Adaptively Anonymous Public-Key Broadcast Encryption Scheme without Random Oracle

Hao Wang\textsuperscript{a,b,c}, Lei Wu\textsuperscript{a,b}

\textsuperscript{a} School of Information Science and Engineering, Shandong Normal University, Jinan 250014, China
\textsuperscript{b} Shandong Provincial Key Laboratory for Novel Distributed Computer Software Technology, Jinan 250014, China
\textsuperscript{c} Shandong Provincial Key Laboratory of Software Engineering, Jinan 250101, China

Email: whatsdnu@gmail.com

Abstract—Anonymous is one of the most important security properties for kinds of Internet applications. In this paper, we consider the privacy-preserving problem in the context of public key broadcast encryption. We provide a new security definition for anonymous public key broadcast encryption, and construct a new scheme. To achieve anonymity, we blind the ciphertexts using the random factors. Moreover, we use a pair of orthogonal bases to construct secret key and ciphertexts for proper decryption. Our anonymous public-key broadcast encryption scheme can be proven in the adaptive model without random oracle. The key technique used to obtain our result is an elaborate combination of the dual system encryption proposed by Waters and a new approach on bilinear pairings using the notion of dual pairing vector spaces (DPVS) proposed by Okamoto and Takasima.

Index Terms—public-key broadcast encryption, anonymous, DPVS, dual system encryption, adaptively secure

I. INTRODUCTION

In many scenarios, it is crucial that the distributed content to a (large) set of users is kept private. In a commercial context, a broadcaster is interested in distributing digital content only to the paying customers. Similarly, an online store selling electronic books or digital music and movies wishes to keep the distributed content protected from any user but the proper customer. Companies are interested in distributing confidential information inside the company itself to a particular subset of employees (e.g.: accounting members, top management,...) avoiding people outside the group (or competitors) to learn about the information. To solve this problem, Fiat and Naor formulated the “Broadcast Encryption” problem and provided a first solution in [1]. In broadcast encryption, a sender can efficiently send a ciphertext to the set of receivers \( S \) that is arbitrary chosen by the sender, and a receiver can decrypt the ciphertext if he belongs to the set \( S \). A trivial broadcast encryption system with linear size of ciphertexts can be built by using multiple instances of an encryption system. Therefore, a non-trivial broadcast encryption system should have sub-linear size of ciphertexts. Broadcast encryption is classified as public key or symmetric key depends on the type of keys, stateful or stateless depends on the need of private key update, and fully-collusion resistant or \( t \)-collusion resistant depends on the maximum number of collusion users.

A. Related Works

In recent years, a variety of BE systems have been proposed in [2]–[12]. Public-key broadcast encryption (PKBE) is a specific type of broadcast encryption such that anyone can create a ciphertext by using the the public key of broadcast encryption. Boneh et al. proposed the first stateless and fully-collusion resistant PKBE scheme by using the algebraic structure of bilinear groups in [10]. They first propose a simple PKBE scheme with linear size of public keys and constant size of ciphertexts, and then they proposed a generalized PKBE scheme with sub-linear size of public keys and ciphertexts. After the pioneering work of Boneh et al., many other PKBE schemes with different properties were proposed in bilinear groups [13]–[15]. However, these PKBE schemes were proven to be secure in the static security model under \( q \)-type assumptions where the value \( q \) depends on the number of users in the system. The static security model is a weaker security model since the adversary should commit the target set \( S^* \) before he receives the public key.

The right security model of PKBE is the adaptive security model where the adversary adaptively requests private keys for arbitrary chosen indexes and later selects a target subset at the challenge step. Generally, a PKBE scheme in the static security model can be converted to a PKBE scheme in the adaptive security model if a simulator predicts the target set \( S^* \) of the adversary by simply selecting an arbitrary set \( S' \). However, this method has a problem such that the probability of \( S^* = S' \) is less than \( 1/2^N \) where \( N \) is the number of users in the system. To achieve the adaptive security, Gentry and Waters proposed a new method that converts a semi-statically secure PKBE scheme to an adaptively secure one by using the two-key technique in [16]. In the semi-static security model, an adversary first commits an initial set \( S' \), and it outputs the target set \( S^* \) that is a subset of \( S' \) in the challenge step. The adversary of the semi-static security model has more flexibility compared to the static security model. The two-key technique is a method to...
use two keys in private keys and the decryption algorithm success if one of the two keys is given.

B. Motivations and Contributions

While the traditional BE schemes have focused on protecting the broadcast contents from unauthorized users and reducing the length of the ciphertext or private key size, they have not concerned about protecting the identities of users allowed to access the contents. Who can access the contents, however, is often more sensitive than the contents themselves.

Suppose a university provides a document to students with low average grades. To maintain the privacy of the students, the set of authorized users should be kept private, not only from outsiders, but from the students in the group as well. In a commercial context an online seller would prefer to keep its list of customers secret and protect it from competing companies, e.g. to avoid competitors advertising. Digital media providers could be interested in protecting their customers privacy avoiding them to be profiled by the analysis of their purchases. A company, giving a call for tenders would like to keep its list of customers secret to which he wishes to broadcast a message.

