Unconditionally Secure Revocable Storage: Tight Bounds, Optimal Construction, and Robustness

Yohei Watanabe[1,2,*], Goichiro Hanaoka[2], and Junji Shikata[3,4]

[1] Graduate School of Informatics and Engineering,
The University of Electro-Communications, Tokyo, Japan

[2] Information Technology Research Institute (ITRI),
National Institute of Advanced Industrial Science and Technology (AIST), Tokyo, Japan

[3] Graduate School of Environment and Information Sciences,
Yokohama National University, Yokohama, Japan

[4] Institute of Advanced Sciences,
Yokohama National University, Yokohama, Japan

watanabe@uec.ac.jp, hanaoka-goichiro@aist.go.jp, shikata@ynu.ac.jp

April 25, 2016

Abstract

Data stored in cloud storage sometimes requires long-term security due to its sensitivity (e.g., genome data), and therefore, it also requires flexible access control for handling entities who can use the data. *Broadcast encryption* can partially provide such flexibility by specifying privileged receivers so that only they can decrypt a ciphertext. However, once privileged receivers are specified, they can be no longer dynamically added and/or removed. In this paper, we propose a new type of broadcast encryption which provides long-term security and appropriate access control, which we call unconditionally secure *revocable-storage broadcast encryption* (RS-BE). In RS-BE, privileged receivers of a ciphertext can be dynamically updated without revealing any information on the underlying plaintext. Specifically, we define a model and security of RS-BE, derive tight lower bounds on sizes of secret keys required for secure RS-BE, and propose a construction of RS-BE which meets all of these bounds. Our lower bounds can be applied to traditional broadcast encryption. Furthermore, to detect an improper update, we consider security against modification attacks to a ciphertext, and present a concrete construction secure against this type of attacks.

1 Introduction

1.1 Background

In recent years, the progress of cloud technologies has been remarkable, and cloud-based applications are becoming widespread. One area in which cloud technology has the potential to provide significant impact, is advanced medical treatment, and applications of cloud technology in this area is currently being investigated intensively [3, 39]. To provide such advanced medical services, it is required to

[*]Part of this work was done while the first author was a Ph.D student at Graduate School of Environment and Information Sciences, Yokohama National University.

store the data of individual patients using cloud storage. However, this data is generally very sensitive and should be protected carefully. Especially, when storing genome data using cloud storage, computationally secure encryption is considered to provide insufficient protection since genetic properties will be inherited by descendants of the genome owner, and thus, significantly long-term security is required [3, 4]. For example, even if we encrypt genome data using a 2048-bit RSA cryptosystem, which is considered sufficiently secure in most applications, security will only be guaranteed until 2030 [5], which is not sufficient for protecting genome privacy (which must take into account the privacy of our descendants).

A promising approach for obtaining sufficiently strong security for medical data is to utilize information-theoretically secure encryption, e.g. the one-time pad. However, the one-time pad is only a (standard) symmetric encryption scheme, and thus, not suitable for effective use in a cloud environment. Namely, in a cloud storage system, there are potentially many users who will be given permission to access the stored data, and these privileged users are furthermore dynamically determined. It is obvious that such a scenario cannot be easily handled by using only (standard) symmetric encryption. *Broadcast encryption* (BE) [18] which allows multiple receivers to decrypt a logically single ciphertext seems to partially yield the required functionality. However, when the sender encrypts a plaintext in BE, he is forced to fix the set of privileged users and cannot dynamically add and/or remove receivers. For handling dynamic changes to the set of privileged receivers (in the context of attribute-based encryption [34]), Sahai, Seyalioglu, and Waters proposed *revocable-storage attribute-based encryption* [33] in which a ciphertext in a cloud storage system can be periodically updated according to a changing set of privileged users. However, their scheme is computationally secure and does not guarantee security against future powerful adversaries.

Therefore, it is important to investigate suitable cryptographic primitives which simultaneously provide a high level of security for sensitive data and sufficient flexibility to implement appropriate access control.

1.2 Our Contributions

In this paper, we propose the notion of unconditionally secure *revocable-storage BE* (RS-BE) which yields information-theoretic security and the above required functionality for cloud storage. In an RS-BE scheme, similarly to BE, the sender chooses a set of (initial) privileged users and encrypts a plaintext so that only these users can decrypt the ciphertext. Moreover, the *storage manager* can update the ciphertext to reflect changes in the set of privileged users. Here, the update procedure is carried out without revealing the plaintext, and thus, the storage manager cannot learn anything about the encrypted plaintext. We furthermore show tight lower bounds on the sizes of ciphertexts and secret keys in the unconditionally secure setting, and present an optimal construction which achieves these bounds as well as a robust construction which is resilient to a maliciously behaving storage manager.

More specifically, our contributions are as follows. Firstly, in Section 2, we give a formal model and security definitions of unconditionally secure RS-BE. Then, in Section 3, we clarify that it is possible to construct an unconditionally secure RS-BE scheme in which the ciphertext length is the same as the plaintext length. We note that this is an important and desired property since ciphertexts are stored in the cloud permanently or for a long time, and therefore, compactness of ciphertexts is one of the most important aspects to consider in the design of an RS-BE scheme. We then investigate lower bounds on the sizes of decryption keys, encryption keys, and the storage manager's keys under the condition that the ciphertext size is the same as the plaintext size. These bounds can also be seen as a generalization of the bounds for (traditional) BE, and furthermore imply a tight bound on the size of encryption keys in BE which, to the best of our knowledge, has not been clarified before our work. In Section 4, we show an unconditionally secure RS-BE scheme with an efficient trade-off between the ciphertext and secret-key sizes. More precisely, for arbitrary $\delta \in \{1, 2, \dots, n\}$ we present an unconditionally secure RS-BE scheme with efficient secret-key sizes when the ciphertext size is at most δ times as large as the plaintext size. In particular, our construction meets all of these bounds with equalities when $\delta = 1$ (i.e., a scheme where the ciphertext size is always equal to the plaintext size). This means that these bounds are *tight* and the proposed construction is *optimal* for $\delta = 1$. In Section 5, we furthermore consider a scenario in which a maliciously behaving storage manager can try to modify the encrypted plaintext. This is related to *non-malleability* in the context of ordinary encryption. In an RS-BE scheme, malleability may cause a serious problem since the ciphertext is periodically updated, but an improper update carried out by a malicious storage manager may not be immediately detectable by the users. We define robustness, which is a security notion against such a malicious update, and derive a lower bound on the ciphertext size for a robust RS-BE scheme. Then, we present a concrete robust construction based on an ordinary RS-BE scheme presented in Section 4 and *an algebraic manipulation detection code* (AMD-code for short) [16]. We show one of instantiations of the robust scheme is *almost optimal* in the sense of the ciphertext size. Therefore, the above lower bound on the ciphertext size is almost tight.

1.3 Related Work

Berkovits [6] first considered the concept of BE, and Fiat and Naor [18] developed a formal and systematic approach to the construction of BE schemes. Since then, BE schemes have been improved both in the computationally secure setting [28, 17, 13, 19, 32] and in the unconditionally secure setting [8, 10, 23, 6, 18, 37, 26, 30, 15, 31, 40], and used in various situations such as copyright protection in the real world. In particular, lower bounds on secret keys for unconditionally secure BE (USBE for short) schemes have previously been investigated [8, 10, 23]. However, some problems nonetheless remain. Blundo and Cresti [8] derived lower bounds on USBE in the context of key predistribution schemes (KPS for short) [27, 7]. However, these bounds are specific to the application to KPS, and are not true lower bounds for USBE in general. Also, Blundo et al. [10] derived lower bounds for USBE, but these bounds are not tight. Furthermore, Kurosawa et al. [23] showed tight lower bounds on the size of decryption keys for USBE through equivalence between USBE and KPS, however, they did not mention lower bounds on encryption keys in their paper. In contrast, we derive tight lower bounds on both of the sizes of encryption keys and decryption keys for USBE without using such equivalence, and it turns out that the tight lower bound on the size of decryption keys in [23] is a special case of ours.

Recently, many researchers have investigated how we can *securely* use cloud data storage for various purposes [22, 33, 1, 20, 35, 36, 25, 24, 41]. Sahai, Seyalioglu, and Waters [33] first dealt with the concept of a revocable storage, and proposed revocable-storage attribute-based encryption (RS-ABE for short). They assume ciphertexts are stored in external storage, such as cloud data storage, and considered revocable attribute-based encryption [12, 2] with ciphertext updatable functionality (to be precise, [12] in the context of identity-based encryption). However, RS-ABE is only computationally secure, and hence cannot guarantee long-term security. In the unconditionally secure setting, proactive secret sharing schemes [21, 38, 29, 14] and fully dynamic secret sharing schemes [9] also provide functionality for updating shares. However, such updating functionality and its aim in these schemes are different from those in our RS-BE scheme. Hence, we cannot directly apply these techniques, and we need to define and to construct RS-BE schemes from scratch.

2 Revocable-Storage Broadcast Encryption

2.1 Model

In RS-BE, there are $n+2$ entities, a sender E, n users $U_1, \ldots, U_n$, and a storage manager SM. Let $\mathcal{U} := \{U_1, \ldots, U_n\}$ be a set of all users. First, E generates own encryption key ek, also generates n decryption keys $dk_1, \ldots, dk_n$ and a maintenance key mk behalf of $U_1, \ldots, U_n, SM$, and distributes them securely. E can specify a subset $\mathcal{S}$ (called a *privileged set*) of $\mathcal{U}$ such that $\mathcal{S} \neq \emptyset$, and encrypt a plaintext by using his encryption key ek so that only users in the privileged set can decrypt the resulting ciphertext. The ciphertext is stored and disclosed in an external storage such as cloud storage. A user U_i in the privileged set $\mathcal{S}$ takes the ciphertext from the storage himself, then he decrypts the ciphertext by using his decryption key dk_i. The storage manager SM can change *any* privileged set $\mathcal{S}$ of the ciphertext into *any* privileged set $\mathcal{S}'$ (even if *not* $\mathcal{S}' \subset \mathcal{S}$) by using his maintenance key mk without decryption (i.e., without revealing the underlying plaintext). At sender's request or by some kind of rule, the storage manager SM changes the privileged set of the ciphertext, and then SM replaces the old one with the new one.

Formally, RS-BE is executed as follows. Let $\mathcal{M}$ be a set of possible plaintexts. For any subset $\mathcal{J} := \{U_{i_1}, \ldots, U_{i_j}\} \subset \mathcal{U}$, let $\mathcal{C}_{\mathcal{J}}$ be a set of all possible ciphertexts for the privileged set $\mathcal{J}$, and let $\mathcal{C} := \bigcup_{\mathcal{J} \subset \mathcal{U}} \mathcal{C}_{\mathcal{J}}$. Let $\mathcal{EK}$ be a set of possible encryption keys, and let $\mathcal{MK}$ be a set of maintenance keys. Let $\mathcal{DK}_i$ be a set of possible decryption keys for U_i, and let $\mathcal{DK} := \bigcup_{i=1}^{n} \mathcal{DK}_i$.

