1-1-2014

Efficient semi-static secure broadcast encryption scheme

Jongkil Kim
University of Wollongong, jk057@uowmail.edu.au

Willy Susilo
University of Wollongong, wsusilo@uow.edu.au

Man Ho Allen Au
University of Wollongong, aau@uow.edu.au

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

Efficient semi-static secure broadcast encryption scheme

Abstract

In this paper, we propose a semi-static secure broadcast encryption scheme with constant-sized private keys and ciphertexts. Our result improves the semi-static secure broadcast encryption scheme introduced by Gentry and Waters. Specifically, we reduce the private key and ciphertext size by half. By applying the generic transformation proposed by Gentry and Waters, our scheme also achieves adaptive security. Finally, we present an improved implementation idea which can reduce the ciphertext size in the aforementioned generic transformation.

Keywords

scheme, encryption, static, broadcast, semi, secure, efficient

Publication Details

Kim, J., Susilo, W., Au, M. & Seberry, J. (2014). Efficient semi-static secure broadcast encryption scheme. Lecture Notes in Computer Science, 8365 62-76.

Efficient Semi-static Secure Broadcast Encryption Scheme

Jongkil Kim, Willy Susilo, Man Ho Au, and Jennifer Seberry

Centre for Computer and Information Security Research
School of Computer Science and Software Engineering
University of Wollongong, Australia
jk057@uowmail.edu.au, {wsusilo,aau,jennie}@uow.edu.au

Abstract. In this paper, we propose a semi-static secure broadcast encryption scheme with constant-sized private keys and ciphertexts. Our result improves the semi-static secure broadcast encryption scheme introduced by Gentry and Waters. Specifically, we reduce the private key and ciphertext size by half. By applying the generic transformation proposed by Gentry and Waters, our scheme also achieves adaptive security. Finally, we present an improved implementation idea which can reduce the ciphertext size in the aforementioned generic transformation.

Keywords: semi-static, broadcast encryption, constant size

1 Introduction

A broadcast encryption [7] is a cryptographic primitive that allows a sender to encrypt a message to a set of users so that only the users within that set can decrypt it and obtain the message. In addition, the set of receivers is not fixed and an arbitrary set of users can be chosen by the sender at the time of encryption. Broadcast encryption is suggested as being efficient in a system having a large number of group members, and it also has many practical applications such as its use in secure database system, DRM (digital right management) and group communications. In a broadcast encryption system, any subset of users can be included in a broadcast, but decryption of the chiphertexts is only possible for users included in the broadcast using their own private keys.

There are many desirable properties of broadcast encryption. It can be *fully collusion resistant*, which means that a ciphertext cannot be decrypted even if all users who are not included in the broadcast encryption collude. This is an essential property of a secure broadcast encryption. Having *stateless receivers* [15] is another desirable property. In a broadcast encryption with stateless receivers, any set of receivers can be included in a broadcast encryption without requiring any update of private keys.

Multi-receiver key encapsulation [22] (mKEM) is a key encapsulation scheme, which allows multiple parties to share a secret key efficiently, and the notion

of mKEM has been extended to multi-receiver identity-based key encapsulation [1] [2] (mID-KEM) by combining it with an identity-based encryption [20].

Identity-based broadcast encryption [5, 19] is a combination of broadcast encryption and identity-based encryption. Although it shares many similar concepts with mID-KEM, an identity-based broadcast encryption focuses more on a broadcast encryption as a generalization of an identity-based encryption. This means that an identity-based encryption is a special case of an identity-based broadcast encryption with a single receiver in the broadcast. In an identity-based broadcast encryption, encryptions and decryptions are based on receivers' identities, in which the recipients in a normal broadcast encryption are usually indexed sequentially from 1 to n. The most important difference between broadcast encryption and identity-based broadcast encryption is the number of users in the system. Identity-based broadcast encryptions are usually designed to support exponentially many users since user identities are merely bit-strings of arbitrary-size and hence, they are unknown during the system setup.

Adaptive security, also known as *full security*, of a broadcast encryption was introduced by Gentry and Waters [9]. In this security model, an adversary can adaptively select a target set by using public parameters and previously compromised private keys. *Static security*, as defined by [3], is a weaker version of adaptive security of a broadcast encryption. In the static security model, an adversary must declare the target set he/she wants to attack before observing public parameters. A *Semi-static security* model [9] is half-way between a static and an adaptive security model. Similar to the case in a static security model, an adversary is still required to declare a potential target set prior to setting public keys in a semi-static security model. However, the adversary can select any target set to be challenged, provided that the target set is a subset of the previously declared potential target set.

In this paper, we improve the semi-static secure broadcast encryption of Gentry and Waters. As in Gentry and Waters' scheme, our scheme offers semi-static security and is fully collusion-resistant. In addition, receivers are stateless receivers, and the sizes of the public key and the private key do not depend on the total number of users. Our scheme also features very short private keys and ciphertexts and is computationally more efficient than Gentry and Waters' scheme. Based on the transformation technique from [9], our scheme can achieve adaptive security while maintaining efficiency.

The rest of this paper is organized as follows. In the next section, we will review some related work. We will highlight our contributions and compare them to existing schemes in the literature. In Section 3, we will review some definitions and complexity assumptions that will be used throughout the paper. In Section 4, we will first describe semi-static secure broadcast encryption and subsequently revisit the construction by Gentry and Waters. In Section 5, we will present our construction that will improve Gentry and Waters' scheme, together with its security analysis. In Section 6, we will present the transformation of our scheme to achieve adaptive security, following the transformation technique from [9]. We will also present a technique in the implementation of the scheme to remove

the linear-sized tag required in the generic transformation. Finally, Section 7 concludes the paper.

2 Related works

Since the introduction of broadcast encryption as a revocation system [15], a number of several fully collusion resistant broadcast encryption schemes have been proposed. [6, 10, 11] A fully collusion resistant broadcast encryption scheme which has short ciphertext was proposed by Boneh, Gentry and Waters (BGW) [3]. They introduced a broadcast encryption scheme with a constant size private key and ciphertext in the static security model, then generalized it to achieve $O(\sqrt{n})$ size ciphertext. As a compensation for generalization, they reduced the size of the public key from $O(n)$ to $O(\sqrt{n})$. A similar achievement in identity-based broadcast encryption scheme was introduced Delerablée [5]. Delerablée's work offers constant size private keys and ciphertexts, and it supports exponentially many identities in the random oracle model.