C. Organization

In Section 2, we recall some preliminaries. In Section 3, we give the formal definition of ANON-PKBE scheme and its new security definition. We describe the construction of our ANON-PKBE scheme in the Section 4. Then, we prove the security of the scheme in Section 5. Finally, we conclude in Section 6.

II. Preliminaries

A. Dual Pairing Vector Space

Okamoto and Takashima [24] described the definition of dual pairing vector spaces.

Definition 1: “Symmetric bilinear pairing groups” $(q, G, GT, g, e)$ are a tuple of a prime q, cyclic (multiplicative) group $G$ and $GT$ of order q, $g \neq 1 \in G$, and a polynomial-time computable non-degenerate bilinear pairing $e: G \times G \rightarrow GT$ i.e., $e(g^a, g^b) = e(g, g)^{ab}$ and $e(g, g) \neq 1$. Let $G_{bgs}$ be an algorithm that takes input $1^\lambda$ and outputs a description of bilinear pairing group $(q, G, GT, g, e)$ with security parameter $\lambda$.

In this paper, we concentrate on this symmetric version of dual pairing vector spaces constructed by using symmetric bilinear pairing groups given in Definition 1.

Definition 2: “Dual pairing vector spaces (DPVS)” $(q, \mathbb{V}, GT, A, e)$ by a direct product of symmetric pairing groups $(q, G, GT, g, e)$ are a tuple of prime q, N-dimensional vector space $\mathbb{V} := \mathbb{G} \times \cdots \times \mathbb{G}$ over $\mathbb{F}_q$, cyclic group $GT$ of order q, canonical basis $A := \{a_1, \ldots, a_n\}$ of $\mathbb{V}$, where $a_i := (1, \ldots, 1, g, 1, \ldots, 1)$, and pairing $e: G \times G \rightarrow GT$. The pairing is defined by $e(x, y) := \prod_{i=1}^{n} e(g_i, h_i) \in GT$ where $x := (g_1, \ldots, g_n) \in \mathbb{V}$ and $y := (h_1, \ldots, h_n) \in \mathbb{V}$. This is non-degenerate bilinear i.e., $e(x, y) = e(x, y)^{st}$ and if $e(x, y) = 1$ for all $x \in \mathbb{V}$, then $x = 0$. For all i and j, $e(a_i, a_j) = g_i^{\delta_{ij}}$, where $\delta_{ij} = 1$ if $i = j$, and 0 otherwise, and $gt := e(g, g) \neq 1 \in GT$. DPVS generation algorithm $G_{dpvs} takes input 1^\lambda (\lambda \in \mathbb{N})$ and $n \in \mathbb{N}$, and output a description of $paramv := (q, \mathbb{V}, GT, A, e)$ with security parameter $\lambda$ and N-dimensional $\mathbb{V}$. It can be constructed by using $G_{bgs}$.

We describe random dual orthonormal bases generator below, which is used as a subroutine in the proposed PPBE scheme.

$G_{ob}(1^\lambda, n) : paramv := (q, \mathbb{V}, GT, A, e) \leftarrow G_{dpvs}(1^\lambda, n)$,
X := (x_{i,j}) \leftarrow GL(n, \mathbb{F}_q), (\nu_{i,j}) := (X^T)^{-1},
\begin{align*}
b_i := \sum_{j=1}^n x_{i,j},& \quad 
\begin{array}{l}
\mathbb{B} := (b_1, \ldots, b_n),
\mathbb{B}^* := (b_1^*, \ldots, b_n^*),
\end{array}
\end{align*}

B. Assumption

Definition 3: “n-eDDH: n-Extended Decisional Diffie-Hellman Assumption” The n-eDDH problem is to guess \( \beta \in \{0,1\} \), given \( \langle \text{param}_G, g, g^k, g^{\gamma_1}h_1, g^{\gamma_2}h_2 \rangle_{1 \leq i,j \leq n}, \ Y_\beta \rangle \), where \( \mathcal{G}^n_{\text{n-eDDH}}(\lambda) := \langle g, \mathcal{G}, \mathcal{G}, g, e \rangle \leftarrow \mathcal{G}_{\text{BBB}}(\lambda) \) for \( i = 1, \ldots, n, \ Y_0 = g^{\omega}, \ Y_1 \leftarrow \mathcal{G}, \ Y_2 = \langle \text{param}_G, g, g^k, g^{\gamma_1}h_1, g^{\gamma_2}h_2 \rangle_{1 \leq i,j \leq n}, \ Y_3 \rangle \), \( \beta \leftarrow \{0,1\} \). For a probabilistic machine \( \mathcal{C} \), we define the advantage of \( \mathcal{C} \) for the n-eDDH problem as:

\[
\text{Adv}_\mathcal{C}^{n\text{-eDDH}}(\lambda) := \left| \Pr[C(1, \rho) \rightarrow 1] - \Pr[C(1, \rho) \rightarrow 1] \right|
\]

The n-eDDH assumption is: For any polynomial-time adversary \( \mathcal{C} \), the advantage \( \text{Adv}_\mathcal{C}^{n\text{-eDDH}}(\lambda) \) is negligible.