Definition 1 (RS-BE)**.** *A revocable-storage broadcast encryption (*RS-BE *for short) scheme* Π *involves* $n+2$ *entities,* E, $U_1, U_2, \ldots, U_n$ *and* SM*, and consists of the following four-tuple of algorithms (Setup, Enc, Dec, Upd) with five spaces,* $\mathcal{M}, \mathcal{C}, \mathcal{EK}, \mathcal{DK}$*, and* $\mathcal{MK}$*, where all of the above algorithms except Setup are deterministic and all of the above spaces are finite.*

1. $(ek, mk, dk_1, \ldots, dk_n) \leftarrow Setup(n)$*: It takes the number of users* n *as input, and outputs an encryption key* $ek \in \mathcal{EK}$*,* n *decryption keys* $(dk_1, \ldots, dk_n) \in \prod_{i=1}^{n} \mathcal{DK}_i$*, and a maintenance key* $mk \in \mathcal{MK}$*.*

2. $c_{\mathcal{S}} \leftarrow Enc(ek, m, \mathcal{S})$*: It takes an encryption key* ek*, a plaintext* $m \in \mathcal{M}$*, and an initial privileged set* $\mathcal{S} \subset \mathcal{U}$ *as input, and outputs a ciphertext* $c_{\mathcal{S}}$*.*

3. m *or* $\perp \leftarrow Dec(dk_i, c_{\mathcal{S}}, \mathcal{S}, U_i)$*: It takes a decryption key* dk_i *of a user* U_i*, the ciphertext* $c_{\mathcal{S}}$*, the privileged set* $\mathcal{S}$*, and the identity* U_i *as input, and outputs* m *or* $\perp$*.*

4. $c_{\mathcal{S}'}$ *or* $\perp \leftarrow Upd(mk, c_{\mathcal{S}}, \mathcal{S}, \mathcal{S}')$*: It takes a maintenance key* mk*, the ciphertext* $c_{\mathcal{S}}$*, its privileged set* $\mathcal{S}$*, and a new privileged set* $\mathcal{S}'$ *as input, and outputs a ciphertext* $c_{\mathcal{S}'}$ *for* $\mathcal{S}'$ *or* $\perp$*.*

In RS-BE Π, we require the following correctness holds: (a) For all $n \in \mathbb{N}$, all $(ek, mk, dk_1, \ldots, dk_n) \leftarrow Setup(n)$, all $m \in \mathcal{M}$, all $\mathcal{S} \subset \mathcal{U}$, and all $U_i \in \mathcal{S}$, $m \leftarrow Dec(dk_i, Enc(ek, m, \mathcal{S}), \mathcal{S}, U_i)$. (b) For all $n \in \mathbb{N}$, all $(ek, mk, dk_1, \ldots, dk_n) \leftarrow Setup(n)$, all $m \in \mathcal{M}$, all $\mathcal{S}, \mathcal{S}' \subset \mathcal{U}$, $Upd(mk, Enc(ek, m, \mathcal{S}), \mathcal{S}') = Enc(ek, m, \mathcal{S}')$. (a) means the *decryption correctness* and (b) means the *updating correctness.*

In RS-BE, for simplicity we assume the one-time model where it is allowed for the sender to encrypt a plaintext and store a ciphertext only once. Note that it is unrestricted for the storage manager to execute the algorithm *Upd* (i.e. the ciphertext can be updated unboundedly).

2.2 Security Definition

We consider perfect secrecy against at most ω colluders and the storage manager. Here, we note that in principle, it is impossible to guarantee security against collusion of them since the storage manager can change any privileged set of a ciphertext into any privileged set. Therefore, we consider security in the case that at most ω colluders and the storage manager try to attack separately.[1] Namely, we consider the following two kinds of security notions: (1) At most ω colluders who are not included in the privileged set cannot get any information on the underlying plaintext from the ciphertext (a traditional security notion for BE). (2) The storage manager cannot get any information on the underlying plaintext from the ciphertext. The reason why we consider the second one is that if the storage manager can obtain the underlying plaintext or some information on it, it is only necessary to encrypt the same plaintext with a new privileged set and replace an old ciphertext with the new one by a sender to change privileged sets. Hence, we require the storage manager can update the ciphertext without decryption (without leaking any information on the underlying plaintext). For any $\mathcal{J} := \{U_{i_1}, \ldots, U_{i_j}\} \subset \mathcal{U}$, let $\mathcal{DK}_{\mathcal{J}} := \mathcal{DK}_{i_1} \times \cdots \times \mathcal{DK}_{i_j}$ be a set of possible secret keys of $\mathcal{J}$. Let M, $C_{\mathcal{S}}$, EK, DK_i $(1 \le i \le n)$, $DK_{\mathcal{J}}$ $(\mathcal{J} \subset \mathcal{U})$, and MK be random variables which takes values on $\mathcal{M}$, $\mathcal{C}_{\mathcal{S}}$, $\mathcal{EK}$, $\mathcal{DK}_i$ $(1 \le i \le n)$, $\mathcal{DK}_{\mathcal{J}}$ $(\mathcal{J} \subset \mathcal{U})$, and $\mathcal{MK}$, respectively. Formally, security of RS-BE is defined as follows.

Definition 2 (Security of RS-BE)**.** *Let* Π *be an RS-BE scheme.* Π *is said to be* $(\le n, \le \omega)$*-one-time secure if the following conditions are satisfied:*

(1) For any privileged set $\mathcal{S} \subset \mathcal{U}$*, and any set of colluders* $\mathcal{W} \subset \mathcal{U}$ *such that* $\mathcal{S} \cap \mathcal{W} = \emptyset$ *and* $|\mathcal{W}| \le \omega$*, it holds that* $H(M \mid C_{\mathcal{S}}, DK_{\mathcal{W}}) = H(M)$*.*

(2) For any privileged set $\mathcal{S} \subset \mathcal{U}$*, it holds that* $H(M \mid C_{\mathcal{S}}, MK) = H(M)$*.*

Remark 1. *In the model of RS-BE (Definition 1), if SM does not exist (i.e., mk is empty string and we do not consider the algorithm Upd), and we therefore do not consider the condition (2) in Definition 2, then Definitions 1 and 2 are the same as those of ((*$\le n, \le \omega$*)-one-time secure) traditional BE schemes [18, 37, 8, 23]. Hence, we can say our scheme is natural extension of the BE schemes.*

Remark 2. *The condition (1) in Definition 2 implies that the number of ciphertexts taken by* $\mathcal{W}$ *from the storage is at most one. However, it is natural to think that* $\mathcal{W}$ *can access the storage multiple time and take ciphertexts for various privileged sets. Namely, for more realistic definition, we should consider the following security condition (1') instead of (1):*

(1') For any privileged sets $\mathcal{S}_1, \ldots, \mathcal{S}_k \subset \mathcal{U}$ $(1 \le k \le 2^n)$*, and any set of colluders* $\mathcal{W} \subset \mathcal{U}$ *such that* $\left(\bigcup_{i=1}^{k} \mathcal{S}_i\right) \cap \mathcal{W} = \emptyset$ *and* $|\mathcal{W}| \le \omega$*, it holds that* $H(M \mid C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_k}, DK_{\mathcal{W}}) = H(M)$*.*

For convenience, we call Π *a strongly secure RS-BE scheme if it satisfies the conditions (1') and (2), and just call* Π *a secure RS-BE scheme if it satisfies Definition 2 (the conditions (1) and (2)). Actually, tight lower bounds on secret keys required for such a strongly secure RS-BE scheme are the same as those required for the secure RS-BE scheme (the bounds will appear in Theorem 2). Therefore, we can obtain the same optimal construction, in the sense that the construction meets equality in every lower bound, which will be proposed in Section 4. In addition to this, to deal with RS-BE as natural extension of traditional BE, we consider the above weaker security definition (Definition 2).*

[1] We also discuss an RS-BE scheme secure against collusion of at most ω colluders and the storage manager under a restricted transformation rule of the storage manager's key in Appendix A.

3 Tight Lower Bounds on Sizes of Ciphertexts and Secret Keys

In this section, we show lower bounds on the sizes of ciphertexts and secret keys required for a $(\leq n, \leq \omega)$-one-time secure RS-BE scheme. As mentioned in [10, 26, 30, 31], in traditional BE schemes, there is a trade-off between the ciphertext size and the secret key size. RS-BE schemes also have such a trade-off. Although our construction which will be presented in Section 4 covers any ciphertext length, we here consider lower bounds on secret-key sizes required for an $(\leq n, \leq \omega)$-one-time secure RS-BE scheme where the ciphertext length is as small as possible. The reason for this is when we consider applying RS-BE to cloud storage, compactness of a ciphertext is one of the most important factors to be taken into account, since in such a scenario, a ciphertext is stored in cloud permanently or for a long-time.

For the above reason, we first investigate the *tight* lower bound on the size of ciphertexts, and then, derive lower bounds on sizes of secret keys under the condition that the ciphertext length is optimal. A lower bound which can be immediately obtained is $H(C_{\mathcal{S}}) \geq H(M)$, and actually, by a simple observation, this bound is proven to be tight. We formally state this as follows.

Theorem 1. *Let Π be an $(\leq n, \leq \omega)$-one-time secure RS-BE scheme. Then, for any $\mathcal{S} \subset \mathcal{U}$, $H(C_{\mathcal{S}}) \geq H(M)$ and there exists a concrete construction which meets this bound with equality.*

Proof. For any $\mathcal{S} \subset \mathcal{U}$ and $U_i \in \mathcal{S}$, we have

$$\begin{aligned} H(C_{\mathcal{S}}) \geq & H(C_{\mathcal{S}} \mid DK_i) & (1)\\ \geq & H(C_{\mathcal{S}} \mid DK_i) - H(C_{\mathcal{S}} \mid DK_i, M) & (2)\\ = & I(C_{\mathcal{S}}; M \mid DK_i) = H(M \mid DK_i) - H(M \mid DK_i, C_{\mathcal{S}}) = H(M), \end{aligned}$$

where the last equality follows from independence of M and DK_i and the decryption correctness.

Then, we show a construction which meets this bound with equality. A secret key of the one-time pad is assigned for every possible $\mathcal{S} \subset \mathcal{U}$. Namely, $ek := (\{k_{\mathcal{S}} \mid \mathcal{S} \subset \mathcal{U}\})$, $dk_i := (k_{\emptyset}, \{k_{\mathcal{S}} \mid \mathcal{S} \subset \mathcal{U} \wedge U_i \in \mathcal{S}\})$ $(1 \leq i \leq n)$, and $mk := \{k_{\mathcal{S}} \mid \mathcal{S} \subset \mathcal{U} \wedge \mathcal{S} \neq \emptyset\}$, where each $k_{\mathcal{S}}$ is chosen from a finite field uniformly at random. In *Enc*, for any $\mathcal{S}$, it outputs $c_{\mathcal{S}} := m + k_{\emptyset} + k_{\mathcal{S}}$. In *Dec*, if $U_i \in \mathcal{S}$, it can output $m = c_{\mathcal{S}} - k_{\emptyset} - k_{\mathcal{S}}$. In *Upd*, for any $\mathcal{S}$ and $\mathcal{S}'$, it outputs $c_{\mathcal{S}'} := c_{\mathcal{S}} - k_{\mathcal{S}} + k_{\mathcal{S}'}$. This construction is $(\leq n, \leq \omega)$-one-time secure since any $\mathcal{W}$ such that $\mathcal{S} \cap \mathcal{W} = \emptyset$ does not have $k_{\mathcal{S}}$ and SM does not have $k_{\emptyset}$. □

Next, we derive lower bounds on sizes of secret keys when the ciphertext size is optimal (i.e. the ciphertext length is equal to the plaintext length).

Theorem 2. *Let Π be an $(\leq n, \leq \omega)$-one-time secure RS-BE scheme. Then, the following lower bounds hold under the condition $H(C_{\mathcal{S}}) = H(M)$ for any $\mathcal{S} \subset \mathcal{U}$:*

$$\text{(i) } H(EK) \geq \sum_{j=0}^{\omega} \binom{n}{j} H(M), \quad \text{(ii) } H(DK_i) \geq \sum_{j=0}^{\omega} \binom{n-1}{j} H(M) \text{ for any } i \in \{1, 2, \ldots, n\},$$

$$\text{(iii) } H(MK) \geq \left(\sum_{j=0}^{\omega} \binom{n}{j} - 1 \right) H(M).$$

Proof. The proof follows from the following lemmas.