Gentry and Waters [9] considered adaptive security from a different approach. They first introduced semi-static security, in which efficient schemes can be constructed. Then, they presented a generic transformation to achieve adaptive security with only a small impact on the ciphertext size. Specifically, the resulting ciphertext size is doubled and a component, called a 'tag' is added, which has a space complexity of $O(|S|)$ where S is the set of receivers of a broadcast. For a normal broadcast encryption, this tag is of $|S|$-bit and can be removed in the random oracle model. In addition, they introduced two broadcast encryption schemes that satisfy semi-static security. Both of the schemes have constant sized ciphertext. In contrast, the first scheme has $O(n)$ private key size, while the second scheme has a constant size private key.

A *revocation system* [15, 16] where only non-revoked users can decrypt ciphertexts is a type of broadcast encryption system and is comparable to semi-static broadcast encryption. Indeed, the selective secure revocation system and semi-static broadcast encryption offer similar functions when the encrypter in the semi-static broadcast encryption only chooses the set of non-revoked users to be included in the broadcast. However, it seems that Gentry and Waters' technique is not applicable to transform selectively secure revocation to offer adaptive security, as noted in [13].

Although our scheme and [9] can achieve adaptive security in broadcast encryption, it is only adaptive chosen plaintext attack (CPA) secure. Recently, a few adaptively chosen ciphertext attack (CCA) secure schemes were introduced, including the schemes by Malek and Miri [14] and Ren and Gu [18], which feature constant size ciphertexts and private keys of size $O(n)$. In addition, Phan et al. [17] suggested a broadcast encryption scheme with constant size private key and ciphertext under a non standard assumption.

2.1 Our Contributions

Compared with Gentry and Waters' semi-static broadcast encryption scheme with constant size private key and ciphertext (denoted as GW_{SS} throughout this paper), our construction offers a reduced-size private key and ciphertext. Also, in terms of computation, the number of pairing and exponentiation computations are reduced. While several adaptively secure broadcast encryption schemes have been introduced recently, our semi-static secure scheme is still important because a semi-static secure broadcast encryption scheme can be transformed into an adaptively secure broadcast encryption scheme. We compare the efficiency of our scheme with other broadcast encryption schemes in Table 1. Our scheme is quite competitive when we consider both efficiency and security. The only scheme offering better efficiency is the broadcast encryption scheme that was suggested by Phan et al. [17]. Unfortunately, this scheme is based on a non-standard assumption.

Table 1. Comparison of efficiency and security of Broadcast Encryption schemes

	Pub. Key	Priv. Key	Ciphertext	Pairing	Exponentiation	Security
MM [14]	$O(n)$	$O(n)$	$O(1)$	0/2	$O(\|S\|)/O(\|S\|)$	ACCA
RG [18]	$O(n)$	$O(n)$	$O(1)$	3/3	$O(\|S\|)/O(1)$	ACCA
PPSS [17]	$O(n)$	$O(1)$	$O(1)$	1/2	$O(1)/O(1)$	ACCA
CD[b] [5]	$O(\ell)$	$O(1)$	$O(1)$	0/2	$O(\|S\|)/O(\|S\|)$	SCCA
BGW [3]	$O(n)$	$O(1)$	$O(1)$	1/2	$O(1)/O(1)$	SCCA
GW_{SS} [9]	$O(\ell)$	O(1)	O(1)	2/2	$O(\ell)/O(\ell)$	SSCPA
GW^{a}_{SS} [9]	$O(\ell)$	$O(1)$	$O(\|S\|)$	4/2	$O(\ell)/O(\ell)$	ACPA
GW_{IBBE} [9]	$O(\sqrt{\|S\|})$	$O(1)$	$O(\sqrt{\|S\|})$	$O(\sqrt{\|S\|})/2$	$O(\|S\|)/O(\sqrt{\|S\|})$	ACPA
Our scheme	$O(\ell)$	$O(1)$	$O(1)$	1/2	$O(\ell)/O(\ell)$	SSCPA
Our scheme[a]	$O(\ell)$	$O(1)$	$O(1)$ *or* $O(\ell)$	2/2	$O(\ell)/O(\ell)$	ACPA

[a] An adaptively secure scheme transformed from semi-static secure schemes
[b] In the random oracle model

3 Definitions and Complexity Assumptions

3.1 Broadcast Encryption System

For simplicity, the definition of a broadcast encryption system is often replaced by a key encapsulation system. Through a key encapsulation system, multiple receivers participating in a broadcast share a symmetric key for further secure communications. We introduce the definition of a semi-static broadcast encryption system, which is useful to understand our scheme, based on the definition of an adaptively secure broadcast encryption system [9]. It consists of four algorithms, setup (**Setup**), private key generation (**KeyGen**), encapsulation (**Enc**), and decapsulation (**Dec**) as defined below.

Setup(λ, n, ℓ) takes as input the number of receivers (n) and the maximal size of a broadcast recipient group ℓ ($\leq n$). It outputs a public/master secret key pair $\langle PK, MSK\rangle$.

KeyGen(i, MSK) takes as input an index $i \in \{1, ..., n\}$ and the secret key MSK. It outputs a private key d_i.

Enc(S, PK) takes as input a subset $S \subseteq \{1, ..., n\}$, a public key PK and a message M to encrypt. If $|S| \leq \ell$, it outputs a pair $\langle Hdr, K\rangle$ where Hdr is called the header and $K \in \mathcal{K}$ is a message encryption key.

Dec(S, i, d_i, Hdr, PK) takes as input a subset $S \subseteq \{1, ..., n\}$ an index $i \in \{1, ..., n\}$, a private key d_i for i, a header Hdr, and the public key PK. If $|S| \leq \ell$ and $i \in S$, then the algorithm outputs the message encryption key $K \in \mathcal{K}$.

Correctness Property. For the correctness, the following property must be satisfied.

For $S = \{1, ..., n\}$ where $|S| \leq \ell \leq n$, let $(PK, SK_1, ..., SK_n) \leftarrow Setup(\lambda, n, \ell)$, and $\langle Hdr, K\rangle \leftarrow Enc(S, PK)$. Then, if $i \in S$, $Dec(S, i, d_i, Hdr, PK) = K$.