III. NEW DEFINITION OF ANONYMOUS PUBLIC-KEY BROADCAST ENCRYPTION

Similar to the traditional public-key broadcast encryption scheme, an anonymous public-key broadcast encryption scheme consists of probabilistic polynomial-time algorithm \textbf{Setup}, \textbf{KeyGen}, \textbf{Encrypt}, \textbf{Decrypt}. They are given as follows:

\textbf{Setup}(\lambda, n): The \textbf{Setup} algorithm takes as input security parameter \( \lambda \) and the total number of users in this system \( n \) (the users are indexed to \( 1, \ldots, n \)) outputs public key \( PK \) and secret key \( SK \).

\textbf{KeyGen}(i, SK): Takes as input an index \( i \in \{1, \ldots, n\} \) and the secret key \( SK \). It outputs a private key \( sk_i \).

\textbf{Encrypt}(PK, S, M): The \textbf{Encrypt} algorithm takes as input the public key \( PK \), subset \( S \) of all users (\( S \subseteq \{1, \ldots, n\} \)), and plaintext \( M \). It returns ciphertext \( C \).

\textbf{Decrypt}(PK, sk_i, C): The \textbf{Decrypt} algorithm takes as input the public key \( PK \), secret key \( sk_i \), and ciphertext \( C \). It outputs either plaintext \( M \) or the distinguished symbol \( \bot \).

Note that, in the description of \textbf{Decrypt} algorithm, the receiver set \( S \) is no longer as input. This point is the main difference between ANON-PKBE scheme and traditional PKBE scheme.

An ANON-PKBE scheme should have the following correctness property: for all receivers sets \( S \) and plaintext \( M \), for correctly generated \( PK, SK, sk_i \leftarrow \text{KeyGen}(i, SK) \), and \( C \leftarrow \text{Encrypt}(PK, S, M) \), it holds that \( M = \text{Decrypt}(PK, sk_i, C) \), if \( i \in S \). Otherwise, it holds with negligible probability.

\textbf{Definition 4}: An anonymous public-key broadcast encryption scheme is adaptively anonymous and indistinguishable under chosen plaintext attacks (ANON-IND-CPA) if for all probabilistic polynomial-time adversaries \( \mathcal{A} \), the advantage of \( \mathcal{A} \) in the following experiment is negligible in the security parameter:

\textbf{Setup, Setup} algorithm is run to generate keys \( PK \) and \( SK \), and \( PK \) is given to \( \mathcal{A} \).

\textbf{Phase 1 (KeyGen)}. \( \mathcal{A} \) may adaptively corrupt user \( i \in \{1, \ldots, n\} \) in this system. In response, \( \mathcal{A} \) is given the corresponding key \( sk_i \).

\textbf{Challenge}. \( \mathcal{A} \) outputs two challenge plaintexts \( M_0, M_1 \) \((|M_0| = |M_1|)\), and two challenge receivers sets \( S_0, S_1 \subseteq \{1, \ldots, n\} \), subject to the restriction that \( i \notin \{S_0 \cup S_1 \} \) for all corrupted user \( i \) in Phase 1. If there are some Corrupt queries to \( i \in S_0 \cap S_1 \), it should restrict that \( M_0 = M_1 \) additionally. A random bit \( \beta \) is chosen. \( \mathcal{A} \) is given \( C^* \leftarrow \text{Encrypt}(PK, S_\beta, M_\beta) \).

\textbf{Phase 2 (KeyGen)}. \( \mathcal{A} \) may continue adaptively corrupt the user \( i \in \{1, \ldots, n\} \) in this system. If \( M_0 = M_1 \) in the Challenge phase, it should restrict that \( i \notin \{S_0 \cup S_1 \} \) if \( i \notin \{S_0 \cap S_1 \} \), else, it should restrict that \( i \notin \{S_0 \cap S_1 \} \). In response, \( \mathcal{A} \) is given the corresponding key \( sk_i \).

\textbf{Guess}. \( \mathcal{A} \) outputs a bit \( \beta' \), and succeeds if \( \beta' = \beta \).

We define the advantage of \( \mathcal{A} \) as the quantity

\[
\text{Adv}_\mathcal{A}^{\text{ANON-IND-CPA}} := \Pr[\beta' = \beta] - 1/2.
\]

IV. ANONYMOUS PUBLIC-KEY BROADCAST ENCRYPTION SCHEME

In this section, we proposed a new construction of ANON-PKBE, which is inspired by a new functional encryption system proposed in EUROCRYPT 2010 by Lewko et al. [26]. Our new ANON-PKBE scheme uses the notion of dual pairing vector spaces (DPVS) proposed by Okamoto and Takashima [24].

