Multimedia Tools and Applications (2020) 79:7889–7910
https://doi.org/10.1007/s11042-019-08574-1

Adaptively secure broadcast encryption with authenticated content distributors

Dianli Guo[1,2] · Qiaoyan Wen[1] · Wenmin Li[1] · Hua Zhang[1] · Zhengping Jin[1]

Received: 28 August 2018 / Revised: 11 October 2019 / Accepted: 6 December 2019 /
Published online: 3 January 2020

Abstract
In public key broadcast encryption systems, anyone could run the encryption algorithm to broadcast messages by using the public parameters. The unsupervised broadcast strategy allows malicious users (even though someone outside the system with the intentionally divulged public parameters) to distribute junk messages without responsibility. Consequently, content distributor authentication is essential for broadcast encryption systems to forbid spreading of junk information. In this work, we devise a solution for public key broadcast encryption system with adaptive security to resolve the aforementioned vicious broadcaster problem, which is neglected in the previous related works. In our scheme, any user could distribute an encryption of messages with both public parameters and his/her own secret keys, and each message is associated to its broadcaster. The construction is based on the composite order bilinear groups and its adaptive security depends on the hardness of the general subgroup decisional assumptions. Furthermore, this allows our scheme to be flexible in terms on the overhead of ciphertexts, which is constant sized. Compared with previous related broadcast encryption systems constructed in the composite order bilinear groups, our scheme inherits the superiority of adaptive security based non-interactive falsifiable assumption, and simultaneously achieves the optimal ciphertext overhead and the authentication of broadcasters.

Keywords Broadcast encryption · Adaptive security · Authenticated broadcaster · Composite order bilinear group

1 Introduction

Broadcast encryption system (BE) [12] enables a broadcaster to encrypt messages to any set S of receivers drawn from the universe of users U, only authorized users included in the set S can decrypt the broadcast with his/her own secret key and any other cannot. Broadcast encryption provide a solution for confidentially broadcasting content to multiple users, and

✉ Hua Zhang
zhanghua_288@bupt.edu.cn

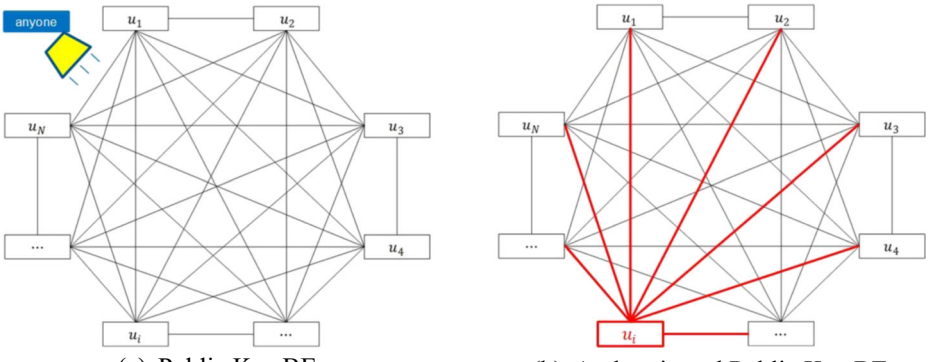
Extended author information available on the last page of the article.

it is regularly employed in many practical applications such as pay-TV, group communication, radio subscription systems and file system access control [3, 29, 31]. In a broadcast encryption system, fully collusion resistant is a fundamental security property in the sense that a ciphertext cannot be recovered by any coalition of users who are not included in the set S. Identity-based broadcast encryption [10, 11, 20, 24, 34] is one kind of BE systems, which should support exponentially many users. The framework is a generalization of the identity-based encryption (IBE). Or, put another way, IBE system [20, 22, 32] is a specific form of the identity-based broadcast encryption, which has only a single receiver in the broadcast.

A public key broadcast encryption system means that any user in the system could encrypt messages and play the role of broadcaster [3, 15]. In contrast, only the trust authority possesses the jurisdiction to distribute content in the broadcast encryption system, the former is more flexible and efficient. Whereas, it is also difficult to be supervised. A Traitor Tracing [4, 8, 16, 21, 26] or Trace & Revoke system [6, 14, 28] is designed to handle the pirate problem, and help content distributors identify malicious users and revoke the corresponding keys. Nevertheless, how to protect users to refrain from receiving junk messages broadcasted venomously by some content distributors.

Consider a scenario in which a vicious content distributor intends to broadcast junk messages, like gambling advertising, illegal commercial advertising, porn and violence information, while any user may access to the content with his/her secret keys [25]. The risk for such a public key broadcast encryption system is that any user could execute the aforementioned operation and ignore any relevant laws and regulations on broadcast content. Even worse, an unauthorized person or organisation could broadcast content with the sold or intentionally divulged public parameters from malicious users, and will not bear any responsibilities for that. The problem is that in this system there exist no verification mechanism for identifying content distributors.

As shown in Fig. 1, the intuitive solution for this issue is that every distributor signs the broadcast. Receivers could verify the signature to confirm the authenticity of its broadcaster. If any user obtains spam from decrypting the broadcast, the law enforcement officer will take legal action against the owner of the corresponding signature for the broadcast content. However, there is a significant problem in this combination of the broadcast encryption



(a) Public Key BE (b) Authenticated Public Key BE

Fig. 1 Authenticated Public Key BE System

with a signature scheme, in which the vicious broadcaster is untraceable if he/she forges a signature for distributed messages and receivers also could decrypt the broadcast to obtain the spam. Some researchers [23, 25, 27, 30] introduce broadcast signcryption schemes to realize broadcaster authentication. However, in these broadcast signcryption systems, the broadcaster is assigned in the initial building phase and every receiver should registers at broadcaster to acquire decryption key. Furthermore, the ciphertext typically grows linearly with either the size of the broadcast subset or the revoked subset. In this paper, we devise a low overhead public key broadcast encryption scheme with authenticated content distributors in another way, it achieves the signature feature and forbid the above matter.

In this paper, we begin by formally defining the notion for a public key broadcast encryption system with authenticated broadcasters. For now we present some intuition of the definition. This system is comprised of four randomized algorithms **Setup**, **KeyGen**, **Encrypt** and **Decrypt**. The setup and user key generation algorithm respectively generate the master secret key with the corresponding public parameters and users' secret keys. The generated user secret keys contain two parts: broadcast key and decryption key. The encrypt algorithm encrypts the content with public parameters and user's broadcast key. The decrypt algorithm is able to decrypt the broadcast with decryption keys of the authorized users. Specifically, the decrypt algorithm could realize the authentication for distributor during the decryption. If the content distributor encrypts messages without his/her own broadcast secret key or with a forged one, the created ciphertext is unavailable.

The main security requirements of conventional public key broadcast encryption systems are the semantic security (the ciphertext should reveal no non-trivial information about the broadcasted plaintext) and fully collusion security (the system is secure against any number of colluders). Except that, the system captured broadcaster authentication should remain secure even if the content distributer is vicious. That is, the broadcast reveals no non-trivial information if it is encrypted without a correct broadcast secret key or with a forged one. Herein, this implies that the venomous broadcaster does not use his/her broadcast secret key to encrypt digital content to prevent being traced. We formalize the definition for adaptive security in broadcast encryption system featured verification of distributor. In such a system, the adversary is allowed to see public parameters and query user private keys before choosing the set of indices that he/she wish to attack. Further, he/she also could assign the identity of sender to create an encrypted version of the content.

Contributions Subsequently, we present a construction for public key broadcast encryption system to attain meaningful guarantees of authenticated broadcasters. We describe such a system for N users with composite bilinear maps, it has ciphertext overhead of only $O(1)$ group elements. The public key size and user secret key size are linear in the total number N of users. We prove the construction is fully collusion resistant under adaptive attacks in the standard model assuming only General Subgroup Decision Assumptions.

Outline The layout of the proposal is organized as follows. We present the related literatures briefly in the next section and some essential definitions in Section 3. Then, we describe the construction of the authenticated broadcast encryption and give the formal security analysis in the standard model respectively in Sections 4 and 5. Subsequently, we show the evaluation of performance with other related solutions in Section 6. The final section conclude this work.