It should be noted that the definition of a semi-static secure broadcast encryption system above can be easily extended to encrypt messages using the standard key encapsulation mechanism/data encapsulation mechanism (KEM/DEM) transformation [21] [4].

3.2 Bilinear Maps

Let p be a large prime number. Let $\mathbb{G}_1$, $\mathbb{G}_2$ be two groups of order p, and g be a generator of $\mathbb{G}_1$. $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is a bilinear map satisfying the following properties:

1. Bilinearity: For all, $u, v \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}, e(u^a, u^b) = e(u, v)^{ab}$.
2. Non-degeneracy: $e(g, g) \notin 1$.
3. Computability: There exists an efficient algorithm to compute $e(u, v), \forall u, v \in \mathbb{G}_1$.

3.3 Complexity Assumptions

Definition 1. ***(The Decision Bilinear Diffie-Hellman Exponent (DBDHE) Sum Problem for (S, m))****[8] Fix $S \subset \mathbb{Z}$ and $m \in Z \setminus (S + S)$. Let $\mathbb{G}$ and $\mathbb{G}_T$ be groups of order p with bilinear map $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_T$, and let g be a generator for $\mathbb{G}$. Set $\alpha \leftarrow \mathbb{Z}_p^*$ and $b \leftarrow \{0, 1\}$. If $b = 0$, set $Z \leftarrow e(g, g)^{\alpha^m}$;otherwise, set $Z \leftarrow \mathbb{G}_T$. Output*

$$\{g^{\alpha^i} : i \in S\} \text{ and } Z$$

The problem is to guess b. The specific BDHE Sum instance we use in our security analysis is for $m = 4d + 4\ell - 1$ and

$$S = [0, \ell - 2] \cup [d + \ell, 2d + \ell - 1] \cup [2d + 2\ell, 2d + 3\ell - 1]$$

$$\cup[3d+3\ell, 4d+3\ell] \cup [4d+4\ell, 5d+4\ell+1]$$

where $d = n + 2\ell$.

Also, we define $AdvBDHES_{\mathcal{A},n,\ell}(\lambda)$ as the advantage of an algorithm $\mathcal{A}$ to solve the decision BDHE Sum problem as defined above.

$$AdvBDHES_{\mathcal{A},n,\ell}(\lambda) = |Pr[b = b'] - 1/2|.$$

4 Semi-static Secure Broadcast Encryption

4.1 Security Definition

Static secure broadcast encryption is a weaker notion of adaptively secure broadcast encryption. In a static secure broadcast encryption, the adversary must declare the target set he/she wants to attack before **Setup**, and ask a challenge against exactly the same target set in **Challenge**. Semi-static secure broadcast encryption is in between static security and adaptive security. In a semi-static secure broadcast encryption, the adversary must also let the challenger know the target set before **Setup** in the same way that static secure requires, but the adversary makes a challenge for any subsets of the target set which the adversary has declared. We review the definition given in Gentry and Waters [9], which is a game between the challenger and the adversary.

Both the adversary and the challenger are given as input ℓ, i.e., the maximal size of a set of receivers S.

Init: The adversary $\mathcal{A}$ first out a set $S^* \subseteq \{1, ..., n\}$ of identities that he/she wants to attack (with $|S| \leq \ell$), and let k = $|S|$.

Setup: The challenger runs **Setup**(λ, ℓ) to obtain a public key PK. He/she gives $\mathcal{A}$ the public key PK.

Extract: The adversary $\mathcal{A}$ adaptively issues queries $q_1, ..., q_{n-k}$, where q_i is that the challenger runs **KeyGen** on ith element of $S^{*c} = \{1, ..., n\} - S^*$ and forwards the resulting private key to the adversary.

Challenge: If **Extract** is over, The challenger runs **Encrypt** algorithm to obtain (Hdr^*, K) = **Encrypt**($\tilde{S}$, PK) where $K \in \mathcal{K}$, and any $\tilde{S} \subseteq S^*$. The challenger set $K_0 = K$, and K_1 to a random value in $\mathcal{K}$, then randomly selects $b \leftarrow \{0, 1\}$. The challenger returns (Hdr^*, K_b) to $\mathcal{A}$.

Guess: Finally, the adversary $\mathcal{A}$ outputs a guess $b' \in \{0, 1\}$ and wins the game if $b = b'$.

In the definition above, the indices of users were noted as ID. However, this is only for the generalization of the definition. For a normal broadcast encryption, the values of ID are taken from the set $\{1, \ldots, n\}$ where n is an integer representing the total number of users and is polynomial in the security parameter. Also, we define $AdvBr^{SS}_{\mathcal{A},n,\ell}(\lambda)$ be the advantage of algorithm $\mathcal{A}$ in winning the semi-static security game through at most ℓ users that can be included a broadcast if the system has total n users. It should be noted that the maximum number of extraction queries in this case is $n-k$ in the definition above because $\mathcal{A}$ cannot make private key queries for users in S^*.

4.2 Semi-static Secure Broadcast Encryption by Gentry and Waters [9]

Our main contribution is to improve the efficiency of the semi-static secure broadcast encryption from [9]. However, their construction of semi-static secure broadcast encryption was not separately written down because it can be obtained by simplifying adaptively secure identity-based broadcast encryption. For comparison with our algorithm, it is helpful to rewrite their semi-static secure broadcast encryption scheme clearly based on their description and proof. Let $GroupGen(\lambda,\ n,\ \ell)$ be an algorithm that outputs suitable bilinear group parameters $\langle \mathbb{G}, \mathbb{G}_T, e\rangle$, where $\mathbb{G}$ is of order $p \geq n + \ell$.