Lemma 1. *For any $\mathcal{S} \subset \mathcal{U}$ and any $\mathcal{W} \subset \mathcal{U}$ such that $\mathcal{W} \cap \mathcal{S} = \emptyset$ and $|\mathcal{W}| \leq \omega$, let Y_i $(1 \leq i \leq k)$ be a privileged set such that $Y_i \cap \mathcal{W} \neq \emptyset$. Then, we have $H(C_{\mathcal{S}} \mid M, C_{Y_1}, \ldots, C_{Y_k}, DK_{\mathcal{W}}) \geq H(M)$ under the condition $H(C_{\mathcal{S}}) = H(M)$ for any $\mathcal{S} \subset \mathcal{U}$.*

Proof. From (1) and (2) in Theorem 1, and the condition $H(C_{\mathcal{S}}) = H(M)$, we have $H(C_{\mathcal{S}} \mid DK_i) = H(C_{\mathcal{S}} \mid DK_i) - H(C_{\mathcal{S}} \mid DK_i, M)$ for any $\mathcal{S} \subset \mathcal{U}$ and $U_i \in \mathcal{S}$. Therefore, we have

$$H(C_{\mathcal{S}} \mid DK_i, M) = 0. \tag{3}$$

For $H(M, C_{\mathcal{S}}, C_{Y_1}, \ldots, C_{Y_k} \mid DK_{\mathcal{W}})$, we have

$$\begin{aligned} H(M, C_{\mathcal{S}}, C_{Y_1}, \ldots, C_{Y_k} \mid DK_{\mathcal{W}}) \\ &= H(C_{\mathcal{S}} \mid DK_{\mathcal{W}}) + H(M \mid DK_{\mathcal{W}}, C_{\mathcal{S}}) + H(C_{Y_1}, \ldots, C_{Y_k} \mid DK_{\mathcal{W}}, C_{\mathcal{S}}, M) \\ &= H(C_{\mathcal{S}} \mid DK_{\mathcal{W}}) + H(M) + H(C_{Y_1}, \ldots, C_{Y_k} \mid DK_{\mathcal{W}}, C_{\mathcal{S}}, M) \qquad (4) \\ &= H(C_{\mathcal{S}} \mid DK_{\mathcal{W}}) + H(M), \qquad (5) \end{aligned}$$

where (4) follows from the condition (1) of Definition 2, and (5) follows from (3) (i.e. $H(C_{Y_j} \mid DK_{\mathcal{W}}, M) = 0$) since $Y_j \cap \mathcal{W} \neq \emptyset$ for any Y_j $(1 \leq j \leq k)$.

On the other hand, for $H(M, C_{\mathcal{S}}, C_{Y_1}, \ldots, C_{Y_k} \mid DK_{\mathcal{W}})$, we have

$$\begin{aligned} H(M, C_{\mathcal{S}}, C_{Y_1}, \ldots, C_{Y_k} \mid DK_{\mathcal{W}}) \\ &= H(M \mid DK_{\mathcal{W}}) + H(C_{Y_1}, \ldots, C_{Y_k} \mid DK_{\mathcal{W}}, M) + H(C_{\mathcal{S}} \mid DK_{\mathcal{W}}, M, C_{Y_1}, \ldots, C_{Y_k}) \\ &= H(M) + H(C_{\mathcal{S}} \mid DK_{\mathcal{W}}, M, C_{Y_1}, \ldots, C_{Y_k}), \qquad (6) \end{aligned}$$

where (6) follows from independence of M and $DK_{\mathcal{W}}$ and the same reason for (5).

Hence, from (5) and (6), we have

$$H(C_{\mathcal{S}} \mid DK_{\mathcal{W}}, M, C_{Y_1}, \ldots, C_{Y_k}) = H(C_{\mathcal{S}} \mid DK_{\mathcal{W}}). \tag{7}$$

In the following, we show $H(C_{\mathcal{S}} \mid DK_{\mathcal{W}}) \geq H(M)$.

For $H(M, C_{\mathcal{S}} \mid DK_{\mathcal{S}}, DK_{\mathcal{W}}, EK)$, we have

$$\begin{aligned} H(M, C_{\mathcal{S}} \mid DK_{\mathcal{S}}, DK_{\mathcal{W}}, EK) &= H(C_{\mathcal{S}} \mid DK_{\mathcal{S}}, DK_{\mathcal{W}}, EK) + H(M \mid DK_{\mathcal{S}}, DK_{\mathcal{W}}, EK, C_{\mathcal{S}}) \\ &= H(C_{\mathcal{S}} \mid DK_{\mathcal{S}}, DK_{\mathcal{W}}, EK), \qquad (8) \end{aligned}$$

where (8) follows from the decryption correctness (i.e. $H(M \mid DK_{\mathcal{S}}, C_{\mathcal{S}}) = 0$).

On the other hand, for $H(M, C_{\mathcal{S}} \mid DK_{\mathcal{S}}, DK_{\mathcal{W}}, EK)$, we have

$$\begin{aligned} H(M, C_{\mathcal{S}} \mid DK_{\mathcal{S}}, DK_{\mathcal{W}}, EK) &= H(M \mid DK_{\mathcal{S}}, DK_{\mathcal{W}}, EK) + H(C_{\mathcal{S}} \mid DK_{\mathcal{S}}, DK_{\mathcal{W}}, EK, M) \\ &= H(M \mid DK_{\mathcal{S}}, DK_{\mathcal{W}}, EK), \qquad (9) \end{aligned}$$

where (9) follows from the algorithm *Enc* (i.e. $H(C_{\mathcal{S}} \mid EK, M) = 0$).

Hence, we have

$$\begin{aligned} H(C_{\mathcal{S}} | DK_{\mathcal{W}}) &\geq H(C_{\mathcal{S}} \mid DK_{\mathcal{S}}, DK_{\mathcal{W}}, EK) \\ &= H(M \mid DK_{\mathcal{S}}, DK_{\mathcal{W}}, EK) \qquad (10) \\ &= H(M), \qquad (11) \end{aligned}$$

where (10) follows from (8) and (9), and (11) follows from independence of M and $(EK, DK_1, \ldots, DK_n)$.

From (7) and (11), we have $H(C_{\mathcal{S}} \mid M, C_{Y_1}, \ldots, C_{Y_k}, DK_{\mathcal{W}}) \geq H(M)$. □

Lemma 2. *We have* $H(EK) \geq \sum_{j=0}^{\omega}\binom{n}{j}H(M)$ *under the condition* $H(C_{\mathcal{S}}) = H(M)$ *for any* $\mathcal{S} \subset \mathcal{U}$*.*

Proof. Let $\mathscr{W} := \{\mathcal{W} \subset \mathcal{U} \mid |\mathcal{W}| \leq \omega\} = \{\mathcal{W}_1, \ldots, \mathcal{W}_t\}$ be the family of all possible sets of colluders, where $t = \sum_{j=0}^{\omega}\binom{n}{j}$. Moreover, let $\mathscr{S}(\mathscr{W}) := \{\mathcal{S}_1, \ldots, \mathcal{S}_t\}$, where $\mathcal{S}_i = \mathcal{U} \setminus \mathcal{W}_i$ such that $\mathcal{W}_i \in \mathscr{W}$ $(1 \leq i \leq t)$. Without loss of generality, $|\mathcal{S}_1| \geq \cdots \geq |\mathcal{S}_t|$. Then, we have

$$\begin{aligned}
H(EK) =& H(EK \mid M) && (12)\\
\geq& I(EK; C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_t} \mid M) = H(C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_t} \mid M) - H(C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_t} \mid M, EK)\\
=& H(C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_t} \mid M) && (13)\\
=& \sum_{j=1}^{t} H(C_{\mathcal{S}_j} \mid M, C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_{j-1}}) \geq \sum_{j=1}^{t} H(C_{\mathcal{S}_j} \mid M, C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_{j-1}}, DK_{\mathcal{W}_j})\\
\geq& \sum_{j=0}^{\omega}\binom{n}{j}H(M), && (14)
\end{aligned}$$

where (12) follows from independence of M and EK, (13) follows from the algorithm *Enc* (i.e. $H(C_{\mathcal{S}_i} \mid EK, M) = 0$ $(1 \leq i \leq t)$), and (14) follows from Lemma 1. □

Lemma 3. *For any* $i \in \{1, \ldots, n\}$*, we have* $H(DK_i) \geq \sum_{j=0}^{\omega}\binom{n-1}{j}H(M)$ *under the condition* $H(C_{\mathcal{S}}) = H(M)$ *for any* $\mathcal{S} \subset \mathcal{U}$*.*

Proof. Let $\mathscr{W}^{(i)} := \{\mathcal{W} \subset \mathcal{U} \setminus \{U_i\} \mid |\mathcal{W}| \leq \omega\} = \{\mathcal{W}_1, \ldots, \mathcal{W}_\ell\}$ be the family of all possible sets of colluders except for sets of colluders containing U_i, where $\ell = \sum_{j=0}^{\omega}\binom{n-1}{j}$. Moreover, let $\mathscr{S}(\mathscr{W}^{(i)}) := \{\mathcal{S}_1, \ldots, \mathcal{S}_\ell\}$, where $\mathcal{S}_i = \mathcal{U} \setminus \mathcal{W}_i$ such that $\mathcal{W}_i \in \mathscr{W}^{(i)}$ $(1 \leq i \leq \ell)$. Without loss of generality, $|\mathcal{S}_1| \geq \cdots \geq |\mathcal{S}_\ell|$. We note $U_i \in \mathcal{S}$ for any $\mathcal{S} \in \mathscr{S}(\mathscr{W}^{(i)})$. Then, we have

$$\begin{aligned}
H(DK_i) =& H(DK_i \mid M) && (15)\\
\geq& I(DK_i; C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_\ell} \mid M) = H(C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_\ell} \mid M) - H(C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_\ell} \mid M, DK_i)\\
=& H(C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_\ell} \mid M) && (16)\\
=& \sum_{j=1}^{\ell} H(C_{\mathcal{S}_j} \mid M, C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_{j-1}}) \geq \sum_{j=1}^{\ell} H(C_{\mathcal{S}_j} \mid M, C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_{j-1}}, DK_{\mathcal{W}_j})\\
\geq& \sum_{j=0}^{\omega}\binom{n-1}{j}H(M), && (17)
\end{aligned}$$

where (15) follows from independence of M and DK_i, (16) follows from (3) in Lemma 1 (i.e. $H(C_{\mathcal{S}_j} \mid DK_i, M) = 0$ $(1 \leq j \leq \ell)$), and (17) follows from Lemma 1. □

Lemma 4. *We have* $H(MK) \geq \left(\sum_{j=0}^{\omega}\binom{n}{j} - 1\right)H(M)$ *under the condition* $H(C_{\mathcal{S}}) = H(M)$ *for any* $\mathcal{S} \subset \mathcal{U}$*.*

Proof. Let $\mathscr{W}$ and $\mathscr{S}(\mathscr{W})$ be the same as those in Lemma 2. Then, we have

$$\begin{aligned}
H(MK) \geq& H(MK \mid C_{\mathcal{S}_1}) \geq I(MK; C_{\mathcal{S}_2}, \ldots, C_{\mathcal{S}_t} \mid C_{\mathcal{S}_1})\\
=& H(C_{\mathcal{S}_2}, \ldots, C_{\mathcal{S}_t} \mid C_{\mathcal{S}_1}) - H(C_{\mathcal{S}_2}, \ldots, C_{\mathcal{S}_t} \mid C_{\mathcal{S}_1}, MK)\\
=& H(C_{\mathcal{S}_2}, \ldots, C_{\mathcal{S}_t} \mid C_{\mathcal{S}_1}) && (18)
\end{aligned}$$

$$= \sum_{j=2}^{t} H(C_{\mathcal{S}_j} \mid C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_{j-1}}) \geq \sum_{j=2}^{t} H(C_{\mathcal{S}_j} \mid M, C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_{j-1}}, DK_{\mathcal{W}_j})$$

$$\geq \left(\sum_{j=0}^{\omega} \binom{n}{j} - 1 \right) H(M), \tag{19}$$

where (18) follows from the algorithm *Upd* (i.e. $H(C_{\mathcal{S}_i} \mid C_{\mathcal{S}_1}, MK) = 0$ $(2 \leq i \leq t)$), and (19) follows from Lemma 1. □

Now, the proof of Theorem 2 is completed. □

As we will see in the next section, the above lower bounds are tight since our construction will meet all the above bounds with equalities. Therefore, we define optimality of constructions of RS-BE as follows.

Definition 3 (Optimality)**.** *A construction of an $(\leq n, \leq \omega)$-one-time secure RS-BE scheme is said to be* optimal *if it meets equality in every bound of (i)–(iii) in Theorem 2.*

In a similar way, we can also derive tight lower bounds on secret keys required for another class of RS-BE schemes, called $(t, \leq \omega)$-one-time secure RS-BE schemes [26, 30, 23, 15], in which the number of privileged users is constant in all time periods, and show an optimal construction under this condition (see Appendix B for details).