2 Related work

A trivial solution to broadcast encryption admits the broadcaster encrypts messages separately by each recipient's public key, the broadcast information expansion is proportional to the size of recipient set. This trivial solution possesses low storage requirements and adaptive security. Nevertheless, such a system has a very high ciphertext expansion. Therefore, there are many researchers provided their broadcast encryption schemes with lower ciphertext expansion. However, such systems tradeoff between security and parameters size, and include a collusion bound t (using larger value of t will affect performance and overall system usability). If more than t users collude and pool their private keys, the system would no longer guarantee security [12].

In 2005, Boneh, Gentry and Waters [3] propose the first broadcast encryption scheme with constant sized ciphertexts and private keys. The public key size in their system is linear in the total number receivers. Their scheme is built from bilinear maps and fully secure against any number of colluders. However, the authors only prove security of their scheme in a static model, where the adversary needs to commits the target set that the challenge ciphertexts is encrypted to before observing public parameters.

Four years later, Gentry and Waters [15] define the adaptive security definition of broadcast encryption and suggest an adaptively secure identity-based broadcast encryption system, in which there is a separate tag value associated with the recipient group size included in the ciphertexts. Subsequently, the authors introduce a way to reuse Tag in the original system by increasing the ciphertext size to sub-linear. The adaptive security captures the fact that an adversary could declare the challenge set he/she wishes to attack, based on the acquired knowledge of the public parameters and previously queried private keys. Obviously, the adaptive model of security is the proper notion of the security for broadcast encryption systems to against the more general adversaries.

In 2009, Waters [32] present a methodology called Dual System Encryption for demonstrating adaptive security of encryption systems. The author also propose a secure broadcast encryption scheme with leveraging their dual system encryption techniques, in which the ciphertext, public key and secret key sizes are $O(1)$, $O(N)$, $O(N)$ respectively.

In 2012, Lewko and Waters [22] provide a dual system encryption in composite order bilinear groups and introduce an improved method for proving encryption scheme under static complexity assumptions (not dependent on the depth of the hierarchy or the number of queries made by an attacker). Later, Kim et al. [20] propose an identity-based broadcast encryption featuring constant sized ciphertext. Technically, they employ the security proof technique introduced by Lewko and Waters, and the proposal offers adaptive security proved in the stand model. In their scheme, the size of public parameters and private keys are both linear in the maximum number of receivers. However, the maximum number of receivers should be fixed in the setup phase, and this restriction would impact the flexibility of the public key broadcast encryption system, in which the contend distributor could broadcast to any authorized set of users.

In 2019, Guo et al. [17] introduce an authenticated public key broadcast encryption with prime bilinear map, in which each user possesses a broadcast key to encrypt content and guarantees the generated ciphertext is traceable. This supervised distributed strategy solves the vicious broadcaster problem in the public key broadcast encryption systems. However, their scheme is proved statically secure with decisional Diffie-Hellman assumption.

Constructions of broadcast encryption from multilinear maps [5, 9, 13] have optimal parameters overhead. Boneh et al. [7] provide the solution for N users from $O(logN)$-linear maps, in which the ciphertext overhead is $O(1)$, secret key size and public key size are all

poly-logarithmic in N. Whereafter, many researchers devise broadcast encryption scheme based on their scheme in prime or composite order multilinear groups for higher security [18, 33]. Nevertheless, in 2016 Hu and Jia [19] show the applications of GGH map (a major candidate of multilinear maps) for encoding is not secure. Therefore, we no longer detailed these results from multilinear maps here.

3 Preliminary

3.1 Public key broadcast encryption systems with broadcaster authentication

Herein, we formally present the definition of public key broadcast encryption systems with broadcaster authentication. Similar to the conventional broadcast encryption systems, it is also defined as a key encapsulation mechanism. Further, the presented definition is general enough to capture identity-based broadcast encryption systems. A broadcast encryption scheme with broadcaster authentication consists of four randomized algorithms: **Setup**, **KeyGen**, **Encrypt** and **Decrypt**.

Setup($\mathcal{ID}$, λ) Take as input identity space $\mathcal{ID}$ and security parameter λ. It outputs the public parameters PK and master secret key msk.

KeyGen(msk, u) Takes as input an identity $u \in \mathcal{ID}$ and master secret key msk. It outputs user secret key sk_u for u.

Encrypt(PK, S, sk_i) The encryption algorithm takes as input the public parameters PK, recipient set $S \subseteq \mathcal{ID}$, the broadcaster's secret key sk_i. It outputs a pair $\langle Hdr, K \rangle$, where Hdr is called the header and K is a message encryption key. Let M be a plaintext message to be broadcasted and let $C \leftarrow SymEnc(K, M)$ be the symmetric encryption of M under the encryption key K. The overall ciphertext broadcasted to users consists of $\{S', Hdr, C\}$, where $S' = S \cup \{i\}$. Notice that, the broadcaster index in S' is explicit, for example, i is always first element in S'. The ciphertext $\{S', Hdr, C\}$ is unavailable if the broadcaster produces them without his/her own broadcast secret key or with a forged one.

Decrypt(PK, S', u, sk_u, Hdr) Take as input the public key PK, a subset S', an index $u \in \mathcal{ID}$, a private key sk_u for u, and the received header Hdr. If $u \in S' \setminus \{i\}$, the decryption algorithm outputs the message encryption key K, which is used to decrypt C to retrieve M; otherwise, it outputs $\perp$. Notice that, if the received ciphertext $\{S', Hdr, C\}$ is unavailable, the decryption algorithm always outputs $\perp$.

Next, we require that the system should satisfy the correctness property. That is, for all $S \subseteq \mathcal{ID}$, $i \in \mathcal{ID}$ and all $u \in S$, if (PK, msk) output by **Setup**$(\mathcal{ID}, \lambda)$, sk_i output by **KeyGen**(msk, i), sk_u output by **KeyGen**(msk, u) and (Hdr, K) output by **Encrypt**(S, PK, sk_i), that **Decrypt**$(PK, S \cup \{i\}, u, sk_u, Hdr) = K$.

3.2 Security definition

We formally define the adaptive security model of the public key broadcast encryption with broadcaster authentication. In such a adaptively secure system, the adversary could query several users' private keys before committing a set which he/she wish to attack. It also captures the collusion attack implicitly by modeling the adversary queries all secret keys

of users outside of the committed set S^*. This basically follows the security definition of broadcast encryption in [15]. The difference is that the adversary needs to specify an identity to simulate broadcaster in the challenge phase.

Setup The challenger runs the **Setup**($\mathcal{ID}$, λ) algorithm and obtains public parameters PK. Afterwards, it gives PK to the adversary $\mathcal{A}$.

Secret key queries The challenger maintains a list $\mathcal{L}$ of $\langle u, sk_u \rangle$, which is initialized empty. When $\mathcal{A}$ adaptively issues secret key queries for indices $u \in \mathcal{ID}$. The challenger looks up the list $\mathcal{L}$ and responds to $\mathcal{A}$ as follows:

(1) If $\langle u, sk_u \rangle$ exists in $\mathcal{L}$, the challenge sends sk_u to $\mathcal{A}$.
(2) Otherwise, it runs the algorithm **KeyGen**(msk, u) and insert a new tuple $\langle u, sk_u \rangle$ into $\mathcal{L}$. Then it sends sk_u to $\mathcal{A}$.

Challenge The adversary specifies a challenge set $S^* \subset \mathcal{ID}$ and a broadcaster identity $i \notin S^*$, which subject to the restriction that each user in S^* never have been requested in the secret key query. And then $\mathcal{A}$ proceeds to declare two equal length messages M_0, M_1. If $\langle i, sk_i \rangle$ exists in the list $\mathcal{L}$, the challenger output sk_i; otherwise, it runs the algorithm **KeyGen**(msk, i) to acquire sk_i and inserts the generated $\langle i, sk_i \rangle$ to $\mathcal{L}$. Subsequently, it computes $(Hdr^*, K^*) \underset{\leftarrow}{R}$ **Enc**(S^*, PK, sk_i), and randomly selects $\beta \in \{0, 1\}$ to calculate $C^* = SymEnc(K^*, M_\beta)$, then it gives (Hdr^*, C^*) to the adversary $\mathcal{A}$.