Setup(n, ℓ): Run $\langle \mathbb{G}, \mathbb{G}_T, e\rangle \leftarrow GroupGen(\lambda, n, \ell)$. Set $g_1, g_2 \xleftarrow{R} \mathbb{G}$. Set $\alpha, \beta, \gamma \xleftarrow{R} \mathbb{Z}_p$. Set $\hat{g}_1 \leftarrow g_1^{\beta}$ and $\hat{g}_2 \leftarrow g_2^{\beta}$. PK contains a description of $\langle \mathbb{G}, \mathbb{G}_T, e\rangle$, the parameters n and ℓ, along with g_1^{γ}, $g_1^{\gamma\cdot\alpha}$ and the set

$$\{g_1^{\alpha^j}, \hat{g}_1^{\alpha^j}, \hat{g}_2^{\alpha^k} : j \in [0, \ell], k \in [0, \ell - 2]\}.$$

Generate a random key κ for a PRF $\Psi : [1, n] \rightarrow \mathbb{Z}_p$. The private key is $SK \leftarrow (\alpha, \gamma, g_2, \kappa)$.

KeyGen$(i,\ SK)$: set $r_i \leftarrow \Psi_\kappa(i)$ and output the private key

$$d_i \leftarrow \langle r_i, h_i\rangle, \text{ where } h_i \leftarrow g_2^{\frac{\gamma - r_i}{\alpha - i}}.$$

Enc$(S,\ PK)$: Let $k = |S|$. Parse S as $\{i_1, ..., i_k\}$. Set $i_j \leftarrow n+j$ for $j \in [k+1, \ell]$. Set $P(x) = \prod_{j=1}^{\ell}(x - i_j)$. Set $t \xleftarrow{R} \mathbb{Z}_p$ and set $K \leftarrow e(g_1, \hat{g}_2)^{\gamma\cdot\alpha^{\ell-1}\cdot t}$. Next, set

$$Hdr \leftarrow \langle C_1, C_2, C_3, C_4\rangle \leftarrow \langle \hat{g}_1^{P(\alpha)\cdot t}, g_1^{\gamma\cdot t}, g_1^t, e(g_1, \hat{g}_2)^{\alpha^{\ell-1}\cdot t}\rangle.$$

Output $\langle Hdr, K\rangle$.

Dec$(S,\ i\ ,\ d_i,\ Hdr,\ PK)$: Suppose $i \in S = \{i_1, ..., i_k\}$. Define $P(x)$ as above. Let $P_i(x) = x^{\ell-1} - \frac{P(x)}{x-i}$. Set

$$K = e(C_1, h_i) \cdot e(C_2 \cdot C_3^{-r_i}, \hat{g}_2^{P_i(\alpha)}) \cdot C_4^{r_i}.$$

Correctness. Note that $K = K_1 \cdot K_2$, where we gather the terms containing a γ in K_1, and the other terms in K_2.

$$K_1 = e(C_1, g_2^{\gamma})^{1/(\alpha-i)} \cdot e(C_2, \hat{g}_2^{P_i(\alpha)}).$$

$$K_2 = e(C_1, g_2^{-r_i/(\alpha-i)}) \cdot e(C_3, \hat{g}_2^{P_i(\alpha)})^{-r_i} \cdot C_4^{r_i}.$$

We have that

$$K_1^{1/t} = e(g_1, \hat{g}_2)^{\gamma(P(\alpha)/(\alpha-i)+P_i(\alpha))} = e(g_1, \hat{g}_2)^{\gamma\cdot\alpha^{\ell-1}}.$$

We also have that

$$\begin{aligned} K_2^{1/t} &= e(g_1, \hat{g}_2)^{-r_i\cdot P(\alpha)/(\alpha-i) - r_i\cdot P_i(\alpha) + r_i\cdot\alpha^{\ell-1}} \\ &= e(g_1, \hat{g}_2)^{r_i\cdot(\alpha^{\ell-1} - P_i(\alpha) - P(\alpha)/(\alpha-i))} \\ &= e(g_1, \hat{g}_2)^0 = 1 \end{aligned}$$

as required.

5 Our Scheme

Our scheme reduces the size of private keys by removing the randomness r_i in GW scheme. Below we give an intuition for the reason that we are able to reduce the private key size (which in turn allows reduction in ciphertext size). Roughly speaking, the key structure, $(r_i, g_2^{\frac{\gamma - r_i}{\alpha - i}})$ for master key (γ, α) and generator g_2, of the GW scheme is commonly used to handle adaptive private key queries. However, we observe that this capability is not required since the goal is to achieve semi-static security. Based on this observation, we are able to remove the randomness r_i in the private key. Additionally, upon successful removal of r_i, we are also able to reduce the ciphertext size by half though removing the component (C_3, C_4) which was used to cancel the effect of r_i in the private key.

To be more specific, recall that in the security proof of GW scheme, the problem instance given to the simulator contains various power of α in the exponents. That is, g^{α^j} for a set of j and a generator g. The simulator chooses a polynomial $f(x)$ of some suitable degree and sets $\gamma = f(\alpha)$. While the simulator cannot compute the value γ, the public key is computable because it is at the form of $g^\gamma = g^{f(\alpha)}$. In order to generate a private key for value i, the simulator is required to compute a value related to $g^{\frac{\gamma - r_i}{\alpha - i}}$. This is where r_i is needed in GW's proof: for any value i, the simulator can set $r_i = f(i)$. Since γ is $f(\alpha)$, this ensures $(\alpha - i)$ is a factor of $\gamma - r_i$ because the latter is equivalent to $f(\alpha) - f(i)$. Note that indeed the simulator is capable of generating private key for any i.

As discussed, our goal is to achieve semi-static security and thus the capability of handling adaptive private key queries is not necessary. Our simple key structure can be proven as follows. Since any query i must come from the set $\dot{S} = \{1, \ldots, n\} \setminus S^*$, the simulator in our scheme sets the polynomial $f(x)$ to be divisible by $(x - i)$ for all $i \in \dot{S}$. That is, $f(x) = \prod_{i \in \dot{S}} (x + i) f'(x)$[1] for some random polynomial $f'(x)$ that is also chosen by the simulator. The master key γ is then set to be $f(\alpha)$. Since the adversary in the semi-static setting is restricted to query private keys from the set $\dot{S}$, the simulator can always compute the corresponding private key since $\gamma = f(\alpha)$ is always divisible by $(x + i)$ for all $i \in \dot{S}$. As such, we eliminate the need of randomness r_i which in turns remove the ciphertext component (C_3, C_4).

Our scheme has identical **Setup** with GW_{SS}, which means the public key remains the same as GW_{SS}. However, in **KeyGen**, the random element r_i of a private key in GW_{SS} was removed. As a result of the removal, **Enc** and **Dec** become simpler. Also, the size of private keys and ciphertexts are reduced by 50% and less computation are required. The detail of the scheme is as follows.