A. Construction

\textbf{Setup}(\lambda, n): \langle \text{param}_G, \mathbb{B}, \mathbb{B}^* \rangle \leftarrow \mathcal{G}_{\text{BBB}}(\lambda, 4n + 3), and sets \( \mathbb{B}^* := (b_1, b^*_2, \ldots, b^*_n, b_{4n+1}^*, b_{4n+2}^*) \), \( \mathbb{B} := (b_1, b_2, \ldots, b_n, b_{4n+1}, b_{4n+2}) \). Then, chooses two collision-resistant hash functions \( h_1, h_2 : \mathbb{Z}_n^* \rightarrow \mathbb{F}_q \), and lets \( PK := (\langle \mathbb{G}, \mathbb{G}, \mathbb{G} \rangle, h_1, h_2, \mathbb{B}^*), \mathbb{S} := (\mathbb{B}, \mathbb{B}^*) \). It returns PK and SK.

\textbf{KeyGen}(i, SK): For all users \( i \in \{1, \ldots, n\} \), \( \sigma_i, \eta_i \leftarrow \mathbb{F}_q^*, \) and sets

\[
\begin{align*}
&sk_i := \sigma_i(h_1(i)b^*_{2i-1} + h_2(i)b^*_{2i}) + b^*_{4n+1} + \eta_i b^*_{4n+2},
&\text{Encrypt}(PK, S, M): \delta_1, \delta_2, \zeta, y_{j,1}, y_{j,2} \leftarrow \mathbb{F}_q, \text{ for } j \in U - S. \text{ For } \forall i \in S, \text{ chooses } x_{i,1}, x_{i,2} \in \mathbb{F}_q, \text{ subject to } (x_{i,1}, x_{i,2}) \cdot (h_1(i), h_2(i)) = 0, \text{ and sets } C_1 := \sum_j \delta_1(x_{i,1}b_{2i-1} + x_{i,2}b_{2i}) + \sum_{j \in U - S} (y_{j,1}b_{2j-1} + y_{j,2}b_{2j}) + \zeta b_{4n+1} + \delta_2 b_{4n+2}.
\end{align*}
\]
C_2 := g_\hat{FK} \cdot M.
It outputs C := (C_1, C_2)

Decrypt(PK, sk, Hdr): M = C_2/e(C_1, sk_i).

B. Correctness

sk_i = \sigma_i(h_1(i)b_{x-1}^* + h_2(i)b_{2}^* + b_{n+1}^* + \eta_i b_{n+2}^*)
= (0, \ldots, 0, \sigma_i h_1(i), \sigma_i h_2(i), 0, \ldots, 0, 1, \eta, 0)_{\mathbb{B}}^*

C_1 = \sum_{i \in S} \delta_i(x_i, b_{2i-1} + x_i b_{2i}) +
\sum_{j \in U - S} (y_{j,i} b_{2i-1} + y_{j,2} b_{2i}) + \zeta \cdot b_{n+1} + \delta_2 b_{n+3}
= (\delta_1 x_1, 1, \delta_1 x_2, \ldots, \delta_1 x_{s,2}, \delta_1 x_{s,1}, y_{s+1,1}, y_{s+1,2}, \ldots,
\sum_{j=1}^{2n} y_{n,1}, y_{n,2}, \ldots, 0, 0, 0, 0, 0, 0)_{\mathbb{B}}

Therefore, e(C_1, sk_i) = g_T^{\delta_i(x_i, h_1(i) + x_i b_{2i}) + \zeta} = g_\hat{FK}^\beta.
So, C_2/e(C_1, sk_i) = M.

V. SECURITY PROOF

Theorem 1: The proposed ANON-PKBE scheme is adaptively anonymous and indistinguishable against chosen plaintext attacks (ANON-IND-CPA) under e-EDDH assumption. For any adversary A, there exist probabilistic machines C_k (k = 0, \ldots, n), whose running times are essentially the same as that of A, such that for any security parameter \lambda,

\text{Adv}_{PKBE, ANON-IND-CPA}^A(\lambda) \leq \text{Adv}_{e-EDDH}^A(\lambda) + n/q

where n is the number of users in this system.

The proof of this theorem is similar to the proof of Theorem 18 in the work of [26]. Firstly, we give two related definitions.

Definition 5: “Problem 1” is to guess \beta \in \{0, 1\}, given (param_{\beta}, \hat{\beta}, \hat{B}, \{e_{i,j}\}_{i=1,\ldots,2n}), for \beta \in \{0, 1\}.

Definition 6: “Problem 2” is to guess \beta \in \{0, 1\}, given (param_{\beta}, \hat{\beta}, \hat{B}, \{e_{i,j}\}_{i=1,\ldots,2n}), for \beta \in \{0, 1\}.

According to the work of [26] (Lemma 20 and Lemma 22), \text{Adv}^{\text{e-EDDH}}(\lambda) = \text{Adv}^{\hat{B}_{\hat{FK}}}_{\hat{FK}}(\lambda).

Proof Outline of Theorem 1: To prove the security, we employ Game 0 (original game) through Game 3. Roughly speaking, the (normal) target ciphertext is changed to a semi-functional ciphertext in Game 1 (or Game 2-0), the secret key of k-th index replied to the adversary is changed to a semi-functional key in Game 2-k (k = 1, \ldots, n), and the (semi-functional) target ciphertext is changed to perfectly randomized key in Game 3, whose advantage is 0. A normal secret key sk_{\text{norm}} is correct form of the secret key of the proposed PPBE scheme, i.e.