More secret key queries The adversary $\mathcal{A}$ is allowed to query more secret keys with the restriction that $u \notin S^*$.

Guess The adversary returns a guess $\beta' \in \{0, 1\}$ of β.

The adaptive advantage of adversary $\mathcal{A}$ wining the above game is defined as $Adv^{\mathcal{A}}_{\mathcal{ID},\lambda} = |\Pr[\beta' = \beta] - 1/2|$.

Definition 1 A broadcast encryption system with broadcaster authentication is secure if for all polynomial time adversaries $\mathcal{A}$, $Adv^{\mathcal{A}}_{\mathcal{ID},\lambda}$ is a negligible functions of λ.

3.3 Composite order bilinear maps

Herein, we briefly review some general notions about composite order bilinear maps and groups which were introduced in [2, 22].

Consider two cyclic groups $\mathbf{G}$ and $\mathbf{G}$ of same order $n = p_1 \cdot p_2 \cdot p_3$ (where p_1, p_2, p_3 are distinct large primes), we let $e : \mathbf{G} \times \mathbf{G} \rightarrow \mathbf{G}_T$ denote its bilinear map, which is assumed an efficiently computable function such that:

– Bilinear: $\forall g, h \in \mathbf{G}, a, b \in Z_n, e(g^a, h^b) = e(g, h)^{ab}$.
– Non-degenerate: $\exists g \in \mathbf{G}$ such that $e(g, g)$ is a generator of $\mathbf{G}_T$, which has order n.

We will use the notation G_i ($i = 1, 2, 3$) to denote the respective subgroup of order p_i of $\mathbf{G}$. The notations g_1, g_2, g_3 respectively denote generators of G_1 through G_3. Each element $\mathbf{h} \in \mathbf{G}$ could be expressed as $\mathbf{h} = g_1^{\gamma_1} g_2^{\gamma_2} g_3^{\gamma_3}$ for some $\gamma_1 \in Z_{p_1}$, $\gamma_2 \in Z_{p_2}$, $\gamma_3 \in Z_{p_3}$. If $\gamma_i (mod\ p_i) \equiv 0$ for $i = 1, 2, 3$, we say that there is no component of G_i in G. The subgroups G_1, G_2, G_3 maintain the orthogonality property under the bilinear map e. Specifically, if $g_i \in G_i$ and $h_j \in G_j$ for $i \neq j$, $e(g_i, h_j) = 1$, which denotes the identity element of $\mathbf{G}_T$.

Similar to some broadcast encryption constructions in composite order bilinear groups, the orthogonality property is also the principal tool in our scheme for realizing dual system, which is significant methodology for proving adaptive security.

3.4 General subgroup decision assumptions

Now that, we review the general subgroup decision assumptions for composite order bilinear groups, which are a family of static complexity assumptions (independent on the number of queries issued by an attacker). We base the security of the proposed public key broadcast encryption system with broadcaster authentication on these three assumptions formulated in [1, 22].

More formally, let $\mathcal{G}(1^{\lambda})$ denote a group generation algorithm. It takes in a security number λ and outputs $(n = p_1 \cdot p_2 \cdot p_3, \mathbf{G}, \mathbf{G}_T, e)$, where p_1, p_2, p_3 are distinct primes, $\mathbf{G}$ and $\mathbf{G}_T$ are cyclic groups of order n, e is a computable bilinear map in polynomial time with respect to $\mathbf{G}$ and $\mathbf{G}_T$.

Assumption 1 If an adversary is given the following parameters

$$(n = p_1 \cdot p_2 \cdot p_3, \mathbf{G}, \mathbf{G}_T, e) \underset{\leftarrow}{R} \mathcal{G}(1^{\lambda}),$$
$$g_1, w_{1,1}, w_{1,2}, \cdots, w_{1,2^{n-1}} \underset{\leftarrow}{R} G_1,$$
$$X_2 \underset{\leftarrow}{R} G_2,$$
$$\mathcal{D} = \{n, \mathbf{G}, \mathbf{G}_T, e, g_1, w_{1,1}, \cdots, w_{1,2^{n-1}}, X_2\},$$
$$T_1 \underset{\leftarrow}{R} G_{1,3}, \ T_2 \underset{\leftarrow}{R} G_1,$$

it must be hard to distinguish T_1 from T_2.

Let define the advantage $Adv^1_{\lambda,\mathcal{A}}$ of $\mathcal{A}$ in breaking Assumption 1:

$$Adv^1_{\lambda,\mathcal{A}} = \mid \Pr[\mathcal{A}(\mathcal{D}, T_1) = 1] - \Pr[\mathcal{A}(\mathcal{D}, T_2) = 1] \mid .$$

Definition 2 We say that Assumption 1 holds if no polynomial time algorithm $\mathcal{A}$ has a non-negligible advantage $Adv^1_{\lambda,\mathcal{A}}$.

Assumption 2 If an adversary is given the following parameters

$$(n = p_1 \cdot p_2 \cdot p_3, \mathbf{G}, \mathbf{G}_T, e) \underset{\leftarrow}{R} \mathcal{G}(1^{\lambda}),$$
$$g_1, X_1 \underset{\leftarrow}{R} G_1,$$
$$U_2, V_2, X_2, Y_2 \underset{\leftarrow}{R} G_2,$$
$$U_3, V_3, X_3, Y_3 \underset{\leftarrow}{R} G_3,$$
$$\mathcal{D} = \{n, \mathbf{G}, \mathbf{G}_T, e, g_1, X_1X_3, X_2, Y_2Y_3, U_2U_3, V_2V_3\}$$
$$T_1 \underset{\leftarrow}{R} \mathbf{G}, \ T_2 \underset{\leftarrow}{R} G_{1,2},$$

it must be hard to distinguish T_1 from T_2.

Let define the advantage $Adv^2_{\lambda,\mathcal{A}}$ of $\mathcal{A}$ in breaking Assumption 2:

$$Adv^2_{\lambda,\mathcal{A}} = \mid \Pr[\mathcal{A}(\mathcal{D}, T_1) = 1] - \Pr[\mathcal{A}(\mathcal{D}, T_2) = 1] \mid .$$

Definition 3 We say that Assumption 2 holds if no polynomial time algorithm $\mathcal{A}$ has a non-negligible advantage $Adv^2_{\lambda,\mathcal{A}}$.

Assumption 3 If an adversary is given the following parameters

$$(n = p_1 \cdot p_2 \cdot p_3, \mathbf{G}, \mathbf{G}_T, e) \xleftarrow{R} \mathcal{G}(1^\lambda),\ \alpha, s \xleftarrow{R} Z_n,$$

$$g_1 \xleftarrow{R} G_1,\ X_2 \xleftarrow{R} G_2,\ X_3, Y_3, H_3, U_3, V_3 \xleftarrow{R} G_3,$$

$$\mathcal{D} = \{n, \mathbf{G}, \mathbf{G}_T, e, g_1, g_1^\alpha X_3, X_2, g_1^k Y_3, H_3, U_3, V_3\},$$

$$T_1 = e(g, g)^{\alpha k},\ T_2 \xleftarrow{R} \mathbf{G}_T,$$

it must be hard to distinguish T_1 from T_2.

Let define the advantage $Adv^3_{\lambda,\mathcal{A}}$ of $\mathcal{A}$ in breaking Assumption 3:

$$Adv^3_{\lambda,\mathcal{A}} = |\Pr[\mathcal{A}(\mathcal{D}, T_1) = 1] - \Pr[\mathcal{A}(\mathcal{D}, T_2) = 1]|.$$

Definition 4 We say that Assumption 3 holds if no polynomial time algorithm $\mathcal{A}$ has a non-negligible advantage $Adv^3_{\lambda,\mathcal{A}}$.

4 Broadcast encryption system with broadcaster authentication

In this section, we present our adaptively secure construction of broadcast encryption with content distributor authentication from composite order bilinear maps. The size of ciphertext in our scheme is optimal ($O(1)$ bits). Furthermore, we employ the methodology of Lewko and Waters for realizing dual system encryption to demonstrate the adaptive security of our construction under the non-interactive assumptions in the standard model.