Let *GroupGen*$(\lambda,\ n,\ \ell)$ be an algorithm that outputs suitable bilinear group parameters $\langle \mathbb{G}, \mathbb{G}_T, e \rangle$, where $\mathbb{G}$ is of order $p \geq n + \ell$.

Setup(n, ℓ): Run $\langle \mathbb{G}, \mathbb{G}_T, e \rangle \leftarrow$ *GroupGen*(λ, n, ℓ). Set $g_1, g_2 \xleftarrow{R} \mathbb{G}$. Set $\alpha, \beta, \gamma \xleftarrow{R} \mathbb{Z}_p$. Set $\hat{g}_1 \leftarrow g_1^\beta$ and $\hat{g}_2 \leftarrow g_2^\beta$. PK contains a description of $\langle \mathbb{G}, \mathbb{G}_T, e \rangle$, the

[1] We use the $(x + i)$ instead of $(x - i)$ as the factor since it appears to be easier to work with in our case.

parameters n and ℓ, along with g_1^{γ}, $g_1^{\gamma \cdot \alpha}$ and the set

$$\{g_1^{\alpha^j}, \hat{g}_1^{\alpha^j}, \hat{g}_2^{\alpha^k} : j \in [0, \ell], k \in [0, \ell - 2]\}.$$

The private key is $SK \leftarrow (\alpha, \gamma, g_2)$.

KeyGen(i, SK): Output the private key

$$d_i \leftarrow g_2^{\frac{\gamma}{\alpha+i}}.$$

Enc (S, PK): Let $k = |S|$. Parse S as $\{i_1, ..., i_k\}$. Set $i_j \leftarrow n+j$ for $j \in [k+1, \ell]$. Set $P(x) = \prod_{j=1}^{\ell}(x + i_j)$. Set $t \xleftarrow{R} \mathbb{Z}_p$ and set $K \leftarrow e(g_1, \hat{g}_2)^{\gamma \cdot \alpha^{\ell-1} \cdot t}$. Next, set

$$Hdr \leftarrow \langle C_1, C_2 \rangle \leftarrow \langle \hat{g}_1^{P(\alpha) \cdot t}, g_1^{\gamma \cdot t} \rangle.$$

Output $\langle Hdr, K \rangle$.

Dec (S, i , d_i, Hdr, PK): Suppose $i \in S = \{i_1, ..., i_k\}$. Define $P(x)$ as above. Let $P_i(x) = x^{\ell-1} - \frac{P(x)}{x+i}$. Set

$$K = e(C_1, d_i) \cdot e(C_2, \hat{g}_2^{P_i(\alpha)}).$$

Correctness. The correctness of our scheme is shown as follows.

$$\begin{aligned} K^{1/t} &= e(\hat{g}_1^{P(\alpha)}, g_2^{\gamma})^{1/(\alpha+i)} \cdot e(g_1^{\gamma}, \hat{g}_2^{P_i(\alpha)}) \\ &= e(g_1, \hat{g}_2)^{\gamma(P(\alpha)/(\alpha+i)+P_i(\alpha))} \\ &= e(g_1, \hat{g}_2)^{\gamma \cdot \alpha^{\ell-1}}. \end{aligned}$$

□

It was modified to a semi-static construction to achieve constant size private key and ciphertext. Thus, as a broadcast encryption in the semi-static security model, this construction can be optimized as per our scheme.

5.1 Security Analysis

In this section, we shall prove that our scheme remains semi-static secure.

Theorem 1. Let $\mathcal{A}$ be a semi-static adversary against the above broadcast encryption system that makes at most $n-|S^*|$ queries. Then, there exists algorithm $\mathcal{B}$ such that

$$AdvBr^{SS}_{\mathcal{A},n,\ell}(\lambda) \leq AdvBDHES_{B,q,\ell}(\lambda) + 2/p$$

where $\mathcal{B}$ runs in time $t(A) + O((n + \ell)^2 \cdot \lambda^3)$ at most, assuming exponentiations take time $O(\lambda^3)$.

Proof. Let us assume that BDHE Sum instance $\{g^{\alpha^i} : i \in S\}$ is given for $m = 4d + 4\ell - 1$ and

$$S = [0, \ell - 2] \cup [d + \ell, 2d + \ell - 1] \cup [2d + 2\ell, 2d + 3\ell - 1]$$

$$\cup[3d+3\ell, 4d+3\ell] \cup [4d+4\ell, 5d+4\ell+1]$$

where $d = n + 2\ell$.

Init $\mathcal{A}$ selects $S^* \subseteq [1, n]$ and sends S^* to $\mathcal{B}$.

Setup $\mathcal{B}$ randomly generates $a_0, a_1, a_2 \xleftarrow{R} \mathbb{Z}_p^*$, and implicitly sets $k = |S^*|$. Then, $\mathcal{B}$ parses S^* as $\{i_1, ..., i_k\}$ and sets $i_j \leftarrow n + j$ for $j \in [k+1, \ell]$ and $P(x) = \prod_{j=1}^{\ell}(x + i_j)$. Also, let $f(x) = \prod_{i \in [1,n] \setminus S^*}(x + i) \cdot f'(x)$, and randomly construct $f'(x)$ that is a $d - n + k$ degree polynomial not to have common roots with $P(x)$. $f(x)$ is constructed in this way because $f(x)$ has to be divided by $(x + i)$ to generate valid private keys if identity i does not belong to the target set S^*.

Now, $\mathcal{B}$ sets

$$\beta \leftarrow a_0 \cdot \alpha^{-d-\ell},\ \gamma \leftarrow f(\alpha),$$

and

$$g_1 \leftarrow g^{a_1 \cdot \alpha^{4d+4\ell}},\ g_2 \leftarrow g^{a_2 \cdot \alpha^{d+\ell}},\ \hat{g}_1 \leftarrow g_1^{\beta},\ \hat{g}_2 \leftarrow g_2^{\beta}.$$

Then, all public keys which are g_1^{γ}, $g_1^{\gamma \cdot \alpha}$ and

$$\{g_1^{\alpha^j}, \hat{g}_1^{\alpha^j}, \hat{g}_2^{\alpha^k} : j \in [0, \ell], k \in [0, \ell - 2]\}$$

can be computed from the instance. Then, $\mathcal{B}$ send PK to $\mathcal{A}$.