4 Construction

In this section, we propose a construction of an $(\leq n, \leq \omega)$-one-time secure RS-BE scheme with a trade-off between ciphertext sizes and secret-key sizes. Namely, we construct an $(\leq n, \leq \omega)$-one-time secure RS-BE scheme with efficient secret-key sizes by allowing a ciphertext to become larger, though we considered lower bounds on the secret-key sizes only when the ciphertext size is equal to the plaintext size in the previous section. To the best of our knowledge, there are only two ways of efficient constructing unconditionally secure BE schemes with such a trade-off: One is *the block-design approach* for $(t, \leq \omega)$-one-time secure BE schemes, which was proposed by Blundo et al. [10]; and the other is *the multi-KPSs approach* for $(\leq n, \leq \omega)$-one-time secure BE schemes, which was recently proposed by Watanabe and Shikata [40]. The block design approach in [10] can be applied to $(t, \leq \omega)$-one-time secure BE schemes since the cardinality of $\mathcal{S}$ is always exactly t, and therefore, it seems difficult to apply the former technique for constructing $(\leq n, \leq \omega)$-one-time secure BE schemes. Therefore, we adopt the latter technique, and improve it by using algebraic structures.

The idea of their original construction is as follows: For $(\leq n, \leq \omega)$-one-time secure BE schemes where the maximum ciphertext size is δ times as large as the plaintext size, the user set $\mathcal{U}$ is split into δ subsets $\mathcal{U}_1, \mathcal{U}_2, \ldots, \mathcal{U}_\delta$ such that $|\mathcal{U}_1| \geq |\mathcal{U}_2| \geq \cdots \geq |\mathcal{U}_\delta|$. Then, we apply an $(\leq |\mathcal{U}_j|, \leq \omega_j)$-KPS to each subset $\mathcal{U}_j$, where $\omega_j := \min\{|\mathcal{U}_j| - 1, \omega\}$. The encryption procedures are just generating session keys for each privileged subset $\mathcal{S}_j := \mathcal{U}_j \cap \mathcal{S}$ and computing at most δ one-time pads of a plaintext by using each session key. They showed the optimal condition of $(|\mathcal{U}_1|, |\mathcal{U}_2|, \ldots, |\mathcal{U}_\delta|)$ for minimizing secret-key sizes as follows:

Proposition 1 (Theorem 2 and Corollary 2 in [40])**.** *Let $a := \lfloor n/\delta \rfloor$, $\delta_2 := n \bmod \delta$, and $\delta_1 := \delta - \delta_2$. When we apply an optimal construction of each underlying KPS (e.g., the Fiat–Naor KPS [18]) to the above $(\leq n, \leq \omega)$-one-time secure BE scheme where the maximum ciphertext size is δ times as* *large as the plaintext size, then sizes of the secret keys are minimized when* $|\mathcal{U}_1| = |\mathcal{U}_2| = \cdots = |\mathcal{U}_{\delta_1}| = a$ *and* $|\mathcal{U}_{\delta_1+1}| = |\mathcal{U}_{\delta_1+2}| = \cdots = |\mathcal{U}_\delta| = a+1$. *Namely, we have*

$$\text{(i)}\ \log|\mathcal{EK}| = \left(\delta_1 \sum_{j=0}^{\tilde{\omega}} \binom{a}{j} + \delta_2 \sum_{j=0}^{\hat{\omega}} \binom{a+1}{j}\right) \log|\mathcal{M}|,$$

$$\text{(ii)}\ \sum_{i=1}^{n} \log|\mathcal{DK}_i| = \left(\delta_1 a \sum_{j=0}^{\tilde{\omega}} \binom{a-1}{j} + \delta_2(a+1) \sum_{j=0}^{\hat{\omega}} \binom{a}{j}\right) \log|\mathcal{M}|,$$

where $\tilde{\omega} := \min\{a-1, \omega\}$ *and* $\hat{\omega} := \min\{a, \omega\}$.

We construct an $(\leq n, \leq \omega)$-one-time secure RS-BE scheme based on the above construction with the following improvement: We here give the basic idea. For simplicity, suppose that $n/\delta \in \mathbb{N}$. Then, each user subset can be expressed as $\mathcal{U}_j := \{U_j^{(1)}, \ldots, U_j^{(a)}\} = \{U_{(j-1)a+1}, \ldots, U_{ja}\}$ $(1 \leq j \leq \delta)$. Since $(\leq a, \leq \tilde{\omega})$-KPSs are applied to each subset in the original construction, $U_i^{(1)}$, $U_i^{(2)}$, …, and $U_i^{(\delta)}$ have the "same" but completely independent decryption keys $dk_i^{(1)}$, $dk_i^{(2)}$, …, and $dk_i^{(\delta)}$, respectively. Therefore, we correlate the "same" decryption keys with each other, and thus we succeed in reducing sizes of an encryption key (and maintenance key).

The detailed construction of an $(\leq n, \leq \omega)$-one-time secure RS-BE scheme $\Pi = $ (*Setup*, *Enc*, *Dec*, *Upd*) is as follows.

1. $(ek, mk, dk_1, \ldots, dk_n) \leftarrow$ *Setup*(n): Let q be a prime power such that $q > n$, and $\mathbb{F}_q$ be a finite field with q elements. Let $a := \lfloor n/\delta \rfloor$, $\delta_2 := n \bmod \delta$, and $\delta_1 := \delta - \delta_2$. Without loss of generality, let $\mathcal{U}_j := \{U_1^{(j)}, U_2^{(j)}, \ldots, U_a^{(j)}\} = \{U_{(j-1)a+1}, \ldots, U_{ja}\}$ for $j \in \{1, 2, \ldots, \delta_1\}$ and $\mathcal{U}_j := \{U_1^{(j)}, U_2^{(j)}, \ldots, U_{a+1}^{(j)}\} = \{U_{\delta_1 a+(j-\delta_1-1)(a+1)+1}, \ldots, U_{\delta_1 a+(j-\delta_1)(a+1)}\}$ for $j \in \{\delta_1+1, \delta_1+2, \ldots, \delta\}$.[2] Consider virtual user sets $\widetilde{\mathcal{U}} := \{V_1, V_2, \ldots, V_a\}$ and $\widehat{\mathcal{U}} := \widetilde{\mathcal{U}} \cup \{V_{a+1}\}$, and define the following families of virtual subsets:

$$\widetilde{\mathscr{W}} := \{\mathcal{W} \subset \widetilde{\mathcal{U}} \mid |\mathcal{W}| \leq \tilde{\omega}\},\quad \widetilde{\mathscr{W}}^{(i)} := \{\mathcal{W} \subset \widetilde{\mathcal{U}} \mid \mathcal{W} \in \widetilde{\mathscr{W}} \wedge V_i \notin \mathcal{W}\},$$
$$\widetilde{\mathscr{W}}(\mathcal{S} \subset \widetilde{\mathcal{U}}) := \{\mathcal{W} \in \widetilde{\mathscr{W}} \mid (\mathcal{W} \cap \mathcal{S} = \emptyset) \wedge (|\mathcal{W}| = \min\{\tilde{\omega}, a - |\mathcal{S}|\})\},$$
$$\widehat{\mathscr{W}} := \{\mathcal{W} \subset \widehat{\mathcal{U}} \mid |\mathcal{W}| \leq \hat{\omega}\},\quad \widehat{\mathscr{W}}^{(i)} := \{\mathcal{W} \subset \widehat{\mathcal{U}} \mid \mathcal{W} \in \widehat{\mathscr{W}} \wedge V_i \notin \mathcal{W}\},$$
$$\widehat{\mathscr{W}}(\mathcal{S} \subset \widehat{\mathcal{U}}) := \{\mathcal{W} \in \widehat{\mathscr{W}} \mid (\mathcal{W} \cap \mathcal{S} = \emptyset) \wedge (|\mathcal{W}| = \min\{\hat{\omega}, a - |\mathcal{S}|\})\},$$

where $\tilde{\omega} := \min\{a-1, \omega\}$ and $\hat{\omega} := \min\{a, \omega\}$. Let $\tilde{k} := \min\{\omega, \delta - 1\}$ and $\hat{k} := \{\omega, \delta_2 - 1\}$. Choose two kinds of polynomials over $\mathbb{F}_q$ uniformly at random as follows:

$$f_{\mathcal{W}}(x) := r_{\mathcal{W}}^{(0)} + r_{\mathcal{W}}^{(1)} x + \cdots + r_{\mathcal{W}}^{(\tilde{k})} x^{\tilde{k}} \text{ for every } \mathcal{W} \in \widetilde{\mathscr{W}},$$
$$f_{\mathcal{W}}(x) := r_{\mathcal{W}}^{(0)} + r_{\mathcal{W}}^{(1)} x + \cdots + r_{\mathcal{W}}^{(\hat{k})} x^{\hat{k}} \text{ for every } \mathcal{W} \in \widehat{\mathscr{W}} \setminus \widetilde{\mathscr{W}}.$$

Furthermore, also compute $f'_\emptyset(x) := f_\emptyset(x) - r_\emptyset^{(0)}$. Set $ek := \{f_{\mathcal{W}}(x) \mid \mathcal{W} \in \widehat{\mathscr{W}}\}$, $mk := \{f_{\mathcal{W}}(x) \mid \mathcal{W} \in \widehat{\mathscr{W}} \setminus \{\emptyset\}\} \cup \{f'_\emptyset(x)\}$. For every $U_h = U_i^{(j)}$, set $dk_h = dk_i^{(j)} := \{f_{\mathcal{W}}(j) \mid \mathcal{W} \in \widetilde{\mathscr{W}}^{(i)}\}$ if $1 \leq h \leq \delta_1 a$, or $dk_h = dk_i^{(j)} := \{f_{\mathcal{W}}(j) \mid \mathcal{W} \in \widehat{\mathscr{W}}^{(i)}\}$ if $\delta_1 a + 1 \leq h \leq n$.[3] Output $(ek, mk, dk_1, \ldots, dk_n)$.

[2]For example, when $n = 8$ and $\delta = 3$, then $\mathcal{U}_1 := \{U_1^{(1)}, U_2^{(1)}\} = \{U_1, U_2\}$, $\mathcal{U}_2 := \{U_1^{(2)}, U_2^{(2)}, U_3^{(2)}\} = \{U_3, U_4, U_5\}$, and $\mathcal{U}_3 := \{U_1^{(3)}, U_2^{(3)}, U_3^{(3)}\} = \{U_6, U_7, U_8\}$.

[3]For readability, we consider $1, 2, \ldots, \delta$ denote elements of $\mathbb{F}_q$.

2. $c_{\mathcal{S}} \leftarrow Enc(ek, m, \mathcal{S})$: For every j such that $1 \le j \le \delta_1$, let $\mathcal{S}_j := \{V_i \in \widetilde{\mathcal{U}} \mid U_i^{(j)} \in \mathcal{S} \cap \mathcal{U}_j\}$. For a plaintext $m \in \mathbb{F}_q$, compute $c_j := m + f_{\emptyset}(j) + \sum_{\mathcal{W} \in \widetilde{\mathscr{W}}(\mathcal{S}_j)} f_{\mathcal{W}}(j)$. For every j such that $\delta_1 + 1 \le j \le \delta$, let $\mathcal{S}_j := \{V_i \in \widehat{\mathcal{U}} \mid U_i^{(j)} \in \mathcal{S} \cap \mathcal{U}_j\}$. For the plaintext $m \in \mathbb{F}_q$, compute $c_j := m + f_{\emptyset}(j) + \sum_{\mathcal{W} \in \widehat{\mathscr{W}}(\mathcal{S}_j)} f_{\mathcal{W}}(j)$ if $\widehat{\mathcal{S}}_j \neq \emptyset$. Output $c_{\mathcal{S}} := \{c_j\}_{\mathcal{S}_j \neq \emptyset}$.

3. m or $\perp \leftarrow Dec(dk_h, c_{\mathcal{S}}, \mathcal{S}, U_h)$: If $U_h \notin \mathcal{S}$, output $\perp$. Otherwise, suppose that $U_h = U_i^{(j)} \in \mathcal{U}_j$. If $j \le \delta_1$, let $\mathcal{S}_j := \{V_i \in \widetilde{\mathcal{U}} \mid U_i^{(j)} \in \mathcal{U}_j \cap \mathcal{S}\}$, and output $m = c_j - f_{\emptyset}(j) - \sum_{\mathcal{W} \in \widetilde{\mathscr{W}}(\mathcal{S}_j)} f_{\mathcal{W}}(j)$. Otherwise, let $\mathcal{S}_j := \{V_i \in \widehat{\mathcal{U}} \mid U_i^{(j)} \in \mathcal{U}_j \cap \mathcal{S}\}$, and output $m = c_j - f_{\emptyset}(j) - \sum_{\mathcal{W} \in \widehat{\mathscr{W}}(\mathcal{S}_j)} f_{\mathcal{W}}(j)$.