Setup (N, λ) The setup algorithm takes in the total number $N = |\mathcal{ID}| = 2^n - 1$ of users in the system and the security parameter λ as input. Let $\mathbf{G}$ be a bilinear group of composite order $n = p_1 p_2 p_3$, where p_1, p_2, p_3 are distinct primes. Afterwards, the algorithm chooses random generators $g_1, w_{1,u} \in G_1$ ($u \in \mathcal{ID}$), where G_1 is a subgroup of $\mathbf{G}$ of order p_1. Next, it picks a random $\alpha \in Z_n$ as master secret key msk. The public parameters are published as $PK = \{g_1, w_{1,u}, e(g_1, g_1)^\alpha\}$ for $u \in \mathcal{ID}$.

KeyGen (msk, u) The key generation algorithm randomly chooses generators $\hat{g}_1, h_{1,i} \in G_1$, $R_{2,i}, \hat{R}_{2,i} \in G_2$ for $i \in \mathcal{ID}$. Subsequently, it generates $r_u \in Z_n$ for identity u in $\mathcal{ID}$. The private keys of user $u \in \mathcal{ID}$ are

$$\begin{aligned}
sk_u &= \{D_u, \hat{D}_u, \forall_{i\in[1,2^n-1]} D_{u,i}, \hat{D}_{u,i}, E_u\},\\
D_u &= g_1^\alpha (w_{1,u}\hat{g}_1)^{r_u} R_{2,u},\\
\hat{D}_u &= g_1^{r_u} \hat{R}_{2,u},\\
\forall_{i\in[1,2^n-1], i\neq u} D_{u,i} &= w_{1,i}^{r_u} R_{2,i},\\
\forall_{i\in[1,2^n-1], i\neq u} \hat{D}_{u,i} &= h_{1,i}^{r_u} \hat{R}_{2,i},\\
E_u &= \hat{g}_1 h_{1,u}.
\end{aligned}$$

Enc (S, PK, sk_i) The encryption algorithm picks random $k \in Z_n$ and computes the key and header as

$$\begin{aligned} K &= e(g_1, g_1)^{\alpha k}, \\ Hdr &= (C_0, C_1) \\ &= \left(g_1^k, \left(E_v \prod_i^S w_{1,i} \right)^k \right) \\ &= \left(g_1^k, \left(\hat{g}_1 h_{1,v} \prod_i^S w_{1,i} \right)^k \right), \end{aligned}$$

where v is the identity of the broadcaster.

It sets $C = SymEnc(K, M)$, where $SymEnc()$ is a symmetric encryption algorithm. The overall ciphertexts are $\{S' = S \cup \{v\}, Hdr, C\}$. The broadcaster identity v in S' is explicit.

Dec (PK, u, sk_u, S', Hdr) Suppose $u \in S$ $(S = S' - \{v\})$, $u \neq v$ and v is a legitimate broadcaster, the decryption algorithm outputs

$$K = \frac{e\left(D_u \cdot \left(\prod_{i \neq u}^S D_{u,i} \right) \cdot \hat{D}_{u,v}, C_0 \right)}{e(C_1, \hat{D}_u)}.$$

Then, it outputs the message $M = SymDec(K, C)$.

Correctness K can be calculated as follows:

$$\begin{aligned} K &= \frac{e\left(D_u \cdot \left(\prod_{i \neq u}^S D_{u,i} \right) \cdot \hat{D}_{u,v}, C_0 \right)}{e(C_1, \hat{D}_u)} \\ &= \frac{e\left(D_u \cdot \left(\prod_{i \neq u}^S D_{u,i} \right), C_0 \right)}{e(C_1, \hat{D}_u)} \cdot e(\hat{D}_{u,v}, C_0) \\ &= \frac{e\left(g_1^\alpha \left(w_{1,u} \hat{g}_1 \right)^{r_u} R_{2,u} \cdot \left(\prod_{i \neq u}^S w_{1,i}^{r_u} R_{2,i} \right), g_1^k \right)}{e\left(\left(\hat{g}_1 h_{1,v} \prod_i^S w_{1,i} \right)^k, g_1^{r_u} \hat{R}_{2,u} \right)} \\ &\quad \cdot e\left(h_{1,v}^{r_u} \hat{R}_{2,i}, g_1^k \right) \end{aligned}$$

$$
\begin{aligned}
&= \frac{e\left(g_1^{\alpha}, g_1^{k}\right) \cdot e\left(\prod_i^S w_{1,i}^{r_u}, g_1^{k}\right) \cdot e\left(\hat{g}_1^{r_u}, g_1^{k}\right) \cdot e\left(h_{1,v}^{r_u}, g_1^{k}\right)}{e\left(\hat{g}_1^{k}, g_1^{r_u}\right) \cdot e\left(h_{1,v}^{k}, g_1^{r_u}\right) \cdot e\left(\left(\prod_i^S w_{1,i}\right)^{k}, g_1^{r_u}\right)} \\
&= e\left(g_1^{\alpha}, g_1^{k}\right) \\
&= e\left(g_1, g_1\right)^{\alpha k}
\end{aligned}
$$

Note that, if the broadcaster v produces the distributed ciphertexts without his/her own broadcast secret key or with a forged one, the receiver will employ the secret key $\hat{D}_{u,v}$ corresponding the index v to calculate K, which does match the encrypted one. Obviously, the decryption algorithm will output $\perp$.

5 Security proof

In this section, we prove our broadcast encryption with broadcaster authentication offers adaptive security in the standard model with the techniques for dual system encryption introduced by Lewko and Waters.

5.1 Semi-functional algorithms

Firstly, we detail two structures named semi-functional ciphertext and semi-functional key, which are necessary in the security proof, instead of being used in our real scheme. They are constructed with the knowledge of the secret exponents from transforming on the normal ciphertext and key.

5.1.1 Semi-functional ciphertext

The simulator executes the encryption algorithm to create the normal header $Hdr' = \left(C_0', C_1'\right)$ for authorized broadcast set S. Then it picks random exponents $x,\ z_c \in Z_n$ and sets $C_0 = C_0' \cdot R_3^{x}$, $C_1 = C_1' R_3^{x z_c}$, where R_3 denotes a generator of G_3 (the subgroup of order p_3 of $\mathbf{G}$).

5.1.2 Semi-functional key

The simulator executes the key generation algorithm to create a normal private key $sk_u' = \{D_u', \hat{D}_u', \forall_{i\in[1,2^n-1]} D_{u,i}', \hat{D}_{u,i}', E_u'\}$ for user $u \in \mathcal{ID}$. Then it picks random exponents $y_i, \hat{y}_i \in Z_n$ $(i = 1, 2, \cdots, 2^n - 1)$ and sets

$$
\begin{aligned}
D_u &= D_u' \cdot R_3^{y_u}, \\
\hat{D}_u &= \hat{D}_u' \cdot R_3^{\hat{y}_u}, \\
\forall_{i\in[1,2^n-1], i\neq u} D_{u,i} &= D_{u,i} R_3^{y_i}, \\
\forall_{i\in[1,2^n-1], i\neq u} \hat{D}_{u,i} &= \hat{D}_{u,i} R_3^{\hat{y}_i}, \\
E_u &= E_u'.
\end{aligned}
$$

The subgroup G_3 of bilinear group $\mathbf{G}$ is a semi-functional space served for security proof. The semi-functional key and ciphertext are attached with some blinding factors in

G_3. The orthogonality property of subgroups G_i for $i = 1, 2, 3$ under paring ensures the nominally semi-functionality. Technically, the attached blinding terms can be cancel out when a normal key is used to decrypt a semi-functional ciphertext. For similar reasons, the semi-functional components of a private key will not impede decryption when applied on a normal ciphertext. Otherwise, an obscured value $e(R_3, R_3)^{x\hat{y}_u\left(\sum_i^S y_i + y_v - z_c\right)}$ will be arisen from paring, which hinders decryption when $z_c \neq \sum_i^S y_i + y_v$. From the formula we could conclude that the decryption still proceed successfully if $z_c = \sum_i^S y_i + y_v$.