\text{sk}_i = \sigma_i(h_1(i)b_{2i-1} + h_2(i)b_{2i} + b_{n+1} + \eta_i b_{n+2})
= (0, \ldots, 0, \sigma_i h_1(i), \sigma_i h_2(i), 0, \ldots, 0, 1, \eta, 0)_{\mathbb{B}}^*

Similarly, a normal ciphertext is (C_{1,\text{norm}}, C_2), where

C_{1,\text{norm}} = \sum_{i \in S} \delta_i(x_i, b_{2i-1} + x_i b_{2i}) +
\sum_{j \in U - S} (y_{j,i} b_{2i-1} + y_{j,2} b_{2i}) + \zeta \cdot b_{n+1} + \delta_2 b_{n+3}
= (\delta_1 x_1, \delta_1 x_2, \ldots, \delta_1 x_{s,1}, \delta_1 x_{s,2}, y_{s+1,1}, y_{s+1,2}, \ldots,
\sum_{j=1}^{2n} y_{n,1}, y_{n,2}, \ldots, 0, 0, 0, 0)_{\mathbb{B}}.
In the following description, we will omit $C_2$, because it is always in the normal form.

Semi-functional key:

$$sk^\text{semi}_i := (0 \ldots 0, \sigma h_1(i), \sigma h_2(i), 0 \ldots 0, \overline{r}, 1, \eta, 0)_{\mathbb{B}}.$$  

Semi-functional ciphertext:

$$C^\text{semi}_i := (\delta x_{i,1}, \delta x_{i,2}, \ldots, \delta x_{i, S}, y_{s+1,1}, y_{s+1,2}, \ldots, y_{n-1, y_{n,2}}, \zeta, 0, \delta_2)_{\mathbb{B}},$$

where $\overline{r}, \overline{s} \in \{0,1\}^n$.

If $i \in S$, i.e., $(x_{i,1}, x_{i,2}) \cdot (h_1(i), h_2(i)) = 0$, then $e(C^\text{norm}_i, sk^\text{norm}_i) = e(C^\text{semi}_i, sk^\text{semi}_i) = \gamma^\overline{r}$, which leads to correct decryption. In contrast, $e(C^\text{norm}_i, sk^\text{semi}_i) = g^\overline{r} \overline{s}$, which is uniformly and independently distributed over $\mathbb{F}_q$ since $\overline{r}, \overline{s} \in \{0,1\}^n$ i.e., leads to random decryption.

To prove that the advantage gap between Game0 and 1 is bounded by the advantage of Problem 1 (to guess $\beta \in \{0,1\}$), we construct a simulator of the challenger of Game 0 (or 1) (against an adversary $A$) by using an instance with $\beta \in \{0,1\}$ of Problem 1. We then show that the distribution of the secret keys and target ciphertexts replied by the simulator is equivalent to those of Game 0 when $\beta = 0$ and Game 1 when $\beta = 1$. That is, the advantage of Problem 1 is equivalent to the advantage gap between Games 0 and 1 (Lemma 1). The advantage of Problem 1 is proven to be equivalent to that of the n-eDDH assumption [26].

The advantage gap between Game 2-(k-1) and 2-k is similarly shown to be bounded by the advantage of Problem 2 (i.e., of the n-eDDH assumption) +1/4 (Lemma 2).

Here, we introduce special form of semi-functional keys and ciphertexts such that

$$sk^\text{speci}_i := (0 \ldots 0, \sigma h_1(i), \sigma h_2(i), 0 \ldots 0, \overline{r}_i, \overline{s}_i, 0)_{\mathbb{B}},$$

where $Z$ is a random regular $(n \times n)$-matrix, $U := (Z^{-1})^T$, and $\tau, \rho \in \mathbb{F}_q$.

$$C^\text{speci}_i := (\delta x_{i,1}, \delta x_{i,2}, \ldots, \delta x_{i, S}, y_{s+1,1}, y_{s+1,2}, \ldots, y_{n,1}, y_{n,2}) U, \zeta, 0, \delta_2)_{\mathbb{B}},$$

where $Z$ is a random regular $(n \times n)$-matrix, $U := (Z^{-1})^T$, and $\tau, \rho \in \mathbb{F}_q$.

$$sk^\text{speci}_i$$ can decrypt $C^\text{speci}_i$ for all $i \in S$, since

$$2i-2 \vdash 2n-2i \vdash \overline{r}_i, \overline{s}_i, 0)_{\mathbb{B}},$$

$$(\rho x_{i,1}, \rho x_{i,2}, \ldots, \rho x_{i, S}, y_{s+1,1}, y_{s+1,2}, \ldots, y_{n,1}, y_{n,2}) U,$$

$$\tau \rho (h_1(i), h_2(i)) \cdot (x_{i,1}, x_{i,2}),$$

i.e., $e(C_i^\text{semi}, sk^\text{semi}_i) = g^\overline{r}$. In addition, when $i \notin S$, $e(C_i^\text{norm}, sk^\text{norm}_i) = g^\overline{r} \overline{s}$, and the joint distribution of $sk^\text{speci}_i$ and $C^\text{speci}_i$ is equivalent to that of an independent pair of $sk^\text{speci}_i$ and $C^\text{speci}_i$ (except with probability $1/4$).