4. $c_{\mathcal{S}'}$ or $\perp \leftarrow Upd(mk, c_{\mathcal{S}}, \mathcal{S}, \mathcal{S}')$: Without loss of generality, choose some $c_j \in c_{\mathcal{S}}$ such that $|\mathcal{U}_j| = a$. Compute $c_{\emptyset} := c_j - f'_{\emptyset}(j) - \sum_{\mathcal{W} \in \widetilde{\mathscr{W}}(\mathcal{S}_j)} f_{\mathcal{W}}(j) = m + r_{\emptyset}^{(0)}$, where $\mathcal{S}_j := \{V_i \in \widetilde{\mathcal{U}} \mid U_i^{(j)} \in \mathcal{S} \cap \mathcal{U}_j\}$. Note that $c_{\emptyset}$ can be computed by choosing c_j such that $|\mathcal{U}_j| = a + 1$. for every j such that $1 \le j \le \delta_1$, let $\mathcal{S}'_j := \{V_i \in \widetilde{\mathcal{U}} \mid U_i^{(j)} \in \mathcal{S}' \cap \mathcal{U}_j\}$. If $\mathcal{S}'_j \neq \emptyset$, compute $c_j := c_{\emptyset} + f'_{\emptyset}(j) + \sum_{\mathcal{W} \in \widetilde{\mathscr{W}}(\mathcal{S}'_j)} f_{\mathcal{W}}(j)$. For every j such that $\delta_1 + 1 \le j \le \delta$, let $\mathcal{S}'_j := \{V_i \in \widehat{\mathcal{U}} \mid U_i^{(j)} \in \mathcal{S}' \cap \mathcal{U}_j\}$. If $\mathcal{S}'_j \neq \emptyset$, compute $c_j := c_{\emptyset} + f'_{\emptyset}(j) + \sum_{\mathcal{W} \in \widehat{\mathscr{W}}(\mathcal{S}'_j)} f_{\mathcal{W}}(j)$. Output $c_{\mathcal{S}} := \{c_j\}_{\mathcal{S}'_j \neq \emptyset}$.

Theorem 3. *Let* Π *be the resulting RS-BE scheme where the maximum ciphertext size is* δ *times as large as the plaintext size by the above construction. Then,* Π *is* $(\le n, \le \omega)$*-one-time secure. In particular,* Π *is optimal when* δ*=1.*

Proof. First, we show the above construction meets the condition (1) in Definition 2. Without loss of generality, we consider $|\mathcal{S}| = n - \omega$ and $|\mathcal{W}| = \omega$. Let $\mathcal{S}_j := \mathcal{U}_j \cap \mathcal{S}$ and $\mathcal{W}_j := \mathcal{U}_j \setminus \mathcal{S}_j$. As in the Fiat–Naor KPS [18], we can easily prove that in each subset $\mathcal{U}_j$, $\mathcal{W}_j$ cannot obtain any information on m from c_j since they do not have at least one randomness $f_{\mathcal{W}}(j)$, where $\mathcal{W} := \{V_i \in \widetilde{\mathcal{U}} \mid U_i^{(j)} \in \mathcal{W}_j\}$, used for the ciphertext c_j. Therefore, we prove that $\mathcal{W}_j$ cannot compute such $f_{\mathcal{W}}(j)$ with decryption keys of other colluders (i.e., $\mathcal{W}_1, \ldots, \mathcal{W}_{j-1}, \mathcal{W}_{j+1}, \ldots, \mathcal{W}_{\delta}$). There are the following three cases: (i) $\omega < \delta_2 < \delta$; (ii) $\delta_2 \le \omega < \delta$; and (iii) $\delta_2 < \delta \le \omega$. We here consider the cases (i) and (iii). (i) For every $\mathcal{W} \in \widetilde{\mathscr{W}}$, the colluders can get at most ω values of the polynomial $f_{\mathcal{W}}(x)$. However, they cannot guess at least one coefficient of $f_{\mathcal{W}}(x)$ with probability larger than $1/q$ since the degree of $f_{\mathcal{W}}(x)$ is ω. Furthermore, for every $\mathcal{W} \in \widehat{\mathscr{W}} \setminus \widetilde{\mathscr{W}}$, the colluders can also get at most ω values of the polynomial $f_{\mathcal{W}}(x)$, and hence they cannot guess at least one coefficient of $f_{\mathcal{W}}(x)$ with probability larger than $1/q$ for the same reason. (iii) The colluders may get δ values of the polynomial $f_{\mathcal{W}}(x)$ for some $\mathcal{W} \in \widetilde{\mathscr{W}}$, and then they can guess the polynomial. However, they cannot get any new information from this since they already have all useful information (i.e., $f_{\mathcal{W}}(1), f_{\mathcal{W}}(2), \ldots, f_{\mathcal{W}}(\delta)$). If the colluders can also get at most $\delta - 1$ values of the polynomial $f_{\mathcal{W}}(x)$ for some $\mathcal{W} \in \widetilde{\mathscr{W}}$, they cannot guess at least one coefficient of $f_{\mathcal{W}}(x)$ with probability larger than $1/q$ the degree of $f_{\mathcal{W}}(x)$ is $\delta - 1$. The same holds for every $\mathcal{W} \in \widehat{\mathscr{W}} \setminus \widetilde{\mathscr{W}}$. We can prove the case (ii) in a way similar to the above cases. Hence, for any $\mathcal{S} \subset \mathcal{U}$, and any $\mathcal{W} \subset \mathcal{U}$ such that $\mathcal{S} \cap \mathcal{W} = \emptyset$ and $|\mathcal{W}| \le \omega$, $H(M \mid C_{\mathcal{S}}, DK_{\mathcal{W}}) = H(M)$.

Next, we show the above construction meets the condition (2) in Definition 2. $r_{\emptyset}^{(0)}$ is always used for computing c_j for any $\mathcal{S} \subset \mathcal{U}$ and any $j \in \{1, 2, \ldots, \delta\}$, whereas SM does not have $r_{\emptyset}^{(0)}$. Hence, he can only guess m randomly as in the one-time pad. Thus, for any $\mathcal{S} \subset \mathcal{U}$, $H(M \mid C_{\mathcal{S}}, MK) = H(M)$.

Moreover, it is straightforward to see that the above construction is optimal when $\delta = 1$. □

Remark 3. *The sizes of secret keys in the above construction are as follows:*

$$\text{(i)}\ \log|\mathcal{EK}| = \left((\tilde{k}-\hat{k})\sum_{j=0}^{\tilde{\omega}}\binom{a}{j} + (\hat{k}+1)\sum_{j=0}^{\hat{\omega}}\binom{a+1}{j}\right)\log|\mathcal{M}|,$$

$$\text{(ii)}\ \sum_{i=1}^{n}\log|\mathcal{DK}_i| = \left(\delta_1 a\sum_{j=0}^{\tilde{\omega}}\binom{a-1}{j} + \delta_2(a+1)\sum_{j=0}^{\hat{\omega}}\binom{a}{j}\right)\log|\mathcal{M}|,$$

$$\text{(iii)}\ \log|\mathcal{MK}| = \left((\tilde{k}-\hat{k})\sum_{j=0}^{\tilde{\omega}}\binom{a}{j} + (\hat{k}+1)\sum_{j=0}^{\hat{\omega}}\binom{a+1}{j} - 1\right)\log|\mathcal{M}|.$$

Note that $\tilde{k} := \min\{\omega, \delta-1\}$, $\hat{k} := \min\{\omega, \delta_2-1\}$, $\tilde{\omega} := \min\{a-1, \omega\}$, and $\hat{\omega} := \min\{a, \omega\}$. This means that the larger the ciphertext size (i.e., δ) is, the smaller sizes of the encryption and maintenance keys are. More precisely, our construction is more efficient than the original construction in [40] when $\delta > \omega$. On the other hand, the decryption-key size is the same as that in [40] (i.e., a construction from δ_1 $(\leq a, \leq \tilde{\omega})$-KPS and δ_2 $(\leq a+1, \leq \hat{\omega})$-KPS). Therefore, in our construction we have to assume $\delta_1\tilde{\omega} + \delta_2\hat{\omega}$ colluders in total, though there are actually only ω colluders at most. Therefore, δ must satisfy $\omega \geq \delta_1\tilde{\omega} + \delta_2\hat{\omega}$ for a non-redundant construction in the sense of the number of colluders. Since it holds $\omega \geq \delta_1(a-1) + \delta_2 a = \delta a - \delta_1 = \delta(\frac{n-(n \bmod \delta)}{\delta}) - \delta_1 = n - \delta$, such a non-redundant RS-BE scheme can be achieved when $\delta = 1$ or $\delta \geq n - \omega$. Hence, in terms of the encryption and maintenance key sizes, our construction is more efficient than a construction based on [40] if $n \geq 2\omega + 1$ especially when $\delta \geq n - \omega$. Note that by setting mk to an empty string, the above construction is also the most efficient $(\leq n, \leq \omega)$-one-time secure BE scheme ever.

5 Robust Construction

We now consider a scenario in which a maliciously behaving storage manager can try to modify the encrypted plaintext. This is related to *non-malleability* in the context of ordinary encryption. In an RS-BE scheme, malleability may cause a serious problem since the ciphertext is periodically updated, but an improper update carried out by a malicious storage manager may not be immediately detectable by the users. More specifically, we consider security against a storage manager who tries to modify a ciphertext so that a user in the privileged set obtains a modified plaintext which differs from an original plaintext encrypted by the sender. In addition to this, since ciphertexts of RS-BE schemes are stored in external storage such as cloud storage (in other words, the ciphertexts are accessible at any time), we should also consider security against such a modification attack by colluders. Formally, we consider two types of adversaries as in Definition 2, and define the robustness of RS-BE as follows.

Definition 4 (Robust RS-BE)**.** *Let Π be an $(\leq n, \leq \omega)$-one-time secure RS-BE scheme. Π is said to be γ-robust if $\max\{P_1, P_2\} \leq \gamma$, where P_1 and P_2 are defined as follows:*

(1) For any $\mathcal{S}_1, \ldots, \mathcal{S}_k \subset \mathcal{U}$ $(1 \leq k \leq 2^n)$, any $U_i \in \mathcal{S}_k$, and any $\mathcal{W} \subset \mathcal{U}$ such that $\left(\bigcup_{i=1}^{k}\mathcal{S}_i\right) \cap \mathcal{W} = \emptyset$ and $|\mathcal{W}| \leq \omega$, we define $P_1(\mathcal{S}_1, \ldots, \mathcal{S}_k, U_i, \mathcal{W})$ as:

$$P_1(\mathcal{S}_1, \ldots, \mathcal{S}_k, U_i, \mathcal{W}) := \max_{c'_{\mathcal{S}_k}} \max_{c_{\mathcal{S}_1},\ldots,c_{\mathcal{S}_k}} \max_{dk_{\mathcal{W}}} \Pr(Dec(dk_i, c'_{\mathcal{S}_k}, \mathcal{S}_k, U_i) \notin \{m, \perp\} \mid c_{\mathcal{S}_1}, \ldots, c_{\mathcal{S}_k}, dk_{\mathcal{W}}),$$

where $c_{\mathcal{S}_j} = Enc(ek, m, \mathcal{S}_j)$ $(1 \leq j \leq k)$. Note that $Enc(ek, m, \mathcal{S}_{j+1}) = Upd(mk, Enc(ek, m, \mathcal{S}_j), \mathcal{S}_j, \mathcal{S}_{j+1})$ for any $\mathcal{S}_j, \mathcal{S}_{j+1}$ $(1 \leq j \leq k-1)$ (the updating correctness). Then, P_1 is defined as $P_1 := \max_{\mathcal{S}_1,\ldots,\mathcal{S}_k,U_i,\mathcal{W}} P_1(\mathcal{S}_1, \ldots, \mathcal{S}_k, U_i, \mathcal{W})$.