5.2 Proof of security

We organize the security proof of our construction as a range of distinguishable games, in which we change first the challenge ciphertext and then private keys one by one to be semi-functional. Let define the first game labeled by $Game_{Real}$ be the real broadcast encryption security game. In the last game, both challenge ciphertext and secret keys are all semi-functional. And thus, the adversary has no advantage to conquer it unconditionally.

The first game is defined as follows:

$Game_{Real}$: The actual broadcast encryption security game in defined in Section 3.2, in which all private keys and the challenge ciphertext are normal.

For t from 0 to q (the total number of key queries the attacker issues), we define $Game_t$ as:

$Game_t$: This game like a restricted real security game, and there are two exceptions compared to the real one. Firstly, the challenge ciphertext given to $\mathcal{A}$ will be a semi-functional form on the challenge authorized set S^*. Secondly, the adversary will receive semi-functional secret keys for the first t secret key queries, and receive normal secret keys for the rest of queries. Noticeable, the adversary is allowed to make at most q queries, and we will focus on the games for $Game_0, \cdots, Game_q$. The challenge ciphertext is semi-functional form and all returned secret keys for all private key queries are normal form in the $Game_0$. In the last game $Game_q$, both the challenge ciphertext and all queried private keys are semi-functional form.

$Game_{Final}$: This game is $Game_q$ except that the semi-functional challenge ciphertext is encrypted of a random message, instead of the committed two messages by the adversary $\mathcal{A}$.

In the following, we demonstrate a series of Lemmas that discuss the distinguishability of the above games.

Lemma 1 *We could construct an algorithm $\mathcal{B}$ to break* Assumption 1 *with advantage ϵ, if there is an algorithm $\mathcal{A}$ such that $Game_{Real}Adv_{\mathcal{A}} - Game_0Adv_{\mathcal{A}} = \epsilon$,.*

Proof The algorithm $\mathcal{B}$ begins by taking the received instance $\mathcal{D} = \{n, \mathbf{G}, \mathbf{G}_T, e, g_1, w_{1,1}, \cdots, w_{1,2^{n-1}}, X_2\}$ of the Assumption 1. It could executes that the **Setup**, **Secret Key Queries**, **Challenge**, **More Secret Key Queries**, **Guess** of broadcast encryption and simulate the $Game_{Real}$ and $Game_0$ with $\mathcal{A}$. □

Setup $\mathcal{B}$ picks random numbers $\alpha \in Z_n$ and sets public parameters are $\{g_1, w_{1,1}, w_{1,2}, \cdots, w_{1,2^{n-1}}, e(g_1, g_1)^{\alpha}\}$. After that, it transmits them to the adversary $\mathcal{A}$.

KeyGen $\mathcal{B}$ maintains a list $\mathcal{L}$ of $\langle u, sk_u \rangle$, which is initialized empty. If the adversary make a secret key query with an indices $\langle u, sk_u \rangle \notin \mathcal{L}$, $\mathcal{B}$ could execute the key generation algorithm **KeyGen**(msk, u) to generate user secret keys with the actual master secret key α and responses to $\mathcal{A}$ with legitimate secret keys sk_u for the queried users u. It generates invariable random numbers $a, c_1, c_2, \cdots, c_N \in Z_n$ for each user. Subsequently, $\mathcal{B}$ selects random exponents $r_u, b_i, \hat{b}_i \in Z_n$ (for $i = 1, 2, \cdots, 2^n - 1$) and sets

$$
\begin{aligned}
sk_u &= \{D_u, \hat{D}_u, \forall_{i\in[1,2^n-1]} D_{u,i}, \hat{D}_{u,i}, E_u\},\\
D_u &= g_1^{\alpha + a r_u} w_{1,u}^{r_u} X_2^{b_u},\\
\hat{D}_u &= g_1^{r_u} X_2^{\hat{b}_u},\\
\forall_{i\in[1,2^n-1], i\neq u} \quad D_{u,i} &= w_{1,i}^{r_u} X_2^{b_i},\\
\forall_{i\in[1,2^n-1], i\neq u} \quad \hat{D}_{u,i} &= h_{1,i}^{r_u} = g_1^{c_i r_u} X_2^{\hat{b}_i},\\
E_u &= h_{1,u} = g_1^{a + c_u}.
\end{aligned}
$$

After that, it inserts the generated $\langle u, sk_u \rangle$ into $\mathcal{L}$. Suppose that $\mathcal{A}$ issues a query with indices u which has queried before, $\mathcal{B}$ looks up the list $\mathcal{L}$ and responds sk_u to $\mathcal{A}$.

Challenge ciphertext The adversary $\mathcal{A}$ commits to $\mathcal{B}$ a broadcaster $v \notin S^*$, two messages M_0, M_1 and a challenge set S^*. If the indices v has been queried before, $\mathcal{B}$ looks up the list $\mathcal{L}$ to acquire sk_v. Otherwise, it generates sk_v as the above procedures. Then, it flips a cion β and computes the ciphertext as follows:

$$
\begin{aligned}
K &= e(g_1, T)^{\alpha},\\
Hdr &= (C_0, C_1)\\
&= \left(T, \left(E_v \prod_i^{S^*} w_{1,i} \right)^k \right)\\
&= \left(T, \left(g_1^{a+c_v} \prod_i^{S^*} w_{1,i} \right)^k \right),\\
C &= SymEnc(K, M_\beta).
\end{aligned}
$$

This assignment implicitly sets that g_1^k equals to the G_1 part of T. If $T \underset{\leftarrow}{R} G_{1,3}$, the generated challenge ciphertext is a semi-functional ciphertext. If $T \underset{\leftarrow}{R} G_1$, it will be distributed identically to a actual ciphertext. Thereby, $\mathcal{B}$ could distinguish between these possibilities for T with the output β' of $\mathcal{A}$ and break Assumption 1 with the same advantage ϵ of $\mathcal{A}$.

Lemma 2 *If there is an algorithm $\mathcal{A}$ that makes at most q queries such that $Game_{t-1}Adv_{\mathcal{A}} - Game_t Adv_{\mathcal{A}} = \epsilon$ for some t where $1 \leq t \leq q$. Then we could construct an algorithm $\mathcal{B}$ to break* Assumption 2 *with advantage ϵ.*

Proof The algorithm $\mathcal{B}$ begins by taking the received instance $\mathcal{D} = \{n, \mathbf{G}, \mathbf{G}_T, e, g_1, X_1X_3, X_2, Y_2Y_3, U_2U_3, V_2V_3\}$ of Assumption 2. It could execute that the **Setup**, **Secret**

Key Queries, **Challenge**, **More Secret Key Queries**, **Guess** of broadcast encryption, and we describe the concrete simulation of the $Game_{t-1}$ and $Game_t$ with the help of $\mathcal{A}$. □

Setup $\mathcal{B}$ chooses random exponents $\alpha, a_1, \cdots, a_N \in Z_n$ and defines

$$\begin{aligned} w_{1,1} &= g_1^{a_1}, \\ w_{1,2} &= g_1^{a_2}, \\ &\vdots \\ w_N &= g_1^{a_N}. \end{aligned}$$

The public parameters of the broadcast encryption system are $\{g_1, w_{1,1}, w_{1,2}, \cdots, w_{1,2^{n-1}}, e(g_1, g_1)^{\alpha}\}$, which will be sent to $\mathcal{A}$.