Finally, we show that Game 2-n can be conceptually changed to Game 3 by using the fact that $2n$ elements of $\mathbb{B}$, $(b_{2n+1}, b_2, \ldots, b_{3n})$, are secret to the adversary (Lemma 3).

**Proof of Theorem 1:** To prove Theorem 1, we consider the following (n+3) games.

**Game 0** Original game.

**Game 1** Same as Game 0 except that the target ciphertext $(C_1, C_2)$ for challenge plaintexts $(M_0, M_1)$ and challenge user sets $(S_0, S_1)$ is

$$C_1 := \delta_1 (x_{i,1} b_{2i-1} + x_{i,2} b_{2i}) + \sum_{j \in U-S_B} (y_{j,1} b_{2i-1} + y_{j,2} b_{2i}) + \sum_{i=1}^{2n} w_i b_{2n+i} + C_1 b_{2i+1} + \delta_2 b_{4n+3},$$

$C_2 := g^\overline{r} \cdot M.$

where, for all $j \notin U - S_{\beta}$, $\delta_1, \delta_2, \zeta, y_{j,1}, y_{j,2} \in \mathbb{F}_q$, for all $i \notin S_B$, choose $x_{i,1}, x_{i,2} \in \mathbb{F}_q$, subject to $(x_{i,1}, x_{i,2}) \cdot (h_1(i), h_2(i)) = 0$, $\beta \in \{0,1\}$, and $(w_1, \ldots, w_{2n}) \leftarrow \mathbb{F}_q^{2n} \setminus \{0\}.$

**Game 2-k** (k=1,...,n) Game 2-0 is Game 1. Game 2-k is same as Game 2-1 except the corrupt query reply to the index of $k$ is $sk_k = \sigma (h_1(k) b_{2k-1} + h_2(k) b_{2k}) + \sum_{i=1}^{2n} r_i b_{2n+i} + \zeta b_{2k+1} + \delta_2 b_{4n+3},$ where $\sigma, \eta \in \mathbb{F}_q, r_i \in \{r_1, \ldots, r_{2n}\} \leftarrow \mathbb{F}_q^{2n}$.

**Game 3** Same as Game 2-n except that the target ciphertext $(C_1, C_2)$ for challenge plaintexts $(m_0, m_1)$ and challenge user sets $(S_0, S_1)$ is $C_1 := \sum_{i=1}^{2n} x_{i,1} b_i + \sum_{i=1}^{2n} w_i b_{2n+i} + \zeta b_{4n+1} + \delta_2 b_{4n+3},$ $C_2 := g^\overline{r} \cdot m_i,$ where $x_{i,1}, x_{i,2}, \delta_2, \zeta, \zeta \in \mathbb{F}_q, \beta \in \{0,1\}$, $(w_1, \ldots, w_{2n}) \leftarrow \mathbb{F}_q^{2n} \setminus \{0\}.$

In particular, we note that $\zeta$ and $(x_{i,1}, x_{i,2})$ are chosen uniformly and independently from $\zeta$ and $(x_{i,1}, x_{i,2})$ of Game 0 Game2-n.

Let $Adv^A_{\mathbb{P}}(\lambda) = Adv^A_{\mathbb{P}-\text{IND-CPA}}(\lambda)$ in Game 0, and $Adv^A_{\mathbb{P}}(\lambda), Adv^A_{\mathbb{P}-\text{IND-CPA}}(\lambda), Adv^A_{\mathbb{P}-\text{IND-CPA}}(\lambda)$ be the advantage of in Game 1, 2-k, 3, respectively. It is clear that $Adv^A_{\mathbb{P}-\text{IND-CPA}}(\lambda) = 0$ by Lemma 4.

We will use three lemmas (Lemmas 1-3) that evaluate the gaps between pairs of $Adv^A_{\mathbb{P}}(\lambda), Adv^A_{\mathbb{P}-\text{IND-CPA}}(\lambda), Adv^A_{\mathbb{P}-\text{IND-CPA}}(\lambda)$ and from these lemmas, we obtain

© 2014 ACADEMY PUBLISHER
\[ \text{Adv}_{A}^{\text{PPPP-IND-CPA}} = \text{Adv}_{A}^{(0)(\lambda)} \]
\[ \leq |\text{Adv}_{A}^{(0)(\lambda)}| + \sum_{k=1}^{n} |\text{Adv}_{A}^{(2-k)(\lambda)}| + |\text{Adv}_{A}^{(2-k)(\lambda)} + \text{Adv}_{B}^{(0)(\lambda)}| \]
\[ \leq \text{Adv}_{B}^{(0)(\lambda)} + \sum_{k=1}^{n} \text{Adv}_{B}^{(0)(\lambda)} + n/q. \]

