Information-Theoretically Secure Key-Insulated Multireceiver Authentication Codes

Takenobu Seito, Tadashi Aikawa, Junji Shikata, and Tsutomu Matsumoto

Graduate School of Environment and Information Sciences,
Yokohama National University, Japan
seito@mlab.jks.ynu.ac.jp, {shikata,tsutomu}@ynu.ac.jp

Abstract. Exposing a secret-key is one of the most disastrous threats in cryptographic protocols. The key-insulated security is proposed with the aim of realizing the protection against such key-exposure problems. In this paper, we study key-insulated authentication schemes with information-theoretic security. More specifically, we focus on one of information-theoretically secure authentication, called multireceiver authentication codes, and we newly define a model and security notions of information-theoretically secure key-insulated multireceiver authentication codes (KI-MRA for short) based on the ideas of both computationally secure key-insulated signature schemes and multi-receiver authentication-codes with information-theoretic setting. In addition, we show lower bounds of sizes of entities' secret-keys. We also provide two kinds of constructions of KI-MRA: direct and generic constructions which are provably secure in our security definitions. It is shown that the direct construction meets the lower bounds of key-sizes with equality. Therefore, it turns out that our lower bounds are tight, and that the direct construction is optimal.

Keywords: information-theoretic security, key-insulated security, multireceiver authentication-code, unconditional security.

1 Introduction

1.1 Background

The security of most of present cryptographic techniques is based on the assumption of difficulty of computationally hard problems such as the integer factoring or discrete logarithm problems. However, taking into account recent rapid development of algorithms and computer technologies, such a scheme based on the assumption of difficulty of computationally hard problems might not maintain sufficient long-term security. In fact, it is known that quantum computers can solve the factoring and discrete logarithm problems in polynomial time [19]. From these aspects, it is necessary and interesting to consider cryptographic techniques whose security does not depend on any computationally hard problems.

One of the most serious threats in cryptographic protocols is exposure of secret-keys. For example, digital signature schemes require use of the secret-keys

D.J. Bernstein and T. Lange (Eds.): AFRICACRYPT 2010, LNCS 6055, pp. 148–165, 2010.

to sign a message, and if a secret-key is compromised, this implies an attacker gaining ability to generate a signature of all messages. Hence, it leads to a total break of the systems. However, we would want to minimize the risk of damage even if such an unfortunate situation as exposure of secret-keys does occur. For this purpose, there have been several approaches proposed to minimize the risk of key-exposure: *Key-splitting* is a method which divides portions of a single secret-key among multiple entities so that no entity will have the ability to reconstruct a whole secret-key [3][5][20]; Another approach is to consider key-evolution to realize *forward-secure schemes* [1][2][4] where lifetime of systems is divided into discrete periods and a secret-key is updated at each new period. It ensures that the security of past periods remains uncompromised even if the current secret-key is exposed. The security notion that is one solution to the key-exposure problems is proposed by Dodis et al., and it is called *Key-Insulated Security* [7][8], which is based on the ideas of combining key-splitting and key-evolution. This method extracts benefits from both approaches: having the information manageable in case of loss of key and leaving authentication as a stand-alone user operation at the same time.

In the model of key-insulated signature schemes, a signer has two kinds of devises: a trusted device (e.g. a smart card, USB flash memory) in which a master-key is stored; and an insecure device in which a signer's secret-key is stored. The actual secret-key updating is performed in the insecure device. When the signer wants to get a signing-key at a period j, the following process is performed in the beginning of the period j: first, the trusted device generates key-updating information by using the master-key and sends it to the signer; and then, the signer updates his secret-key by using the key-updating information, and he deletes the previous secret-key. In key-insulated signature schemes, if the trusted device is not compromised, then signer's secret-keys of at most γ periods can be exposed without losing security, where γ is a predefined number. In addition, even if the trusted device is exposed, the system will not be violated if no signer's secret-key is exposed. This property is called *strong key-insulation* [7][8]. Hence the system having strong key-insulation guarantees the security against two different types of attacks: (i) the attack to steal a secret-key stored in an insecure device via a network; and (ii) the attack to steal a master-key stored in a (physically-protected) secure device directly. We consider that the property of strong key-insulation is important and useful when using a system in the real world.

As mentioned earlier, the first constructions of key-insulated schemes are proposed in [7][8]. Since then, many papers on this subject have been reported to give theoretical and practical key-insulated schemes. Also, Itkis et al. proposed an extended version of key-insulated signature schemes, *Intrusion-resilient signatures* [13]. The security of most of key-insulated schemes described so far is based on the assumption of difficulty of computationally hard problem such as the integer factoring or discrete logarithm problems. In this paper, we study key-insulated schemes in the setting of the *information-theoretic security* (a.k.a. *unconditional security*) rather than the computational security.