KeyGen A list $\mathcal{L}$ stores the tuple $\langle u, sk_u \rangle$ (sk_u is the value which respond to $\mathcal{A}$'s uth secret key query) is maintained by $\mathcal{B}$. The list is initialized empty. If $\mathcal{A}$ makes a query with a queried indices u, $\mathcal{B}$ looks up the list $\mathcal{L}$ and sends the corresponding sk_u to $\mathcal{A}$. Otherwise, $\mathcal{B}$ performs the following procedures to respond the private key queries and adds the corresponding values into $\mathcal{L}$. First of all, $\mathcal{B}$ selects random exponents $a, c_1, c_2, \cdots, c_N \in Z_n$ and sets

$$\begin{aligned} \hat{g}_1 &= g_1^{a}, \\ h_{1,1} &= g_1^{c_1}, \\ h_{1,2} &= g_1^{c_2}, \\ &\vdots \\ h_N &= g_1^{c_N}. \end{aligned}$$

Case 1 $u > t$

In such situation, the algorithm $\mathcal{B}$ will produce normal secret key for the queried user u. It could run the key generation algorithm to generate the requested keys with the actual master secret key α. Furthermore, it selects $b_i, \hat{b}_i \in Z_n$ for $i = 1, 2, \cdots, 2^n - 1$ and r_u for the queried user u, and then computes his/her secret key as follows:

$$\begin{aligned} sk_u &= \{D_u, \hat{D}_u, \forall_{i \in [1,2^n-1]} D_{u,i}, \hat{D}_{u,i}, E_u\}, \\ D_u &= g_1^{\alpha + a r_u} w_{1,u}^{r_u} X_2^{b_u}, \\ \hat{D}_u &= g_1^{r_u} X_2^{\hat{b}_u}, \\ \forall_{i \in [1,2^n-1], i \neq u} \quad D_{u,i} &= w_{1,i}^{r_u} X_2^{b_i}, \\ \forall_{i \in [1,2^n-1], i \neq u} \quad \hat{D}_{u,i} &= h_{1,i}^{r_u} X_2^{\hat{b}_i}, \\ E_u &= \hat{g}_1 h_{1,u} = g_1^{a + c_u}. \end{aligned}$$

Case 2 $u < t$

In such situation, the algorithm $\mathcal{B}$ should produce the semi-functional private key queried user u. $\mathcal{B}$ picks random exponents $b_i, \hat{b}_i \in Z_n$ for $i = 1, 2, \cdots, 2^n - 1$ and $r_u \in Z_n$ for the queried user u, then it computes:

$$\begin{aligned}
sk_u &= \{D_u, \hat{D}_u, \forall_{i\in[1,2^n-1]} D_{u,i}, \hat{D}_{u,i}, E_u\},\\
D_u &= g_1^{\alpha+ar_u} w_{1,u}^{r_u} (Y_2Y_3)^{b_u},\\
\hat{D}_u &= g_1^{r_u} (Y_2Y_3)^{\hat{b}_u},\\
\forall_{i\in[1,2^n-1],i\neq u}\ D_{u,i} &= w_{1,i}^{r_u} (U_2U_3)^{b_i},\\
\forall_{i\in[1,2^n-1],i\neq u}\ \hat{D}_{u,i} &= h_{1,i}^{r_u} (V_2V_3)^{\hat{b}_i},\\
E_u &= \hat{g}_1 h_{1,u} = g_1^{a+c_u}.
\end{aligned}$$

This assignment implicitly sets that $r_3^y = (Y_3)^{y_u}$.

Case 3 $u = t$

In such situation, $\mathcal{B}$ will produce a nominally semi-functional secret key for the queried user u. It does this by computing:

$$\begin{aligned}
sk_t &= \{D_t, \hat{D}_t, \forall_{i\in[1,2^n-1]} D_{t,i}, \hat{D}_{t,i}, E_t\},\\
D_t &= g_1^{\alpha} T^{a+a_t}\\
\hat{D}_t &= T,\\
\forall_{i\in[1,2^n-1],i\neq u} D_{t,i} &= T^{a_i},\\
\forall_{i\in[1,2^n-1],i\neq u} \hat{D}_{t,i} &= T^{b_i},\\
E_u &= \hat{g}_1 h_{1,u} = g_1^{a+c_u}.
\end{aligned}$$

Challenge ciphertext $\mathcal{B}$ is given a committed broadcaster $v \notin S^*$, two messages M_0, M_1 and a challenge set S^*. Then it looks up the list $\mathcal{L}$ to examine the indices v is queried before. If so, $\mathcal{B}$ extracts the corresponding secret key sk_v; otherwise, it produces sk_v according to the aforementioned steps. Finally, it picks $\beta \in \{0, 1\}$ randomly and calculates the ciphertext as follows:

$$\begin{aligned}
K &= e(X_1X_3, g_1)^{\alpha},\\
Hdr &= (C_0, C_1)\\
&= \left(X_1X_3, (X_1X_3)^{a+c_v+\sum_i^{S^*} a_i} \right),\\
C &= SymEnc(K, M_\beta).
\end{aligned}$$

This implicitly sets g_1^k is equal to $R_3^{xz_c} = X_3^{\sum_i^{S^*} a_i + c_v}$ and X_1. If $z_c = \sum_i^{S^*} a_i + c_v$, the nominally semi-functional formed secret key could decrypt this ciphertext successfully, and

the simulator $\mathcal{B}$ could not examine whether the secret key of user t is semi-functional form or not. That is, $\mathcal{B}$ has to produce the nominally semi-functional key sk_t.

If $T \in G_{1,2}$, $\mathcal{B}$ has properly simulated $Game_{t-1}$. If $T \in \mathbf{G}$, it means that $\mathcal{B}$ has properly simulated $Game_t$. From the received guess of β from $\mathcal{A}$, $\mathcal{B}$ can distinguish between these possibilities for T.

Lemma 3 *We could construct an algorithm $\mathcal{B}$ to break* Assumption 3 *with advantage ϵ, if there is an algorithm $\mathcal{A}$ such that $Game_q Adv_{\mathcal{A}} - Game_{Final} Adv_{\mathcal{A}} = \epsilon$.*

Proof The challenge ciphertext and the queried private keys are all semi-functional in both these two games. $\mathcal{B}$ begins by taking the received instance $\mathcal{D} = \{n, \mathbf{G}, \mathbf{G}_T, e, g_1, g_1^{\alpha} X_3, X_2, g_1^{k} Y_3, H_3\}$ of Assumption 3. It could executes the **Setup**, **Secret Key Queries**, **Challenge**, **More Secret Key Queries**, **Guess** of broadcast encryption, and we describe the concrete simulation of $Game_q$ and $Game_{Final}$ with the help of $\mathcal{A}$. □

Setup $\mathcal{B}$ begins by picking random exponents $a_1, \cdots, a_N \in Z_n$ and defines

$$\begin{aligned} e(g_1, g_1)^{\alpha} &= e\left(g_1, g_1^{\alpha} X_3\right), \\ w_{1,1} &= g_1^{a_1}, \\ w_{1,2} &= g_1^{a_2}, \\ &\vdots \\ w_N &= g_1^{a_N}. \end{aligned}$$

The public parameters of the broadcast encryption system are $\{g_1, \hat{g}_1, w_{1,1}, w_{1,2}, \cdots, w_{1,2^{n-1}}, e(g_1, g_1)^{\alpha}\}$. $\mathcal{B}$ will transmit them to $\mathcal{A}$. From the above formulas, we could conclude that $\mathcal{B}$ does not possess the master secret key α.

KeyGen Similar to the above proof, $\mathcal{B}$ also maintains a list $\mathcal{L}$ (which is initialized empty) to store the tuple $\langle u, sk_u \rangle$. If the queried indices u exits in $\mathcal{L}$, $\mathcal{A}$ will receive the corresponding sk_u; otherwise, he/she will receive the calculated semi-functional private key, which will be added in $\mathcal{L}$ in the form of $\langle u, sk_u \rangle$. Noticeably, in this game, all the returned secret keys are all semi-functional. Firstly, $\mathcal{B}$ selects random exponents $a, c_1, c_2, \cdots, c_N \in Z_n$ and sets

$$\begin{aligned} \hat{g}_1 &= g_1^{a}, \\ h_{1,1} &= g_1^{c_1}, \\ h_{1,2} &= g_1^{c_2}, \\ &\vdots \\ h_N &= g_1^{c_N}. \end{aligned}$$

