdot \\
&\quad \left(\Pr[b' = b] - \Pr[\text{Guess}H_2] - \frac{1}{2}\right)
\end{aligned}$$

Since \mathcal{A} makes at most q_d decryption queries during the whole attack, $\Pr[\text{Guess}H_2] \leq \frac{q_d}{2^{l_2}}$. Thus

$$\Pr[\mathcal{B} \text{ success}] \geq \frac{1}{q_{H_2}} \left(\varepsilon - \frac{q_d}{2^{l_2}}\right) \left(1 - \frac{q_{H_1}}{2^{l_1}} - \frac{q_{H_2}}{2^{l_2}}\right)$$

□

6 Conclusions

In this paper, we proposed pairing based provably secure multi-recipient public key encryption schemes (PBMRE) that can broadcast encrypted data efficiently. We provided a complete security proof for these schemes. In the future work, we will apply this scheme in secure distribution systems, such as an online TV payment and E-auditing.

References

- [1] J. Baek, R. Safavi-Naini, and W. Susilo, *Efficient Multi-receiver Identity-Based Encryption and Its Application to Broadcast Encryption*, PKC 2005, LNCS 3386, pp. 380-397, Springer-Verlag, 2005.
- [2] A. Shamir, *How to Share a Secret*, Communications. ACM, Vol.22, pp.612-613, 1979.
- [3] O. Goldreich, *The Foundations of Cryptography - Volume 2*, Cambridge University Press, 2004.
- [4] O. Baudron, D. Pointcheval, and J. Stern, *Extended Notions of Security for Multicast Public Key Cryptosystems*, ICALP 2000, LNCS 1853, pp. 499-511, Springer-Verlag, 2000.
- [5] M. Bellare, A. Boldyreva, and S. Micali, *Public-key Encryption in a Multi-User Setting: Security Proofs and Improvements*, Eurocrypt 2000, LNCS 1807, pp. 259-274, Springer-Verlag, 2000.
- [6] M. Bellare, A. Boldyreva, and D. Pointcheval, *Multi-Recipient Encryption Schemes: Security Notions and Randomness Re-Use*, PKC 2003, LNCS 2567, pp. 85-99, Springer-Verlag, 2003.
- [7] D. Boneh, and M. Franklin, *Identity-Based Encryption from the Weil Pairing*, Crypto 2001, LNCS 2139, pp. 213-229, Springer-Verlag, 2001.
- [8] L. Chen, K. Harrison, D. Soldera, and N. P. Smart, *Applications of Multiple Trust Authorities in Pairing Based Cryptosystems*, InfraSec 2002, LNCS 2437, pp. 260-275, Springer-Verlag, 2002.
- [9] T. ElGamal, *A Public key Cryptosystem and a Signature Scheme Based on Discrete Logarithms*, IEEE Transactions on Information Theory, Vol. 31, pp. 469-472, IEEE, 1985
- [10] K. Kurosawa, *Multi-Recipient Public-Key Encryption with Shortened Ciphertext*, PKC 2002, LNCS 2274, pp. 48-63, Springer-Verlag, 2001.
- [11] T. Okamoto, and D. Pointcheval, *REACT: Rapid Enhanced-security Asymmetric Cryptosystem Transform*, CT-RSA 2001, LNCS 2020, pp. 159-174, Springer-Verlag, 2001.
- [12] N. P. Smart, *Access Control Using Pairing Based Cryptography*, CT-RSA 2003, LNCS 2612, pp. 111-121, Springer-Verlag, 2003.
- [13] M. Bellare, and P. Rogaway, *Random Oracles are Practical: A Paradigm for Designing Efficient Protocols*, ACM CCCS 1993, pp. 62-73, 1993.
- [14] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, *Relations Among Notions of Security for Public-Key Encryption Schemes*, Crypto 1998, LNCS 1462, pp. 26-45, Springer-Verlag, 1998.
- [15] T. Okamoto and D. Pointcheval, *The Gap-Problems: A New Class of Problems for the Security of Cryptographic Schemes*, PKC 2001, LNCS 1992, pp. 104-118, Springer-Verlag, 2001.
- [16] D. Boneh and X. Boyen, *Efficient Selective-ID Secure Identity Based Encryption Without Random Oracles*, Eurocrypt 2004, LNCS 3027, pp. 223-238, Springer-Verlag, 2004.
- [17] A. Fiat and M. Naor, *Broadcast Encryption*, Crypto 1994, LNCS 773, pp. 480-491, Springer-Verlag, 1994.
- [18] Y. Dodis and N. Fazio, *Public Key Broadcast Encryption for Stateless Receivers*, ACM-DRM, 2002.

- [19] Y. Dodis and N. Fazio, *Public Key Trace and Revoke Scheme Secure against Adaptive Chosen Ciphertext Attacks*, PKC 2003, LNCS 2567, pp. 100-115, Springer-Verlag, 2003.
- [20] D. Naor, M. Naor, and J. Lotspiech, *Revocation and Tracing Schemes for Stateless Receivers*, Crypto 2001, LNCS 2139, pp. 41-62, Springer-Verlag, 2001.
- [21] Y. Mu, W. Susilo, and Y. Lin, *Identity-Based Broadcasting*, Indocrypt 2003, LNCS 2904, pp. 177-190, Springer-Verlag, 2003.
- [22] J. Anzai, N. Matsuzaki, and T. Matsumoto, *A Quick Group Key Distribution Scheme with "Entity Revocation"*, Asiacrypt 1999, LNCS 1716, pp. 333-347, Springer-Verlag, 1999.
- [23] M. Naor and B. Pinkas, *Efficient Trace and Revoke Schemes*, FC 2000, LNCS 1962, pp. 1-20, Springer-Verlag, 2001.
- [24] D. M. Wallner, E. J. Harder, and R. C. Agee, *Key management for multicast: Issues and architectures*, Internet Draft <ftp://ftp.ietf.org/internet-drafts/draft-wallner-key-arch-01.txt>.