(2) For any $\mathcal{S}, \mathcal{S}' \subset \mathcal{U}$ and any $U_i \in \mathcal{S}'$, we define $P_2(\mathcal{S}, \mathcal{S}', U_i)$ as:

$$P_2(\mathcal{S}, \mathcal{S}', U_i) := \max_{c'_{\mathcal{S}'}} \max_{c_{\mathcal{S}}} \max_{mk} \Pr(\mathit{Dec}(dk_i, c'_{\mathcal{S}'}, \mathcal{S}', U_i) \notin \{m, \perp\} \mid c_{\mathcal{S}}, mk),$$

where $c_{\mathcal{S}} = \mathit{Enc}(ek, m, \mathcal{S})$. Then, P_2 is defined as $P_2 := \max_{\mathcal{S}, \mathcal{S}', U_i} P_2(\mathcal{S}, \mathcal{S}', U_i)$.

We can derive a lower bound on the ciphertext-size as follows.

Theorem 4. *Let Π be an γ-robust and $(\le n, \le \omega)$-one-time secure RS-BE scheme. Then, for any $\mathcal{S} \subset \mathcal{U}$ it holds that $|\mathcal{C}_{\mathcal{S}}| \ge \frac{|\mathcal{M}|-1}{\gamma^2} + 1$.*

Proof. First, let $\mathcal{C}_i(m, \mathcal{S}) := \{c_{\mathcal{S}} \in \mathcal{C}_{\mathcal{S}} \mid \mathit{Dec}(dk_i, c_{\mathcal{S}}, \mathcal{S}, U_i) = m \text{ for some } dk_i \in \mathcal{DK}_i\}$. We fix arbitrary $m \in \mathcal{M}$, $U_i \in \mathcal{U}$, and $\mathcal{S} \subset \mathcal{U}$ such that $U_i \in \mathcal{S}$. Then, we have

$$\begin{aligned}
\gamma &\ge \max_{c'_{\mathcal{S}}} \max_{c_{\mathcal{S}}} \Pr(\mathit{Dec}(dk_i, c'_{\mathcal{S}}, \mathcal{S}, U_i) \notin \{m, \perp\} \mid c_{\mathcal{S}}) && (20)\\
&\ge \max_{m'} \max_{c'_{\mathcal{S}}} \max_{c_{\mathcal{S}}} \Pr(\mathit{Dec}(dk_i, c'_{\mathcal{S}}, \mathcal{S}, U_i) = m' \mid c_{\mathcal{S}})\\
&\ge \max_{m'} \frac{1}{|\mathcal{C}_i(m', \mathcal{S})|} \sum_{c'_{\mathcal{S}} \in \mathcal{C}_i(m', \mathcal{S})} \max_{c_{\mathcal{S}}} \Pr(\mathit{Dec}(dk_i, c'_{\mathcal{S}}, \mathcal{S}, U_i) = m' \mid c_{\mathcal{S}}) && (21)\\
&\ge \frac{1}{|\mathcal{C}_i(m', \mathcal{S})|},
\end{aligned}$$

where (20) follows from $P_2(\mathcal{S}, \mathcal{S}, U_i) \ge P_1(\mathcal{S}, U_i, \mathcal{W} = \emptyset) = \max_{c'_{\mathcal{S}}} \max_{c_{\mathcal{S}}} \Pr(\mathit{Dec}(dk_i, c'_{\mathcal{S}}, \mathcal{S}, U_i) \notin \{m, \perp\} \mid c_{\mathcal{S}})$, and (21) follows from the following simple fact: For n real numbers $x_1, x_2, \ldots, x_n \in \mathbb{R}$, it holds that $\max\{x_i\}_{i=1}^n \ge \frac{1}{n} \sum_{i=1}^n x_i$. Therefore, we have $|\mathcal{C}_i(m', \mathcal{S})| \ge 1/\gamma$.

On the other hand, we have

$$\begin{aligned}
\gamma &\ge \max_{c'_{\mathcal{S}}} \max_{c_{\mathcal{S}}} \Pr(\mathit{Dec}(dk_i, c'_{\mathcal{S}}, \mathcal{S}, U_i) \notin \{m, \perp\} \mid c_{\mathcal{S}})\\
&\ge \frac{|\bigcup_{m' \neq m} \mathcal{C}_i(m', \mathcal{S})|}{|\mathcal{C}_{\mathcal{S}}| - 1} && (22)\\
&= \frac{\sum_{m' \neq m} |\mathcal{C}_i(m', \mathcal{S})|}{|\mathcal{C}_{\mathcal{S}}| - 1} && (23)\\
&\ge \frac{|\mathcal{M}| - 1}{(|\mathcal{C}_{\mathcal{S}}| - 1)\gamma}, && (24)
\end{aligned}$$

where (22) follows from probability of random guessing of $c'_{\mathcal{S}}$ such that $\mathit{Dec}(dk_i, c'_{\mathcal{S}}, \mathcal{S}, U_i) \notin \{m, \perp\}$, (23) follows from the fact that the Dec algorithm is deterministic, and (24) follows from $|\mathcal{C}_i(m', \mathcal{S})| \ge 1/\gamma$. Hence, we have $|\mathcal{C}_{\mathcal{S}}| \ge (|\mathcal{M}| - 1)/\gamma^2 + 1$. □

We can construct a robust scheme by using an *algebraic manipulation detection code* (AMD-code), which is defined as follows.

Definition 5 (AMD-code [16])**.** *Let $\mathcal{M}_{\text{AMD}}$ be a set of messages such that $|\mathcal{M}_{\text{AMD}}| = \eta$, and $\mathbb{G}$ be a commutative group of order λ. An algebraic manipulation detection code (AMD-code) Φ consists of the following two-tuple algorithms (Encode, Decode), where Encode is a probabilistic encoding map $\mathsf{Encode} : \mathcal{M}_{\text{AMD}} \to \mathbb{G}$ and a deterministic decoding map $\mathsf{Decode} : \mathbb{G} \to \mathcal{M}_{\text{AMD}} \cup \{\perp\}$ such that $\mathsf{Decode}(\mathsf{Encode}(m)) = m$ with probability one for every $m \in \mathcal{M}_{\text{AMD}}$. Φ is an $(\eta, \lambda, \varepsilon)$-AMD-code if for every $m \in \mathcal{M}_{\text{AMD}}$ and for every $\Delta \in \mathbb{G}$, the probability that $\mathsf{Decode}(\mathsf{Encode}(m) + \Delta) \notin \{m, \perp\}$ is at most ε.*

A robust RS-BE scheme is constructed by modifying the construction proposed in Section 4 as follows: Before encrypting a plaintext $m \in \mathbb{F}_q$, the *Enc* algorithm runs $\hat{m} \leftarrow \mathsf{Encode}(m)$; and after decrypting a ciphertext, then the *Dec* algorithm runs $m \leftarrow \mathsf{Decode}(\tilde{m})$, where $\tilde{m}$ is the decryption result. We assume outputs of Encode and Decode are properly encoded into (a sequence of) elements of $\mathbb{F}_q$. Note that most of this construction is realized by using algebraic structure (i.e., over $\mathbb{F}_q$).

Theorem 5. *If Φ is an $(\eta, \lambda, \varepsilon)$-AMD-code, then the resulting RS-BE scheme Π by the above construction is $(\leq n, \leq \omega)$-one-time secure and ε-robust.*

Proof Sketch. It is easy to see the above construction is $(\leq n, \leq \omega)$-one-time secure. Let $k_{\mathcal{S}}$ be a part of a key in the ciphertext $c_{\mathcal{S}}$ (i.e., $c_{\mathcal{S}} = \mathsf{Encode}(m) + k_{\mathcal{S}}$). If an adversary, SM or colluders, applies any algebraic operation F to the ciphertext, then it holds $F(c_{\mathcal{S}}) = F(\mathsf{Encode}(m) + k_{\mathcal{S}}) = \mathsf{Encode}(m) + \Delta + k_{\mathcal{S}}$. Since $\Pr(\mathsf{Decode}(\mathsf{Encode}(m) + \Delta) \notin \{m, \perp\}) \leq \varepsilon$, it holds $\max\{P_1, P_2\} \leq \varepsilon$. $\square$

Remark 4. *If we want to construct an $(\leq n, \leq \omega)$-one-time secure and γ-robust RS-BE scheme over $\mathbb{F}_q$, we have $|\mathcal{C}_{\mathcal{S}}| \geq (|\mathcal{M}| - 1)/\gamma^2 + 1 = (q^2(q-1))/c^2 + 1 = q^3/c^2 - o(q^3)$, where we assume $\mathcal{M} = \mathbb{F}_q$ and $\gamma = c/q$ for some constant c. This means that we cannot realize a robust RS-BE scheme where a ciphertext consists of only one or two elements of $\mathbb{F}_q$.*

Actually, for example, one of the most efficient construction of an $(\eta, \lambda, \varepsilon)$-AMD-code, where $\eta = q$, $\lambda = q^3$, and $\varepsilon = 1/q$, is as follows. Encode: *For $m \in \mathbb{F}_q$, choose $r \in \mathbb{F}_q$ and output $(m, r, mr) \in \mathbb{F}_q^3$.* Decode: *For (m', r', π), output m' if it holds $m'r' = \pi$. Otherwise, output $\perp$. If we apply the above specific $(q, q^3, 1/q)$-AMD-code to our robust construction, then we have $|\mathcal{M}| = q$, $|\mathcal{C}_{\mathcal{S}}| = q^{3\delta}$, and $\gamma = 1/q$. Therefore, since $(|\mathcal{M}| - 1)/\gamma^2 + 1 = q^2(q-1) + 1$, the construction is almost optimal in the sense of the ciphertext size if the underlying $(\leq n, \leq \omega)$-one-time secure RS-BE scheme proposed in the previous section is also optimal in the sense of the ciphertext size (i.e., if $\delta = 1$).*

Furthermore, the above specific construction requires triple sizes of each parameter in the normal (i.e., non-robust) construction. Then, the proposed robust construction seems to achieve optimal parameter sizes if the underlying RS-BE scheme is optimal (only when $\delta = 1$).

Acknowledgments. We would like to thank "Shin-Akarui-Angou-Benkyou-Kai" for their valuable comments. Yohei Watanabe is supported by JSPS Research Fellowships for Young Scientists. This work (Yohei Watanabe) was supported by Grant-in-Aid for JSPS Fellows Grant Number 25·3998. This work (Junji Shikata) was supported by JSPS KAKENHI Grant Number 15H02710, and it was partially conducted under the auspices of the MEXT Program for Promoting the Reform of National Universities.

References

[1] G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. Peterson, and D. Song. Remote data checking using provable data possession. *ACM Trans. Inf. Syst. Secur.*, 14(1):12:1–12:34, June 2011.

[2] N. Attrapadung and H. Imai. Attribute-based encryption supporting direct/indirect revocation modes. In M. Parker, editor, *Cryptography and Coding*, volume 5921, pages 278–300. Springer Berlin Heidelberg, 2009.

[3] E. Ayday, E. De Cristofaro, J. Hubaux, and G. Tsudik. The chills and thrills of whole genome sequencing. *Computer*, PP(99):1, 2013.

[4] E. Ayday, E. De Cristofaro, J.-P. Hubaux, and G. Tsudik. Whole genome sequencing: Revolutionary medicine or privacy nightmare? *Computer*, 48(2):58–66, Feb 2015.

[5] E. Barker, W. Barker, W. Burr, W. Polk, and M. Smid. Recommendation for key management – part 1: General (revision 3). NIST Special Publication 800-57, July 2012.

[6] S. Berkovits. How to broadcast a secret. In D. Davies, editor, *Advances in Cryptology – EUROCRYPT '91*, volume 547, pages 535–541. Springer Berlin Heidelberg, 1991.

[7] R. Blom. An optimal class of symmetric key generation systems. In T. Beth, N. Cot, and I. Ingemarsson, editors, *Advances in Cryptology – EUROCRYPT'84*, volume 209 of *Lecture Notes in Computer Science*, pages 335–338. Springer Berlin Heidelberg, 1985.

[8] C. Blundo and A. Cresti. Space requirements for broadcast encryption. In A. Santis, editor, *Advances in Cryptology – EUROCRYPT'94*, volume 950, pages 287–298. Springer Berlin Heidelberg, 1995.