Extract If $\mathcal{A}$ makes a private key query against i, $\mathcal{B}$ computes

$$d_i \leftarrow g_2^{\frac{\gamma}{\alpha+i}}$$

and sends d_i to $\mathcal{A}$. Notice that $f_i(x) \leftarrow f(x)/(x + i)$ is a polynomial of degree $d - 1$ for all $i \in [1, n] \setminus S^*$. Hence, $\mathcal{B}$ can calculate

$$g_2^{\frac{f(\alpha)}{\alpha+i}} = g^{a_2 \alpha^{d+\ell} \cdot f_i(\alpha)}$$

because $\{g^{\alpha^i} : i \in [d+\ell, 2d+\ell-1]\}$ is given in the instance.

Challenge For simplifying the notations, let $g_3 = g_1^{\alpha^{-d-\ell}} = g^{a_1 \cdot \alpha^{3d+3\ell}}$, and $\hat{g}_3 = g_3^{\beta}$. Then, g_3 and $\hat{g}_3$ are only possible to be computed from the BDHE Sum instance

$$\{g_3^{\alpha^j}, \hat{g}_3^{\alpha^k} : j \in [0, d] \cup [d+\ell, 2d+\ell+1], k \in [0, \ell-1] \cup [d+\ell, 2d+\ell]\}.$$

If $\mathcal{A}$ sends a set $\tilde{S} \subseteq S^*$, $\mathcal{B}$ computes a polynomial $t(x)$ of degree $d + \ell - 1$ satisfying

$$t(x)f(x)|_i = 0, \text{ if } i \in [d+1, d+\ell-1] \quad t(x)f(x)|_d = 1.$$

$$t(x)P(x)|_i = 0, \text{ if } i \in [\ell, d+\ell-1].$$

where $f(x)|_i$ is the coefficient of x^i in function f.
$t(x)$ exists due to Lemma 1 of [9]. $\mathcal{B}$ now sets the ciphertext values:

$$Hdr^* \leftarrow \langle C_1, C_2 \rangle \leftarrow \langle \hat{g}_3^{P(\alpha)\cdot t(\alpha)}, g_3^{f(\alpha)\cdot t(\alpha)} \rangle.$$

$$K \leftarrow Z^{a_0 a_1 a_2} \cdot e(g,g)^{a_0 a_1 a_2 (f(\alpha)\cdot t(\alpha)\cdot \alpha^{3d+4\ell-1} - \alpha^{4d+4\ell-1})}.$$

It should be noted that if $Z = e(g,g)^{\alpha^{4d+4\ell-1}}$, K is valid because $t(x)f(x)|_d = 1$.

Guess Finally, $\mathcal{A}$ outputs a bit b'. $\mathcal{B}$ sends b' to the challenger.

Almost Perfect Simulation We show that $\mathcal{B}$'s simulation is almost perfect from the point of $\mathcal{A}$. Most of our analysis is identical with GW's analysis [9]. In a semi-static security model, the maximum number of extraction queries is limited as $n-k$ because $\mathcal{A}$ only queries private keys for receivers not in $\tilde{S}$.

- PK is uniformly distributed since a_0, a_1, a_2, and α are random.
- Private key is uniformly distributed if $f(x)$ is uniformly distributed. In order to verify the uniformity of $f(x)$, the information leaking to $\mathcal{A}$ is formalized as follows.
  - In **Init**, $\mathcal{A}$ gets

    $$f(-i) \neq 0 \text{ for } i \in \{S^* \cup [n+1, n+\ell]\}.$$

  - In **Setup**, From the PK, $\mathcal{A}$ gets

    $$f(\alpha) = DL_{g_1}(g_1^{\gamma}).$$

  - In **Extract**, to $\mathcal{A}$, each private key query reveals

    $$f(-i) = 0 \text{ for } i \notin S^*.$$

  Since at most $n-k$ extraction queries can be made, therefore the information about $f(x)$ to $\mathcal{A}$ can be formulated by total $n+\ell-k+1$ equations described above even if we consider all non-zero equations. Because degree of $f(x)$ is $n+2\ell$, $f(x)$ can be random and independent. This implies that the private key is also appropriately distributed.
- Suppose Z is random, then the statistical difference from uniform distribution is less than 2/p. Let $Z = e(g,g)^{\delta+\alpha^{4d+4\ell-1}}$, then $K = e(g,g)^{\delta a_0 a_1 a_2} \cdot K'$ where K' is the correct key for Hdr^*. When $\delta = 0$, there is only one possible value of K. However, when $\delta \neq 0$, there are $p-1$ equally probable values of K depending on $a_0 a_1 a_2$ which is non-zero.

Abort There is no additional abortion which gives advantages to $\mathcal{A}$ except the cases we mentioned in *Almost Perfect Simulation* part.

Running Time of Simulation The running time of this game is dominated by two computations, computing $g_2^{f_i(\alpha)}$ and $t(x)$. $O(n+\ell)$ exponentiation is

necessary to calculate $g_2^{f_i(\alpha)}$ for each private key query, and $n-k$ private key queries can be made at most. Also, for computing $t(x)$, the algorithm must calculate at least one column of a $(d+\ell-1)$ dimension Sylvester matrix. This requires $O(\ell(n+\ell))$ algorithm with the current knowledge [9]. Therefore, the running time of this simulation is at most about $O((n+\ell)^2)$. □

6 Transforming Semi-static Security to Adaptively Security

The adaptive security model [9] is the strongest and most realistic notion in broadcast encryption. An adversary is not required to declare any target set before observing public keys. As such, there is no **Init** phase. Moreover, the set for a challenge cipertext can be any subsets of the set of identities that has never been queried in the **Extract** phase.

6.1 Transforming Semi-static Security to Adaptive Security

In addition to the semi-static security model, Gentry and Waters also showed how to transform a semi-static secure broadcast encryption scheme to an adaptively secure broadcast algorithm based on the two key technique [12]. In their technique, two keys are assigned for each user, but only one private key is allocated randomly to an individual user to respond extraction queries adaptively. Since the sender does not know which key each receiver has, the ciphertext must be constructed for both keys. Furthermore, users can also figure out which ciphertext can be decrypted by their private keys through a bit included in their private key.