From the work of [26] (Lemma 20 and 22), there exist probabilistic machines \( C_b(k = 1, \ldots, n) \), whose running times are essentially the same as those of \( B_b \), respectively, such that 
\[ \text{Adv}_{C_b}^{(0)(\lambda)}(\lambda) = \text{Adv}_{B_b}^{(0)(\lambda)}(\lambda) \]
and 
\[ \text{Adv}_{C_b}^{(2-k)(\lambda)}(\lambda) = \text{Adv}_{B_b}^{(2-k)(\lambda)}(\lambda). \]

**Proof.** The proof of this lemma is similar to the work of [26] (Lemma 24). In order to prove Lemma 2, we construct a probabilistic machine \( B \) against Problem 1 by using any adversary \( A \) in a security game (Game 0 or 1) as a black box as follows:

1. \( B \) is given Problem 1 instance \((\text{paramy}, \hat{\beta}, \hat{\beta}^*, \{e_{\gamma,i}\}_{i=1,2n}).\)
2. \( B \) plays a role of the challenger in the security game against adversary \( A \).
3. At the first step of the game, \( B \) returns \( PK := (\lambda, \text{paramy}, \hat{\beta}, h_1, h_2) \) to \( A \).
4. When a corrupt query is issued, \( B \) answers a correct secret key computed by using \( \hat{\beta}^* \), i.e., normal key.
5. When \( B \) gets challenge plaintexts \( M_0, M_1 \) (\(|M_0| = |M_1|\)), and challenge receivers sets \( S_0, S_1 \subseteq \{1, \ldots, n\} \) (from \( A \)), \( B \) calculates and returns \( C := (C_1, C_2) \) such that 
\[ C_1 := \sum_{i \in S_0} e_{\gamma,i} + \zeta b_{4n+1} \]
and 
\[ C_2 := g^b \cdot M_0. \]
6. After the challenge encryption query, corrupt oracle simulation for a corrupt query is executed in the same manner as step 4.
7. \( A \) outputs bit \( b \). If \( b = b' \), \( B \) outputs \( \gamma' := 1 \).
   Otherwise, \( B \) outputs \( \gamma' := 0 \).

**Claim 1:** If \( \gamma = 0 \), the distribution of \((C_1, C_2)\) generated in step 5 is the same as that in Game 0. If \( \gamma = 1 \), the distribution of \((C_1, C_2)\) generated in step 5 is the same as that in Game 1.

**Proof.** If \( \gamma = 0 \), 
\[ C_1 := \sum_{i \in S} \delta_i (x_i, b_{2i-1} + x_i, b_{2i}) + \sum_{j \in U-S} (y_j, b_{2i-1} + y_j, b_{2i}) + \zeta b_{4n+1} + \delta b_{4n+3}. \]
and 
\[ C_2 := g^b \cdot M_\beta. \]
This is the target ciphertext in Game 0. If \( \gamma = 1 \), 
\[ C_1 := \sum_{i \in S} \delta_i (x_i, b_{2i-1} + x_i, b_{2i}) + \sum_{j \in U-S} (y_j, b_{2i-1} + y_j, b_{2i}) + \sum_{i=1}^{2n} w_i b_{2n+i} + \zeta b_{n+1} + \delta b_{4n+3}. \]

From Claim 1, when \( \gamma = 0 \), the advantage of \( A \) in the above game is equal to that in Game 0, i.e., \( \text{Adv}_{A}^{(0)(\lambda)}(\lambda) \), and is also equal to \( \text{Pr}_{T_0} := \text{Pr}[B_0(\lambda, \sigma, \delta) \in G_{0}^{\hat{P}_1(\lambda, n)}] \). Similarly, when \( \gamma = 1 \), we see that the advantage of \( A \) in the above game is equal to \( \text{Adv}_{A}^{(1)(\lambda)}(\lambda) \), and is also equal to \( \text{Pr}_{T_1} := \text{Pr}[B_1(\lambda, \sigma, \delta) \in G_{1}^{\hat{P}_1(\lambda, n)}] \). Therefore, 
\[ |\text{Adv}_{A}^{(0)(\lambda)}(\lambda) - \text{Adv}_{A}^{(1)(\lambda)}(\lambda)| = |\text{Pr}_{T_0} - \text{Pr}_{T_1}| = \text{Adv}_{A}^{(1)(\lambda)}(\lambda). \]
This completes the proof of Lemma 1. \( \square \)

**Lemma 2:** For any adversary \( A \), there exists a probabilistic machine \( B \), whose running time is essentially the same as that of \( A \), such that for any security parameter \( \lambda \), 
\[ |\text{Adv}_{A}^{(2-k)(\lambda)}(\lambda) - \text{Adv}_{A}^{(2-k)(\lambda)}(\lambda)| = \text{Adv}_{B}^{(2-k)(\lambda)}(\lambda)/1 + g. \]

**Proof.** The proof of this lemma is similar to the work of [26] (Lemma 25). In order to prove Lemma 2, we construct a probabilistic machine \( B \) against Problem 2 by using any adversary \( A \) in a security game (Game 2-(k-1) or 2-k) as a black box as follows:

1. \( B \) is given Problem 2 instance \((\text{paramy}, \hat{\beta}, \hat{\beta}^*, \{h_{i,j}, e_{i}\}_{i=1,2n}).\)
2. \( B \) plays a role of the challenger in the security game against adversary \( A \).
3. At the first step of the game, \( B \) returns \( PK := (\lambda, \text{paramy}, \hat{\beta}, h_1, h_2) \) to \( A \).
4. When the s-th corrupt query is issued for \( i \in [1, \ldots, n] \), \( B \) answers as follows:
   a) When \( 1 \leq s \leq k - 1 \), \( B \) calculates and answers (by using \( \hat{\beta}^* \)) 
   \[ s k_i^*: = \sigma_i (h_1(i) b_{2s-1} + h_2(i) b_{2s}) + \sum_{j=1}^{2n} r_j b_{2n+i} + b_{4n+1} + \eta b_{4n+2}. \]
   where \( \sigma_i, \eta, r_1, \ldots, r_{2n} \in \mathbb{F}_q \) (i.e., semifunctional key).
   b) When \( s = k \), \( B \) calculates and answers \( s k_i^* \) as follows:
   \[ s k_i^*: = \sum_{i=1}^{2n} h_{i,j}^* b_{4n+1}. \]
   c) When \( s \geq k + 1 \), \( B \) answers a correct secret key computed by using \( \hat{\beta}^* \), i.e., normal key.
5) When $B_k$ gets challenge plaintexts $M_0$, $M_1$ ($|M_0| = |M_1|$), and challenge receivers sets $S_0, S_1 \subseteq \{1, \ldots, n\}$ (from $A$), $B_k$ calculates and returns $C := (C_1, C_2)$ such that $C_1 := \sum_{i \in S_0} e_{\beta,i} + \zeta b_{4n+1} + \delta_2 b_{4n+3}$, where $e_{\beta,i}$ are from the Problem 2 instance, $\zeta, \delta_2 \in \mathbb{F}_q$, $b \in \{0, 1\}$.

6) After the challenge encryption query, corrupt oracle simulation for a corrupt query is executed in the same manner as step 4.

7) $A$ outputs bit $b'$. If $b = b'$, $B_k$ outputs $b' := 1$. Otherwise, $B_k$ outputs $b' := 0$.

Claim 2: The secret key $sk^*_B$ generated in case (b) of step 4 or 6 and ciphertext $C_1$ generated in step 5 has the same distribution as that in Game 2-$(k-1)$ (resp. Game 2-$k$) when $\beta = 0$ (resp. $\beta = 1$) except with probability $1/q$.

Proof. We consider the joint distribution of $C_1$ and $sk^*_B$.

Ciphertext $C_1$ generated in step 5 is $C_1 := \sum_{i \in S_0} e_{\beta,i} + \zeta b_{4n+1} + \delta_2 b_{4n+3}$, where $e_{\beta,i}$ are from the Problem 2 instance, $\zeta, \delta_2 \in \mathbb{F}_q$.

When $\beta = 0$, secret key $sk^*_B$ generated in step 4 or 6 is

$$sk^*_B := \sum_{i = 1}^{2n} b_{i,\beta,i} + b_{4n+1}$$

When $\beta = 0$, secret key $sk^*_B$ generated in step 4 or 6 is

$$sk^*_B := \sigma_i(h_1(i) b_{2i-1} + h_2(i) b_{2i}^*) + \sum_{j=1}^{2n} r_j \cdot b_{2n+j}^* + b_{4n+1} + \eta b_{4n+2}.$$
In the light of the adversary’s view, both $(B, B^*)$ and $(D, D^*)$ are consistent with public key $PK := (1^λ, \text{param}_B, h_1, h_2)$. Therefore, $\{sk_i\}_{i=1, \ldots, n}$ and $C_1$ above can be expressed as keys and ciphertext in two ways, in Game 2 $− n$ over bases $(B, B^*)$ and in Game 3 over bases $(D, D^*)$. Thus, Game $2 − n$ can be conceptually changed to Game 3. □

Lemma 4: For any adversary $A$, Adv$^{(3)}_{A}(\lambda) = 0$.

Proof. The value of $b$ is independent from the adversary’s view in Game 3. Hence, Adv$^{(3)}_{A}(\lambda) = 0$.

VI. CONCLUSIONS

In this paper, we propose the formal definition of anonymous public-key broadcast encryption (ANON-PKBE) scheme, and described the new security definition. Then we proposed a specific ANON-PKBE scheme, and proved it in the standard model.

Although our scheme meets all of security requirements, its efficiency is relatively low. It is still an open problem, to construct a practical ANON-PKBE scheme, which is ANON-IND-CPA in the standard model.

ACKNOWLEDGMENT

This work was supported in part by the National Natural Science Foundation of China (No.61272434), and the Natural Science Foundation of Shandong Province (No.ZR2013FQ021 and No.ZR2011FQ032).

REFERENCES


Hao Wang received his B.S. degree in computational mathematics from Qufu Normal University, China, in June 2007 and his Ph.D. degree in computer science from Shandong University, China, in June 2012. His current research interest includes information security and cryptography.

Lei Wu received his B.S. and Ph.D. degree in applied mathematics from Shandong University, China, in 2002 and 2009, respectively. His current research interest includes information security and cryptography.