[9] C. Blundo, A. Cresti, A. Santis, and U. Vaccaro. Fully dynamic secret sharing schemes. In D. Stinson, editor, *Advances in Cryptology – CRYPTO' 93*, volume 773, pages 110–125. Springer Berlin Heidelberg, 1994.

[10] C. Blundo, L. Mattos, and D. Stinson. Trade-offs between communication and storage in unconditionally secure schemes for broadcast encryption and interactive key distribution. In N. Koblitz, editor, *Advances in Cryptology – CRYPTO '96*, volume 1109, pages 387–400. Springer Berlin Heidelberg, 1996.

[11] C. Blundo, A. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung. Perfectly-secure key distribution for dynamic conferences. In E. Brickell, editor, *Advances in Cryptology – CRYPTO' 92*, volume 740, pages 471–486. Springer Berlin Heidelberg, 1993.

[12] A. Boldyreva, V. Goyal, and V. Kumar. Identity-based encryption with efficient revocation. In *Proceedings of the 15th ACM conference on Computer and communications security*, CCS '08, pages 417–426, New York, NY, USA, 2008. ACM.

[13] D. Boneh, C. Gentry, and B. Waters. Collusion resistant broadcast encryption with short ciphertexts and private keys. In V. Shoup, editor, *Advances in Cryptology – CRYPTO 2005*, volume 3621, pages 258–275. Springer Berlin Heidelberg, 2005.

[14] R. Canetti, R. Gennaro, and A. Herzberg. Proactive security: Long-term protection against break-ins. *CryptoBytes*, 3:1–8, 1997.

[15] H. Chen, S. Ling, C. Padró, H. Wang, and C. Xing. Key predistribution schemes and one-time broadcast encryption schemes from algebraic geometry codes. In M. Parker, editor, *Cryptography and Coding*, volume 5921, pages 263–277. Springer Berlin Heidelberg, 2009.

[16] R. Cramer, Y. Dodis, S. Fehr, C. Padró, and D. Wichs. Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors. In N. Smart, editor, *Advances in Cryptology – EUROCRYPT 2008*, volume 4965 of *Lecture Notes in Computer Science*, pages 471–488. Springer Berlin Heidelberg, 2008.

[17] Y. Dodis and N. Fazio. Public key broadcast encryption for stateless receivers. In J. Feigenbaum, editor, *Digital Rights Management*, volume 2696, pages 61–80. Springer Berlin Heidelberg, 2003.

[18] A. Fiat and M. Naor. Broadcast encryption. In D. Stinson, editor, *Advances in Cryptology – CRYPTO' 93*, volume 773, pages 480–491. Springer Berlin Heidelberg, 1994.

[19] C. Gentry and B. Waters. Adaptive security in broadcast encryption systems (with short ciphertexts). In A. Joux, editor, *Advances in Cryptology – EUROCRYPT 2009*, volume 5479, pages 171–188. Springer Berlin Heidelberg, 2009.

[20] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg. Proofs of ownership in remote storage systems. In *Proceedings of the 18th ACM conference on Computer and communications security*, CCS '11, pages 491–500, New York, NY, USA, 2011. ACM.

[21] A. Herzberg, S. Jarecki, H. Krawczyk, and M. Yung. Proactive secret sharing or: How to cope with perpetual leakage. In D. Coppersmith, editor, *Advances in Cryptology – CRYPTO' 95*, volume 963, pages 339–352. Springer Berlin Heidelberg, 1995.

[22] S. Kamara and K. Lauter. Cryptographic cloud storage. In R. Sion, R. Curtmola, S. Dietrich, A. Kiayias, J. Miret, K. Sako, and F. Sebé, editors, *Financial Cryptography and Data Security*, volume 6054, pages 136–149. Springer Berlin Heidelberg, 2010.

[23] K. Kurosawa, T. Yoshida, Y. Desmedt, and M. Burmester. Some bounds and a construction for secure broadcast encryption. In K. Ohta and D. Pei, editors, *Advances in Cryptology – ASIACRYPT'98*, volume 1514, pages 420–433. Springer Berlin Heidelberg, 1998.

[24] J. Liu, H. Wang, M. Xian, and K. Huang. A secure and efficient scheme for cloud storage against eavesdropper. In S. Qing, J. Zhou, and D. Liu, editors, *Information and Communications Security*, volume 8233 of *Lecture Notes in Computer Science*, pages 75–89. Springer International Publishing, 2013.

[25] Z. Liu, J. Li, X. Chen, J. Yang, and C. Jia. Tmds: Thin-model data sharing scheme supporting keyword search in cloud storage. In W. Susilo and Y. Mu, editors, *Information Security and Privacy*, volume 8544 of *Lecture Notes in Computer Science*, pages 115–130. Springer International Publishing, 2014.

[26] M. Luby and J. Staddon. Combinatorial bounds for broadcast encryption. In K. Nyberg, editor, *Advances in Cryptology – EUROCRYPT'98*, volume 1403, pages 512–526. Springer Berlin Heidelberg, 1998.

[27] T. Matsumoto and H. Imai. On the key predistribution system: A practical solution to the key distribution problem. In C. Pomerance, editor, *Advances in Cryptology – CRYPTO '87*, volume 293, pages 185–193. Springer Berlin Heidelberg, 1988.

[28] D. Naor, M. Naor, and J. Lotspiech. Revocation and tracing schemes for stateless receivers. In J. Kilian, editor, *Advances in Cryptology – CRYPTO 2001*, volume 2139, pages 41–62. Springer Berlin Heidelberg, 2001.

[29] V. Nikov and S. Nikova. On proactive secret sharing schemes. In H. Handschuh and M. Hasan, editors, *Selected Areas in Cryptography*, volume 3357, pages 308–325. Springer Berlin Heidelberg, 2005.

[30] C. Padró, I. Gracia, and S. Martín. Improving the trade-off between storage and communication in broadcast encryption schemes. *Discrete Applied Mathematics*, 143(1-3):213–220, 2004.

[31] C. Padró, I. Gracia, S. Martín, and P. Morillo. Linear broadcast encryption schemes. *Discrete Applied Mathematics*, 128(1):223–238, 2003.

[32] D. Phan, D. Pointcheval, and M. Strefler. Security notions for broadcast encryption. In J. Lopez and G. Tsudik, editors, *Applied Cryptography and Network Security*, volume 6715, pages 377–394. Springer Berlin Heidelberg, 2011.

[33] A. Sahai, H. Seyalioglu, and B. Waters. Dynamic credentials and ciphertext delegation for attribute-based encryption. In R. Safavi-Naini and R. Canetti, editors, *Advances in Cryptology – CRYPTO 2012*, volume 7417, pages 199–217. Springer Berlin Heidelberg, 2012.

[34] A. Sahai and B. Waters. Fuzzy identity-based encryption. In R. Cramer, editor, *Advances in Cryptology – EUROCRYPT 2005*, volume 3494 of *Lecture Notes in Computer Science*, pages 457–473. Springer Berlin Heidelberg, 2005.

[35] H. Shacham and B. Waters. Compact proofs of retrievability. *Journal of Cryptology*, 26(3):442–483, 2013.

[36] J. Stanek, A. Sorniotti, E. Androulaki, and L. Kencl. A secure data deduplication scheme for cloud storage. In N. Christin and R. Safavi-Naini, editors, *Financial Cryptography and Data Security*, Lecture Notes in Computer Science, pages 99–118. Springer Berlin Heidelberg, 2014.

[37] D. Stinson. On some methods for unconditionally secure key distribution and broadcast encryption. *Designs, Codes and Cryptography*, 12(3):215–243, 1997.

[38] D. Stinson and R. Wei. Unconditionally secure proactive secret sharing scheme with combinatorial structures. In H. Heys and C. Adams, editors, *Selected Areas in Cryptography*, volume 1758, pages 200–214. Springer Berlin Heidelberg, 2000.

[39] The Presidential Commission for the Study of Bioethical Issues. Privacy and progress in whole genome sequencing. President's Bioethics Commission Releases Report on Genomics and Privacy, October 2012.

[40] Y. Watanabe and J. Shikata. Constructions of unconditionally secure broadcast encryption from key predistribution systems with trade-offs between communication and storage. In M.-H. Au and A. Miyaji, editors, *Provable Security*, volume 9451 of *Lecture Notes in Computer Science*, pages 489–502. Springer International Publishing, 2015.

[41] K. Yang, X. Jia, and K. Ren. Attribute-based fine-grained access control with efficient revocation in cloud storage systems. In *Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security*, ASIA CCS '13, pages 523–528, New York, NY, USA, 2013. ACM.

A Collusion Resistant RS-BE Scheme

We consider security against collusion of at most ω colluders and a storage manager. Intuitively, if a storage manager can change any privileged set of a ciphertext into any privileged set by using his maintenance key mk, we cannot achieve RS-BE secure against collusion of a set of colluders and the storage manager. Therefore, here we simply set the following transformation rule for mk: For any $\mathcal{S}, \mathcal{S}' \subset \mathcal{U}$, $\mathit{Upd}(mk, c_{\mathcal{S}}, \mathcal{S}, \mathcal{S}')$ outputs an updated ciphertext $c_{\mathcal{S}'}$ if $\mathcal{S}' \subset \mathcal{S}$ holds, otherwise it outputs $\perp$.

We define collusion resistant security as follows.

Definition 6 (Collusion Resistant RS-BE)**.** *Let* Π *be an RS-BE scheme.* Π *is said to be collusion-resistantly* $(\leq n, \leq \omega)$*-one-time secure if the following conditions are satisfied: For any privileged set* $\mathcal{S} \subset \mathcal{U}$*, and any set of colluders* $\mathcal{W} \subset \mathcal{U}$ *such that* $\mathcal{S} \cap \mathcal{W} = \emptyset$ *and* $|\mathcal{W}| \leq \omega$*, it holds that*

$$H(M \mid C_{\mathcal{S}}, DK_{\mathcal{W}}, MK) = H(M).$$

A construction which satisfies Definition 6 is as follows.

1. $(ek, mk, dk_1, \ldots, dk_n) \leftarrow Setup(n)$: Let q be a prime power such that $q > n$, and $\mathbb{F}_q$ be a finite field with q elements. It chooses n polynomials $f^{(h)}(x) := \sum_{i=0}^{\omega} a_i x^i$ $(h = 1, \ldots, n)$ over $\mathbb{F}_q$ uniformly at random, and computes $n-1$ polynomials $g^{(\ell)}(x) := f^{(\ell)}(x) - f^{(\ell-1)}(x)$ $(2 \leq \ell \leq n)$. Then, it outputs $ek := f^{(1)}(x)$, $dk_i := (f^{(1)}(i), \ldots, f^{(n)}(i))$ $(1 \leq i \leq n)$, and $mk := (g^{(2)}(x), \ldots, g^{(n)}(x))$.

2. $c_{\mathcal{S}} \leftarrow Enc(ek, m, \mathcal{S})$: Let $\mathcal{S} = \{U_{i_1}, \ldots, U_{i_k}\}$ $(1 \leq k \leq n)$ be a privileged set. For every U_{i_j}, it computes $c_{i_j}^{(1)} := m + f^{(1)}(i_j)$, and sets a counter $t := 1$. Finally, it outputs $c_{\mathcal{S}} := (t, c_{i_1}^{(t)}, \ldots, c_{i_k}^{(t)})$.

3. m or $\perp \leftarrow Dec(dk_i, c_{\mathcal{S}}, \mathcal{S}, U_i)$: If $U_i \in \mathcal{S}$, it computes $m = c_i^{(t)} - f^{(t)}(i)$ and outputs it. Otherwise, it outputs $\perp$.

4. $c_{\mathcal{S}'}$ or $\perp \leftarrow Upd(mk, c_{\mathcal{S}}, \mathcal{S}, \mathcal{S}')$: Let $\mathcal{S}' = \{U_{i_1}, \ldots, U_{i_k}\}$. If $\mathcal{S}' \subset \mathcal{S}$ does not hold, it outputs $\perp$. Otherwise, for every $U_{i_j} \in \mathcal{S}' \subset \mathcal{S}$, it computes $c_i^{(t+1)} := c_{i_j}^{(t)} + g^{(t+1)}(i_j)$ $(1 \leq j \leq k)$. Finally, it sets $t := t+1$ and outputs $c_{\mathcal{S}'} := (t, c_{i_1}^{(t)}, \ldots, c_{i_k}^{(t)})$.