When a request for user u's key is made, $\mathcal{B}$ chooses random exponents $b_i, \hat{b}_i \in Z_n$ for $i = 1, 2, \cdots, 2^n - 1$ and r_u for the queried user u and sets:

$$\begin{aligned} sk_u &= \left\{ D_u, \hat{D}_u, \forall_{i\in[1,2^n-1]} D_{u,i}, \hat{D}_{u,i}, E_u \right\}, \\ D_u &= g_1^{\alpha} X_3 w_{1,u}^{r_u} (X_2 U_3)^{b_u}, \\ \hat{D}_u &= g_1^{r_u} (X_2 U_3)^{\hat{b}_u}, \\ \forall_{i\in[1,2^n-1],i\neq u} \quad D_{u,i} &= w_{1,i}^{r_u} (X_2 H_3)^{b_i}, \\ \forall_{i\in[1,2^n-1],i\neq u} \quad \hat{D}_{u,i} &= h_{1,i}^{r_u} (X_2 V_3)^{\hat{b}_i}, \\ E_u &= \hat{g}_1 h_{1,u} = g_1^{a+c_u}. \end{aligned}$$

Challenge ciphertext $\mathcal{B}$ receives a committed broadcaster $v \notin S^*$, a challenge set S^* and two messages M_0, M_1 from the attacker. $\mathcal{B}$ will create a secret key for broadcaster v or extracts the corresponding secret key from $\mathcal{L}$ according to whether the indices v has been queried before or not. The produced challenge ciphertext is a semi-functional formed ciphertext of either M_β or a random message depending on T. It flips a coin and chooses $\beta \in \{0, 1\}$ randomly. Finally, it forms the challenge ciphertext as follows:

$$\begin{aligned} K &= T, \\ Hdr &= (C_0, C_1) \\ &= \left(g_1^k Y_3, \left(g_1^k Y_3 \right)^{a+c_v+\sum_i^{S^*} a_i} \right) \\ C &= SymEnc(K, M_\beta). \end{aligned}$$

We implicitly set $Y_3^{xz_c} = Y_3^{a+c_v+\sum_i^{S^*} a_i}$. Suppose that T is a random element of $\mathbf{G}_{n+1}$, the generated ciphertext is a semi-functional formed ciphertext based on a random message. If $T = e(g, g)^{\alpha k}$, the generated one is a properly distributed semi-functional ciphertext with message M_β. Therefore, $\mathcal{B}$ could distinguish between these possibilities for T from the received $\mathcal{A}$' guess of β.

Theorem 1 *If all of* Assumption 1, 2, *and* 3 *hold, then our broadcast encryption system with broadcaster authentication is secure.*

Proof The final game $Game_{Final}$ information theoretically hide the value of β from the adversary $\mathcal{A}$, he/she has no advantage to compromise the construction of broadcast encryption. We also present the demonstration of a sequence of Lemmas which prove that the real security game $Game_{Real}$ is indistinguishable from $Game_{Final}$ based on the Assumption 1, 2, 3. If these three assumptions hold, we could conclude that the advantage of adversary to compromise the game $Game_{Real}$ is negligibly close to 0. □

6 Performance and functionality evaluation

In this section, we present performance and functionality evaluation analysis of the proposed construction and other related solutions in the field of broadcast encryption [3, 15, 17, 25,

Table 1 Comparison

Scheme	Function	Ciphertext size	Public key size	Private key size	Security
Trivial	*	$O(\mid S \mid)$	$O(N)$	$O(1)$	Adaptive
BGW05 [3]	*	$O(1)$	$O(N)$	$O(1)$	Static
	*	$O(\sqrt{N})$	$O(\sqrt{N})$	$O(1)$	Static
GW09 [15]	*	$O(\sqrt{S})$	$O(\sqrt{\ell})$	$O(1)$	Semi-static
W09 [32]	*	$O(1)$	$O(N)$	$O(N)$	Adaptive
MSLR04 [25]	Broadcaster authentication	$O(\|S\|)$	$O(1)$	$O(1)$	Static
SVGK08 [30]	Broadcaster authentication	$O(\|S\|)$	$O(1)$	$O(1)$	Adaptive
PHHY12 [27]	Broadcaster authentication	$O(\tau\omega)$	$O(1)$	$O(1)$	Static
GWJZL19 [17]	Broadcaster authentication	$O(1)$	$O(N)$	$O(N)$	Static
Ours	Broadcaster authentication	$O(1)$	$O(N)$	$O(N)$	Adaptive

N: The number of users in the system; $\mid S \mid$: The size of the target set S; ℓ: The maximum number of receivers; $*$: It could not provide the function; τ: The stateless duration ω: The threshold

27, 30, 32]. Table 1 shows the classified comparisons in terms of function, ciphertext size, public key size, private key size and security.

Ciphertext size is the amount of information which should be transmitted in addition to the description of the recipient set and the symmetric encryption of the broadcasted plaintext, it is the most critical efficiency aspect for broadcast encryption systems. It is optimized for such a system with constant ciphertext size. Literally, the public key and private key size mean the number of contained group elements, respectively. The sizes of public key and private key are also important measures to evaluate the storage consumption of broadcast encryption systems. From Table 1, we could see that only Guo et al.'s proposal [17] achieves $O(1)$ ciphertext size and possesses the broadcaster authentication, simultaneously. However, their scheme is proved secure in the weaker static model. Our construction achieves the adaptive security based on static and simple assumptions in the standard model, meanwhile preserving optimal ciphertext overhead. This system has longer user secret keys, however it could realize the broadcaster authentication and has a tighter security proof in generic bilinear groups.

The time consumption for computing $\prod_{i}^{S} w_{1,i}$ with $\mid S \mid$ group operations and $\prod_{i \neq u}^{S} D_{u,i}$ with $\mid S \mid -1$ group operations determines the computation efficiency of encryption and decryption algorithm, respectively. The broadcaster executes the encryption algorithm, for example, he/she could re-use the computed value $\sigma = \prod_{i}^{\hat{S}} w_{1,i}$ for authorized set $\hat{S}$ which in prior broadcast, and compute $\prod_{i}^{S} w_{1,i}$ with just δ group operations using the cached value σ, where δ is the size of the set difference between S and S' (the receiver set $\hat{S}$ that is similar to S). The aforementioned precomputation procedures could bring down the computation consumption of encryption and decryption algorithm greatly.

7 Conclusion

The public key broadcast encryption system with broadcaster authentication possesses a supervised broadcast strategy, each one is responsible for his/her distributed content. In this

paper, we formally define the notion for a public key broadcast encryption system with authenticated broadcaster and formalize the adaptive security definition in the system. Next, we devise a construction to attain meaningful guarantees of authenticated broadcaster in the composite order bilinear groups. In our constructions for N users, the ciphertext size is of $O(1)$ (only constant number of group elements). The public key size and user private key size are of $O(N)$. Next, we prove the adaptive security of our scheme in the standard model under static general subgroup decisional assumptions using the methodology of dual system encryption. Finally, the performance and functionality evaluations with other solutions shows that our constructions achieves adaptive security with tighter reductions, while preserving optimal ciphertext overhead. In the future work, devising constructions for authenticated broadcast encryption system with logarithmic public key size and user private key (rather than $O(N)$) size is very meaningful.

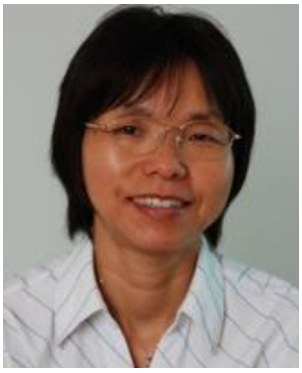
Acknowledgments The authors are grateful to the editor and anonymous reviewers for their valuable suggestions. This work is supported by NSFC (Grant Nos. 61502044), the Fundamental Research Funds for the Central Universities (Grant No. 2015RC23).