We basically follow GW's approaches to make our semi-static secure broadcast encryption scheme be adaptively secure. In addition to their technique, we suggest an implementation technique to remove a linearly increasing element in GW's transformation. Let S be the set of receivers. The original transformation requires that for all $i \in S$, a bit $b_i \in \{0,1\}$ is also included in the ciphertext. In other words, the ciphertext contains an additional component of $|S|$-bit.

Let $S = \{ID_1, \ldots, ID_{|S|}\}$ be the set of receivers. The original transformation requires an additional one bit information for each identity ID_i, denoted as b_{ID_i}, to be transmitted along the ciphertext. In order to transmit this information, the transformation includes an additional bit-string t of length $|S|$ such that $t[i] = b_{ID_i}$, where $t[i]$ represents the i-th bit of t.

In the transformation, the i-th receiver $ID_i \in S$ is associated with a bit $t[i]$. And therefore, the $|S|$-bit t is required.

Since decryption requires the knowledge of S, it is possible that in some scenarios, S has to be transmitted along the ciphertext. In this case, we describe an implementation trick that reduces the component t from $|S|$ bits to one bit. As the set S is normally not counted as part of the ciphertext, truly constant size ciphertext can be achieved.

Our Implementation Technique
Based on the observation that transmitting a set S and a sequence $\tilde{S}$, such that for any $i \in \tilde{S}$, $i \in S$, requires the same space complexity, we are able to replace $\{b_i\}$ with one single bit as follows. Denote i_s as the smallest value in S. Let $S_{b0} = \{i \in S \setminus \{i_s\} | b_i = 0\}$ and $S_{b1} = \{i \in S \setminus \{i_s\} | b_i = 1\}$. In other words, S_{b0} and S_{b1} are *the partition* of $S \setminus \{i_s\}$ based on the bit b_i.

We can construct a sequence $\left(S_{separated}\right)$ as $\mathsf{seq}(S_{b0}), i_s, \mathsf{seq}(S_{b1})$ where $\mathsf{seq}(S)$ represents the random arrangement of elements of a set S to form a sequence (for simplicity, it can be in the normal ascending order). The sequence $S_{separated}$, together with a bit b_{i_s} would be sufficient to recover b_i for all i. For instance, the receiver first recovers the smallest identity i_s from the sequence $S_{separated}$. For any i in the sequence $S_{separated}$, $b_i = 0$ if i is before i_s and $b_i = 1$ otherwise. The only bit that needs to be transmitted along with the ciphertext is therefore b_{i_s}. Note that the cost of transmitting the sequence $S_{separated}$ is identical to that of S. We do not claim significant reduction in transmission cost in practice despite the saving in asymptotic complexity is from $O(|S|)$ to $O(1)$. In practice, if the set of receivers is to be transmitted together with the ciphertext, which is possibly true in some cases when S is highly dynamic, the actual saving of our tricks is $\lceil \log(|S|) \rceil - 1$ bits only. However, if the set S is known to the set of receivers, the trick is not applicable as in those cases, S does not need to be transmitted repeatedly.

Our construction using $S_{separated}$ is as follows. Note that the size of $S_{separated}$ is identical that of S.

Setup(n, ℓ): Run $\langle PK', SK' \rangle \leftarrow Setup_{SS}(2n, \ell)$. Set $s \leftarrow \{0,1\}^n$, Set $PK \leftarrow PK'$ and $SK \leftarrow (SK', s)$. Output $\langle PK, SK \rangle$.

KeyGen$(i,\ SK)$: Run $d'_i \leftarrow KeyGen_{SS}(i + n \cdot s_i, SK')$. Set $d_i \leftarrow \langle d'_i, s_i \rangle$. Output d_i.

Enc$(S,\ PK)$: Generate a random set of $|S|$ bits: $t \leftarrow \{t_i \leftarrow \{0,1\} : i \in S\}$. Generate $K \leftarrow \mathcal{K}$. Set

$$
\begin{aligned}
&S_{t_0} \leftarrow \{i \text{ if } t_i = 0 : i \in S\}, \quad S_{t_1} \leftarrow \{i \text{ if } t_i = 1 : i \in S\} \\
&S_0 \leftarrow S_{t_0} \cup \{i + n : i \in S_{t_1}\}, \qquad \langle Hdr_0, k_0 \rangle \leftarrow Enc_{SS}(S_0, PK') \\
&S_1 \leftarrow \{i + n : i \in S_{t_0}\} \cup S_{t_1}, \qquad \langle Hdr_1, k_1 \rangle \leftarrow Enc_{SS}(S_1, PK').
\end{aligned}
$$

Set $C_0 \leftarrow SymEnc(k_0, K), C_1 \leftarrow SymEnc(k_1, K), Hdr \leftarrow \langle Hdr_0, C_0, Hdr_1, C_1, b_{i_s} \rangle$ where b_{i_s} is the bit for the smallest identity in $i_s \in S$. Output $\langle Hdr, K \rangle$. Also, replace S with the sequence $S_{separated} \leftarrow \{\mathsf{seq}(S_{b0}), i_s, \mathsf{seq}(S_{b1})\}$ where

$$S_{b0} \leftarrow S_{t_0} \setminus \{i_s\}, \quad S_{b1} \leftarrow S_{t_1} \setminus \{i_s\}.$$

Dec($S_{separated}$, i, d_i, Hdr, PK): Parse d_i as $\langle d'_i, s_i \rangle$ and Hdr as $\langle Hdr_0, C_0, Hdr_1, C_1, b_{i_s} \rangle$. Set S_0 and S_1. Run

$$k_{s_i \oplus t_i} \leftarrow Dec_{SS}(S_{s_i \oplus t_i}, i, d'_i, Hdr_{s_i \oplus t_i}, PK').$$

Run $K \leftarrow SymDec(k_{s_i \oplus t_i}, C_{s_i \oplus t_i})$. Output K.

Since we just compress t to S through $S_{seperated}$, the security analysis remains the same as in the original Gentry and Waters' proof. Our adaptive broadcast encryption, following this generic transformation, compares favourably to the transformation of GW_{SS} since the impact of the transformation on efficiency is linear.