Theorem 6. *The resulting RS-BE scheme* Π *by the above construction is collusion-resistantly* $(\leq n, \leq \omega)$*-one-time secure.*

Proof. It is not so difficult to prove this theorem. Without loss of generality, we consider that $\mathcal{W} := \{U_1, \ldots, U_\omega\}$ is a set of colluders and $\mathcal{S} := \{U_{\omega+1} \ldots, U_n\}$ is a privileged set. Consider the case that the set of colluders $\mathcal{W}$ and the storage manager will guess $k_{\mathcal{S}}$ to obtain the plaintext m by the using their secret keys. Since each degree of x of $f^{(h)}(x)$ $(1 \leq h \leq n)$ is at most ω, at most ω colluders cannot obtain $f^{(h)}(x)$ from $f^{(h)}(1), \ldots, f^{(h)}(\omega)$ $(1 \leq h \leq n)$. Hence, they cannot obtain any information on $f^{(h)}(x)$ $(1 \leq h \leq n)$ even if they have $g^{(\ell)}(x)$ $(2 \leq \ell \leq n)$. Hence, for any $\mathcal{S} \subset \mathcal{U}$, and any $\mathcal{W} \subset \mathcal{U}$ such that $\mathcal{S} \cap \mathcal{W} = \emptyset$ and $|\mathcal{W}| \leq \omega$, $H(M \mid C_{\mathcal{S}}, DK_{\mathcal{W}}, MK) = H(M)$. □

B $(t, \leq \omega)$-one-time secure RS-BE

As in traditional BE schemes [26, 30, 23, 15], we can also consider another class of RS-BE schemes, which is called $(t, \leq \omega)$-one-time secure RS-BE schemes, where $t + \omega \leq n$. A model and security of such a scheme are almost the same as that described in Section 2, and the only difference from those in Section 2 is that a sender can specify only a privileged set whose cardinality is exactly t (i.e., $|\mathcal{S}| = t$).

Then, we can derive lower bounds on secret keys in a similar way to Section 3, and these bounds can also be applied to traditional $(t, \leq \omega)$-one-time secure BE schemes [26, 30, 23, 15].

Theorem 7. *Let* Π *be a* $(t, \leq \omega)$*-one-time secure RS-BE scheme. Then, for any* $\mathcal{S} \subset \mathcal{U}$*, the following lower bounds hold under the condition* $H(C_{\mathcal{S}}) = H(M)$*:*

$$\text{(i) } H(EK) \geq \binom{t+\omega}{t} H(M), \quad \text{(ii) } H(DK_i) \geq \binom{t+\omega-1}{t-1} H(M) \text{ for any } i \in \{1, 2, \ldots, n\},$$

(iii) $H(MK) \geq \left(\binom{t+\omega}{t} - 1\right) H(M)$.

Proof. The proof follows from the following lemmas.

Lemma 5. *We have $H(EK) \geq \binom{t+\omega}{t} H(M)$ under the condition $H(C_{\mathcal{S}}) = H(M)$ for any $\mathcal{S} \subset \mathcal{U}$.*

Proof. Without loss of generality, let $\mathcal{I} := \{U_1, \ldots, U_{t+\omega}\}$. Let $\mathscr{W} := \{\mathcal{W} \subset \mathcal{I} \mid |\mathcal{W}| = \omega\} = \{\mathcal{W}_1, \ldots, \mathcal{W}_\ell\}$ be the family of all possible set of colluders, where $\ell = \binom{t+\omega}{\omega} = \binom{t+\omega}{t}$. Moreover, let $\mathscr{S}(\mathscr{W}) := \{\mathcal{S}_1, \ldots, \mathcal{S}_\ell\}$, where $\mathcal{S}_i = \mathcal{I} \setminus \mathcal{W}_i$ such that $\mathcal{W}_i \in \mathscr{W}$ $(1 \leq i \leq \ell)$. Then, we have

$$\begin{aligned}
H(EK) =& H(EK \mid M) \qquad (25)\\
\geq& I(EK; C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_\ell} \mid M)\\
=& H(C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_\ell} \mid M) - H(C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_\ell} \mid M, EK)\\
=& H(C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_\ell} \mid M) \qquad (26)\\
=& \sum_{j=1}^{\ell} H(C_{\mathcal{S}_j} \mid M, C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_{j-1}})\\
\geq& \sum_{j=1}^{\ell} H(C_{\mathcal{S}_j} \mid M, C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_{j-1}}, DK_{\mathcal{W}_j})\\
\geq& \binom{t+\omega}{t} H(M), \qquad (27)
\end{aligned}$$

where (25) follows from independence of M and EK, (26) follows from the algorithm *Enc* (i.e. $H(C_{\mathcal{S}_i} \mid EK, M) = 0$ $(1 \leq i \leq \ell)$), and (27) follows from Lemma 1. □

Lemma 6. *For any $i \in \{1, \ldots, n\}$, then we have $H(DK_i) \geq \sum_{j=0}^{\omega} \binom{n-1}{j} H(M)$ under the condition $H(C_{\mathcal{S}}) = H(M)$ for any $\mathcal{S} \subset \mathcal{U}$.*

Proof. Without loss of generality, let $\mathcal{I} := \{U_1, \ldots, U_i, \ldots, U_{t+\omega}\}$. Let $\mathscr{W}^{(i)} := \{\mathcal{W} \subset \mathcal{I} \setminus \{U_i\} \mid |\mathcal{W}| = \omega\} = \{\mathcal{W}_1, \ldots, \mathcal{W}_\ell\}$ be the family of all possible set of colluders except for sets of colluders containing U_i, where $\ell = \binom{t+\omega-1}{\omega} = \binom{t+\omega-1}{t-1}$. Let $\mathscr{S}(\mathscr{W}^{(i)}) := \{\mathcal{S}_1, \ldots, \mathcal{S}_\ell\}$, where $\mathcal{S}_i = \mathcal{I} \setminus \mathcal{W}_i$ such that $\mathcal{W}_i \in \mathscr{W}^{(i)}$ $(1 \leq i \leq \ell)$ We note $U_i \in \mathcal{S}$ for any $\mathcal{S} \in \mathscr{S}(\mathscr{W}^{(i)})$. Then, we have

$$\begin{aligned}
H(DK_i) =& H(DK_i \mid M) \qquad (28)\\
\geq& I(DK_i; C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_\ell} \mid M)\\
=& H(C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_\ell} \mid M) - H(C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_\ell} \mid M, DK_i)\\
=& H(C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_\ell} \mid M) \qquad (29)\\
=& \sum_{j=1}^{\ell} H(C_{\mathcal{S}_j} \mid M, C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_{j-1}})\\
\geq& \sum_{j=1}^{\ell} H(C_{\mathcal{S}_j} \mid M, C_{\mathcal{S}_1}, \ldots, C_{\mathcal{S}_{j-1}}, DK_{\mathcal{W}_j})\\
\geq& \binom{t+\omega-1}{t-1} H(M), \qquad (30)
\end{aligned}$$

where (28) follows from independence of M and DK_i, (29) follows from (3) in Lemma 1 (i.e. $H(C_{\mathcal{S}_j} \mid DK_i, M) = 0$ $(1 \leq j \leq \ell)$), and (30) follows from Lemma 1. □

Lemma 7. *We have* $H(MK) \geq \left(\binom{t+\omega}{t} - 1\right) H(M)$ *under the condition* $H(C_{\mathcal{S}}) = H(M)$ *for any* $\mathcal{S} \subset \mathcal{U}$*.*

Proof. Let $\mathcal{I}$, $\mathscr{W}$ and $\mathscr{S}(\mathscr{W})$ be the same as those in Lemma 5. Then, we have

$$
\begin{aligned}
H(MK) \geq & H(MK \mid C_{\mathcal{S}_1}) \\
\geq & I(MK; C_{\mathcal{S}_2}, \dots, C_{\mathcal{S}_\ell} \mid C_{\mathcal{S}_1}) \\
= & H(C_{\mathcal{S}_2}, \dots, C_{\mathcal{S}_\ell} \mid C_{\mathcal{S}_1}) - H(C_{\mathcal{S}_2}, \dots, C_{\mathcal{S}_\ell} \mid C_{\mathcal{S}_1}, MK) \\
= & H(C_{\mathcal{S}_2}, \dots, C_{\mathcal{S}_\ell} \mid C_{\mathcal{S}_1}) \qquad (31) \\
= & \sum_{j=2}^{\ell} H(C_{\mathcal{S}_j} \mid C_{\mathcal{S}_1}, \dots, C_{\mathcal{S}_{j-1}}) \\
\geq & \sum_{j=2}^{\ell} H(C_{\mathcal{S}_j} \mid M, C_{\mathcal{S}_1}, \dots, C_{\mathcal{S}_{j-1}}, DK_{\mathcal{W}_j}) \\
\geq & \left(\binom{t+\omega}{t} - 1\right) H(M), \qquad (32)
\end{aligned}
$$

where (31) follows from the algorithm *Upd* (i.e. $H(C_{\mathcal{S}_i} \mid C_{\mathcal{S}_1}, MK) = 0$ $(2 \leq i \leq \ell)$), and (32) follows from Lemma 1. □

Now, the proof of Theorem 7 is completed. □

We can construct a $(t, \leq \omega)$-one-time secure RS-BE scheme based on the idea of our construction described in Section 4 and an ω-secure non-interactive t-conference KPS [11] as follows. We here consider a construction when the ciphertext size is equal to the plaintext size (i.e., $\delta = 1$). We omit the security proof since it is easy to prove in a way similar to the proof of [11, Theorem 5.1]. Also, We can consider a robust scheme in the same manner as the proposed robust scheme in Section 5.

1. $(ek, mk, dk_1, \dots, dk_n) \leftarrow$ *Setup*(n): Let $\mathbb{F}_q$ be a finite field with q $(> n)$ elements, where q is a prime power. It chooses a symmetric polynomial $f(x_1, \dots, x_t) := \sum_{i_1=0}^{\omega} \cdots \sum_{i_t=0}^{\omega} a_{i_1 i_2 \cdots i_t} x_1^{i_1} \cdots x_t^{i_t}$ over $\mathbb{F}_q$, where $a_{i_1 i_2 \cdots i_t} = a_{\sigma(i_1)\sigma(i_2)\cdots\sigma(i_t)}$ for all permutations $\sigma = (\sigma(i_1), \sigma(i_2), \dots, \sigma(i_t))$. Also, it computes $g(x_1, x_2, \dots, x_t) := f(x_1, x_2, \dots, x_t) - a_{00\cdots 0}$. Then, it outputs $ek := f(x_1, x_2, \dots, x_t)$, $dk_i := f(i, x_2, \dots, x_t)$ $(1 \leq i \leq n)$, and $mk := g(x_1, x_2, \dots, x_t)$.

2. $c_{\mathcal{S}} \leftarrow$ *Enc*$(ek, m, \mathcal{S})$: For any privileged set $\mathcal{S} := \{U_{i_1}, \dots, U_{i_t}\}$, it computes a session key $k_{\mathcal{S}} := f(i_1, \dots, i_t)$, and then outputs $c_{\mathcal{S}} := m + k_{\mathcal{S}}$.

3. m or $\perp \leftarrow$ *Dec*$(dk_i, c_{\mathcal{S}}, \mathcal{S}, U_i)$: If $U_i \in \mathcal{S}$, then it computes $k_{\mathcal{S}}$ as in the algorithm *Enc* and outputs $m = c_{\mathcal{S}} - k_{\mathcal{S}}$. Otherwise, it outputs $\perp$.

4. $c_{\mathcal{S}'}$ or $\perp \leftarrow$ *Upd*$(mk, c_{\mathcal{S}}, \mathcal{S}, \mathcal{S}')$: For any pair of privileged sets $\mathcal{S} := \{U_{i_1}, \dots, U_{i_t}\}$ and $\mathcal{S}' := \{U_{j_1}, \dots, U_{j_t}\}$, it computes and outputs $c_{\mathcal{S}'} := c_{\mathcal{S}} + g(j_1, \dots, j_t) - g(i_1, \dots, i_t)$.

Theorem 8. *The resulting RS-BE scheme* Π *by the above construction is* $(t, \leq \omega)$*-one-time secure and meets equality in every bound of (i)–(iii) in Theorem 7.*