References

1. Bellare M, Waters B, Yilek S (2011) Identity-based encryption secure against selective opening attack. In: Proc. conference on theory of cryptography. Springer, Providence, USA, pp 235–252
2. Boneh D, Franklin M (2001) Identity based encryption from the weil pairing. In: Advances in cryptology-CRYPTO 2001. Springer, pp 213–229
3. Boneh D, Gentry C, Waters B (2005) Collusion resistant broadcast encryption with short ciphertexts and private keys. Springer, Advances in cryptology-CRYPTO 2005, pp 258–275
4. Boneh D, Sahai A, Waters B (2006) Fully collusion resistant traitor tracing with short ciphertexts and private keys. In: Advances in cryptology-EUROCRYPT 2006. Springer, pp 573–592
5. Boneh D, Silverberg A (2003) Applications of multilinear forms to cryptography. Contemporary Mathematics 324(1):71–90
6. Boneh D, Waters B (2006) A fully collusion resistant broadcast, trace, and revoke system. In: Proc. 13th ACM conference on computer and communications security. ACM, pp 211–220
7. Boneh D, Waters B, Zhandry M ((2014)) Low overhead broadcast encryption from multilinear maps. In: Advances in cryptology-CRYPTO 2014. Springer, pp 206–223
8. Boneh D, Zhandry M (2014) Multiparty key exchange, efficient traitor tracing, and more from indistinguishability obfuscation. In: Advances in cryptology-CRYPTO 2014. Springer, pp 480–499
9. Coron JS, Lepoint T, Tibouchi M (2013) Practical multilinear maps over the integers. In: Advances in cryptology-CRYPTO 2013, pp 476–493
10. Delerablée C (2007) Identity-based broadcast encryption with constant size ciphertexts and private keys. In: Advances in cryptology-ASIACRYPT 2007. Springer, pp 200–215
11. Du X, Wang J, Ge J, Wang Y (2005) An ID-based broadcast encryption scheme for key distribution. IEEE Trans Broadcast 51(2):264–266
12. Fiat A, Naor M (1993) Broadcast encryption. In: Advances in cryptology-CRYPTO 1993. Springer, pp 480–491
13. Garg S, Gentry C, Halevi S (2013) andidate multilinear maps from ideal lattices. In: Advances in cryptology-EUROCRYPT 2013. Springer, pp 1–17
14. Garg S, Kumarasubramanian A, Sahai A, Waters B (2010) Building efficient fully collusion-resilient traitor tracing and revocation schemes. In: Proc. 17th ACM conference on Computer and communications security. ACM, pp 121–130
15. Gentry C, Waters B (2009) Adaptive security in broadcast encryption systems (with short ciphertexts). In: Advances in cryptology-EUROCRYPT 2009. Springer, pp 171–188
16. Goodrich MT, Sun JZ, Tamassia R (2004) Efficient tree-based revocation in groups of low-state devices. In: Advances in cryptology-CRYPTO 2004. Springer, pp 511–527
17. Guo D, Wen Q, Jin Z, Zhang H, Li W (2019) Authenticated public key broadcast encryption with short ciphertexts. Multimed Tools Appl. https://doi.org/10.1007/s11042-019-7598-0

18. Guo D, Wen Q, Li W, Zhang H, Jin Z (2016) Adaptively secure broadcast encryption with constant ciphertexts. IEEE Trans Broadcast 62(3):709–715
19. Hu Y, Jia H (2016) Cryptanalysis of GGH map. In: Advances in cryptology-EUROCRYPT 2016. Springer, pp 537–565
20. Kim K, Susilo W, Ho Au M, Seberry J (2015) Adaptively secure identity-based broadcast encryption with a constant-sized ciphertext. IEEE Trans Inform Forensics Secur 10(3):679–693
21. Lewko A, Sahai A, Waters B (2010) Revocation systems with very small private keys. In: Proc. IEEE symposium on security and privacy 2010. IEEE, pp 273–285
22. Lewko A, Waters B (2010) New techniques for dual system encryption and fully secure HIBE with short ciphertexts. In: Proc. theory of cryptography 2010. Springer, pp 455–479
23. Li F, Xin X, Hu Y (2008) Identity-based broadcast signcryption. Comput Standards Interfaces 30(1):89–94
24. Liu W, Liu J, Wu Q, Qin B, Li Y (2016) Practical chosen-ciphertext secure hierarchical identity-based broadcast encryption. Int J Inform Secur 15(1):35–50
25. Mu Y, Susilo W, Lin Y, Ruan C (2004) Identity-based authenticated broadcast encryption and distributed authenticated encryption. In: Proc. of 9th Asian computing science conference ASIAN 2004. Springer, pp 169–181
26. Nishimaki R, Wichs D, Zhandry M (2016) Anonymous traitor tracing: how to embed arbitrary information in a key. In: Advances in cryptology-EUROCRYPT 2016. Springer, pp 388–419
27. Park C, Hur J, Hwang S, Yoon H (2012) Authenticated public key broadcast encryption scheme secure against insiders attack. Mathem Comput Modell 55(1):113–122
28. Park JH, Rhee HS, Dong HL (2011) Fully collusion-resistant trace-and-revoke scheme in prime-order groups. J Commun Netw 13(5):428–441
29. Qin C, Zhou Q, Cao F, Dong J, Zhang X (2018) Flexible lossy compression for selective encrypted image with image in painting. IEEE Trans Circ Sys Video Technol: 1–1. https://doi.org/10.1109/TCSVT.2018.2878026
30. Selvi SSD, Vivek SS, Gopalakrishnan R, Karuturi NN, Rangan CP (2008) Cryptanalysis of Mu, et al., and Li et al. schemes and a provably secure id-based broadcast signcryption (IBBSC) scheme. In: International workshop on information security applications 2008. Springer, pp 115–129
31. Sun M, Ge C, Fang L, Wang J (2017) A proxy broadcast re-encryption for cloud data sharing. Multimed Tools Appl 77(9):10455–10469
32. Waters B (2009) Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions. In: Advances in cryptology-CRYPTO 2009. Springer, pp 619–636
33. Zhandry M (2014) Adaptively secure broadcast encryption with small system parameters. IACR Cryptology ePrint Archive 757. http://eprint.iacr.org/2014/757
34. Zhang L, Hu Y, Wu Q (2012) Adaptively secure identity-based broadcast encryption with constant size private keys and ciphertexts from the subgroups. Math Comput Modell 55(1-2):12–18

Dianli Guo received the B.S. degree in Math and Applied Math from Heze College in 2011 and M.S. degree in Applied Math from University of Jinan in 2014 respectively, and the Ph.D degree in Cryptography from Beijing University of Posts and Telecommunications in 2018. Now he is a R &D engineer of National Computer System Engineering Research Institute of China. His research interests include cryptography, information security and mobile communications security.



Qiaoyan Wen received the B.S. and M.S. degrees in Mathematics from Shaanxi normal University, Xi'an, China, in 1981 and 1984, respectively, and the Ph.D degree in cryptography from Xidian University, Xi'an, China, in 1997. She is a professor of Beijing University of Posts and Telecommunications. Her present research interests include coding theory, cryptography, information security, internet security and applied mathematics.

Wenmin Li received the B.S. and M.S. degrees in Mathematics and Applied Mathematics from Shaanxi Normal University, Xi'an, Shaanxi, China, in 2004 and 2007, respectively, and the Ph.D. degree in Cryptology from Beijing University of Posts and Telecommunications, Beijing, China, in 2012. She is lecturer in Beijing University of Posts and Telecommunications, Beijing, China. Her research interests include cryptography and information security.

Hua Zhang received the BS degree in telecommunications engineering from the Xidian University in 1998, the MS degree in cryptology from Xidian University in 2005, and the Ph.D degree in cryptology from Beijing University of Posts and Telecommunications in 2008. Now she is an associate professor of Beijing University of Posts and Telecommunications. Her research interests include cryptography, information security and network security.

Zhengping Jin received the BS degree in Math and Applied Math, MS degree in Applied Math from Anhui Normal University in 2004 and in 2007 respectively, and the Ph.D degree in Cryptography from Beijing University of Posts and Telecommunications in 2010. Now he is a lecturer of Beijing University of Posts and Telecommunications. His research interests include cryptography, information security, internet security and applied mathematics.

Affiliations

Dianli Guo[1,2] · Qiaoyan Wen[1] · Wenmin Li[1] · Hua Zhang[1] · Zhengping Jin[1]

Dianli Guo
guodianli@163.com

Qiaoyan Wen
wqy@bupt.edu.cn

Wenmin Li
liwenmin02@outlook.com

Zhengping Jin
zhpjin@bupt.edu.cn

1 State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China

2 The 6th Research Institute of China Electronics Corporation, Beijing, 100083, China