1.2 Our Contribution

Confidentiality (secrecy) and authenticity (integrity) are currently fundamental cryptographic functions, and encryption and authentication/signature schemes are usually used for providing confidentiality and authenticity, respectively. As key-insulated schemes with information-theoretic security, Hanaoka et al. first proposed the information-theoretically secure key-insulated encryption schemes [11]. However, information-theoretically secure authentication/signature schemes with key-insulated security have not proposed so far. Therefore, we study authentication schemes which have both information-theoretic and key-insulated security, and the purpose of this paper is to consider a simple model of information-theoretically secure key-insulated authentication schemes.

We note that information-theoretically secure signature schemes were proposed by Shikata et al. in [12] [18]. Thus, one may consider the information-theoretically secure key-insulated signature schemes. However, the model of those schemes in [12] [18] is not so simple, since it requires complicated security notions. On the other hand, we note that the model of *multireceiver authentication codes* (*MRA-codes* for short) was proposed by Desmedt et al. in [6] and later generalized by Safavi-Naini et al. [17] and Johansson [14]. The MRA-code is one of the information-theoretically secure authentication schemes which allows a single honest sender to transmit an authenticated message to a group of receivers via a broadcast channel. And each receiver can individually verify the authenticated message. Note that the model of MRA-codes is simpler than that of information-theoretically secure signature schemes.

In this paper, we study the model of *key-insulated MRA-codes* (*KI-MRA* for short), which are information-theoretically secure authentication schemes with key-insulated security, rather than information-theoretically secure key-insulated signature schemes, since the model of MRA-codes is simpler than that of information-theoretically secure signature schemes. More specifically, we newly introduce the model and security definitions, and show lower bounds and constructions of KI-MRA. We begin by formalizing the model and security notions of KI-MRA based on those of MRA-codes and computationally secure key-insulated signature schemes. In particular, the notion of strong key-insulation is formalized along with our model. In addition, we show lower bounds of sizes of entities' secret-keys. We also provide two kinds of constructions of KI-MRA, direct and generic constructions which are provably secure in our security definitions: we propose the direct construction by using polynomials over finite fields; and we provide the generic construction of KI-MRA starting from cover-free-families(CFF) [9] and MRA-codes. Furthermore, it is shown that the direct construction meets the lower bounds of key-sizes with equality. Therefore, it turns out that our lower bounds are tight, and that the direct construction is optimal.

The rest of this paper is organized as follows. In Section 2, we introduce the model of KI-MRA based on the ideas according to [7], [8], [17], and formalize the security notions of KI-MRA. We also show lower bounds of memory-sizes of

secret-keys of entities. In Section 3, we propose two kinds of constructions: direct and generic constructions which are provably secure in our security notions. Finally, in Section 4, we give concluding remarks of the paper.

2 The Model and Security Definitions

In this section, we introduce the model and security notions of KI-MRA, based on those of key-insulated signatures with computational security and those of MRA-codes with information-theoretic security.

2.1 The Model

We show the model of KI-MRA, which is the model of MRA-codes with key-insulated security. As in the models of many schemes with information-theoretic security (e.g. [16] [17] [18]), we assume that there is a trusted authority whose role is to generate and to distribute secret-keys of entities. We call this model the *trusted initializer model* as in [16]. In KI-MRA, there are $n+3$ entities, a sender S, a secure device H, n receivers R_1, R_2, ..., R_n and a trusted initializer TI. We assume that the sender is honest in the model. In our model, the notion of a *secure device* implies that it is usually isolated from a network (e.g. the Internet or LAN) and that the attacker can neither wiretap nor substitute information stored in the device via the network. For example, a smart card or USB flash memory seems to be a candidate of such devices. In addition, in KI-MRA, we assume that lifetime of the system is divided into N periods. For simplicity, we consider a *one-time model* of KI-MRA, in which the sender is allowed to generate and broadcast an authenticated message at most only once per period[1].

Informally, KI-MRA is executed as follows. In the initial phase, TI generates secret-keys on behalf of S, H and R_i ($1 \leq I \leq n$). After distributing these secret-keys via a secure channel, TI deletes them in his memory. For updating the sender's secret-key for the period j, S receives key-updating information from H by connecting with H, and S computes a secret-key at the period j by using the secret-key of the previous period and the key-updating information. S then deletes the secret-key of the previous period and the key-updating information. On the other hand, each receiver's secret-key used to check the validity of an authenticated messages will not be updated at each period as key-insulated signature schemes with computational security. If S generates and broadcasts an authenticated message α at a period j, each receiver, R_i, can check the validity of α by using his secret-key. Formally, we give the definition as follows.