7 Conclusion

Gentry and Waters [9] introduced the security model and constructions for semi-static broadcast encryption, which can be transformed to an adaptively secure broadcast encryption. Based on their contributions, we introduced a more efficient semi-static broadcast encryption scheme. Our scheme enjoys smaller ciphertexts, shorter private keys and is more efficient in terms of computation cost.

We also showed that an adaptively secure broadcast encryption scheme transformed from our semi-static broadcast encryption scheme is still competitive against other adaptively secure broadcast encryption schemes that have been introduced recently. In addition, we elaborated an implementation technique to add to Gentry and Waters' transformation technique, which removes the linearly increasing part in the ciphertext. By adopting this idea, the resulting adaptively secure broadcast encryption scheme has a constant ciphertext if the underlying semi-static secure broadcast encryption scheme has a constant size ciphertext.

Furthermore, our scheme can be used as an identity-based broadcast encryption, but limited for polynomially many users. Extending our scheme for exponentially many users might be possible following the approach introduced by Delerablée [5] , but it will rely on a random oracle.

Acknowledgements

We would like to thank the anonymous referees of Pairing 2013 for their constructive feedback to improve our paper. Additionally, we would like to thank Madeleine Cincotta for her thorough check to improve the linguistic quality of our paper. Finally, we would like to thank Dario Fiore who helped us to improve the quality of our paper. The second author is supported by ARC Future Fellowship FT0991397 and partly supported by the Natural Science Foundation of China through project 61370190.

References

1. J. Baek, R. Safavi-Naini, and W. Susilo. Efficient multi-receiver identity-based encryption and its application to broadcast encryption. In S. Vaudenay, editor, *Public Key Cryptography*, volume 3386 of *Lecture Notes in Computer Science*, pages 380–397. Springer, 2005.
2. M. Barbosa and P. Farshim. Efficient identity-based key encapsulation to multiple parties. In N. P. Smart, editor, *IMA Int. Conf.*, volume 3796 of *Lecture Notes in Computer Science*, pages 428–441. Springer, 2005.
3. D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In V. Shoup, editor, *CRYPTO*, volume 3621 of *Lecture Notes in Computer Science*, pages 258–275. Springer, 2005.
4. R. Cramer and V. Shoup. Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack. *SIAM Journal on Computing*, 33(1):167–226, 2003.
5. C. Delerablée. Identity-based broadcast encryption with constant size ciphertexts and private keys. In K. Kurosawa, editor, *ASIACRYPT*, volume 4833 of *Lecture Notes in Computer Science*, pages 200–215. Springer, 2007.
6. Y. Dodis and N. Fazio. Public key broadcast encryption for stateless receivers. In J. Feigenbaum, editor, *Digital Rights Management Workshop*, volume 2696 of *Lecture Notes in Computer Science*, pages 61–80. Springer, 2002.
7. A. Fiat and M. Naor. Broadcast encryption. In D. R. Stinson, editor, *CRYPTO*, volume 773 of *Lecture Notes in Computer Science*, pages 480–491. Springer, 1993.
8. C. Gentry and S. Halevi. Hierarchical identity based encryption with polynomially many levels. In O. Reingold, editor, *TCC*, volume 5444 of *Lecture Notes in Computer Science*, pages 437–456. Springer, 2009.
9. C. Gentry and B. Waters. Adaptive security in broadcast encryption systems (with short ciphertexts). In A. Joux, editor, *EUROCRYPT*, volume 5479 of *Lecture Notes in Computer Science*, pages 171–188. Springer, 2009.
10. M. T. Goodrich, J. Z. Sun, and R. Tamassia. Efficient tree-based revocation in groups of low-state devices. In M. K. Franklin, editor, *CRYPTO*, volume 3152 of *Lecture Notes in Computer Science*, pages 511–527. Springer, 2004.
11. D. Halevy and A. Shamir. v. In M. Yung, editor, *CRYPTO*, volume 2442 of *Lecture Notes in Computer Science*, pages 47–60. Springer, 2002.
12. J. Katz and N. Wang. Efficiency improvements for signature schemes with tight security reductions. In S. Jajodia, V. Atluri, and T. Jaeger, editors, *ACM Conference on Computer and Communications Security*, pages 155–164. ACM, 2003.
13. A. B. Lewko, A. Sahai, and B. Waters. Revocation systems with very small private keys. In *IEEE Symposium on Security and Privacy*, pages 273–285. IEEE Computer Society, 2010.
14. B. Malek and A. Miri. Adaptively secure broadcast encryption with short ciphertexts. *I. J. Network Security*, 14(2):71–79, 2012.
15. D. Naor, M. Naor, and J. Lotspiech. Revocation and tracing schemes for stateless receivers. In J. Kilian, editor, *CRYPTO*, volume 2139 of *Lecture Notes in Computer Science*, pages 41–62. Springer, 2001.
16. M. Naor and B. Pinkas. Efficient trace and revoke schemes. In Y. Frankel, editor, *Financial Cryptography*, volume 1962 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2000.
17. D. H. Phan, D. Pointcheval, S. F. Shahandashti, and M. Strefler. Adaptive CCA broadcast encryption with constant-size secret keys and ciphertexts. In W. Susilo,

Y. Mu, and J. Seberry, editors, *ACISP*, volume 7372 of *Lecture Notes in Computer Science*, pages 308–321. Springer, 2012.
18. Y. Ren and D. Gu. Fully CCA2 secure identity based broadcast encryption without random oracles. *Inf. Process. Lett.*, 109(11):527–533, 2009.
19. R. Sakai and J. Furukawa. Identity-based broadcast encryption. *IACR Cryptology ePrint Archive*, 2007:217, 2007.
20. A. Shamir. Identity-based cryptosystems and signature schemes. In G. R. Blakley and D. Chaum, editors, *CRYPTO*, volume 196 of *Lecture Notes in Computer Science*, pages 47–53. Springer, 1984.
21. V. Shoup. A proposal for an iso standard for public key encryption. *IACR Cryptology ePrint Archive*, 2001:112, 2001.
22. N. P. Smart. Efficient key encapsulation to multiple parties. In C. Blundo and S. Cimato, editors, *SCN*, volume 3352 of *Lecture Notes in Computer Science*, pages 208–219. Springer, 2004.