Definition 1 (KI-MRA). A *key-insulated multireceiver authentication codes* (*KI-MRA* for short) Π involves $n+3$ entities, TI, S, H and R_1, R_2, ..., R_n,

[1] We can consider a more general setting: the number up to which the sender is allowed to generate authenticated messages is more than one per period. However, the one-time model of KI-MRA is simpler than this model in terms of the number of generating authenticated messages. Therefore, we focus on the model since our purpose is to study a simple model as mentioned in Section 1.2.

and consists of a five-tuple of algorithms (*KGen*, *KUpd**, *KUpd*, *KAuth*, *KVer*) with eight spaces, $\mathcal{M}$, $\mathcal{A}$, $\mathcal{I}$, $\mathcal{T}$, $\tilde{\mathcal{T}}$, $\mathcal{MK}$, $\mathcal{E}_S$ and $\mathcal{E}_R$, where all of the above algorithms except *KGen* are deterministic and all of the above spaces are finite. In addition, Π is executed with four phases as follows.

– **Notation:**
  - TI is a trusted initializer, S is a sender, H is a secure device and R_i $(i = 1, 2, \ldots, n)$ is a receiver. Let $R := \{R_1, R_2, \ldots, R_n\}$ be a set of receivers.
  - $\mathcal{M}$ is a set of possible messages with a probability distribution $\Pr_M$.
  - $\mathcal{A}$ is a set of possible authenticated messages.
  - $\mathcal{I}$ is a set of possible key-updating information.
  - $\mathcal{T} := \{1, 2, \ldots, N\}$ is a set of time periods. Let $\tilde{\mathcal{T}} := \mathcal{T} \cup \{0\}$.
  - $\mathcal{MK}$ is a set of possible master-keys for the device H with a probability distribution $\Pr_{MK}$.
  - $\mathcal{E}_S^{(j)}$ is a set of possible secret-keys at the period j for the sender with a probability distribution $\Pr_{E_S^{(j)}}$. Let $\mathcal{E}_S := \mathcal{E}_S^{(0)} \cup \mathcal{E}_S^{(1)} \cup \ldots \cup \mathcal{E}_S^{(N)}$.
  - $\mathcal{E}_i$ is a set of secret-keys for a receiver R_i with a probability distribution $\Pr_{E_i}$. Let $\mathcal{E}_R := \mathcal{E}_1 \cup \mathcal{E}_2 \cup \ldots \cup \mathcal{E}_n$.
  - *KGen* is a key generation algorithm which on input a security parameter 1^k, outputs a master-key, a sender's secret-key and each receiver's secret-key.
  - *KUpd**: $\mathcal{MK} \times \tilde{\mathcal{T}} \times \mathcal{T} \to \mathcal{I}$ is a key-updating algorithm for the device H.
  - *KUpd*: $\mathcal{E}_S \times \mathcal{I} \to \mathcal{E}_S$ is a key-updating algorithm for the sender S.
  - *KAuth*: $\mathcal{E}_S \times \mathcal{M} \to \mathcal{A}$ is an authentication algorithm for producing authenticated messages.
  - *KVer*: $\mathcal{E}_R \times \mathcal{A} \times \mathcal{T} \to \{true, false\}$ is a verification algorithm.

1. **Key Generation and Distribution by TI.** In the initial phase, TI generates the following keys by using *KGen*: a master-key $mk \in \mathcal{MK}$; an initial secret-key $e_S^{(0)} \in \mathcal{E}_S^{(0)}$ (i.e., a secret-key at the period 0) for the sender; and the receiver R_i's secret-key $e_i \in \mathcal{E}_i$ $(i = 1, 2, \ldots, n)$. These keys are distributed to corresponding entities via secure channels. After distributing these keys, TI deletes these keys from his memory. And, H, S, and R_i keep their keys secret, respectively.
2. **Updating Sender's Secret-keys.** For updating a sender's secret-key for a period j from a period h, H generates key-updating information $mk^{(h,j)} = KUpd^*(mk, h, j) \in \mathcal{I}$ by using the master-key mk, the information on periods $h \in \tilde{\mathcal{T}}, j \in \mathcal{T}$ and *KUpd**, and then sends it to S via a secure channel. After that, S computes a secret-key $e_S^{(j)} = KUpd(e_S^{(h)}, mk^{(h,j)}) \in \mathcal{E}_S^{(j)}$ at the period j. Then, S deletes $e_S^{(h)}$ and $mk^{(h,j)}$ from his memory.
3. **Authentication.** During a period j, for a message $m \in \mathcal{M}$, S generates an authenticated message $\alpha = KAuth(e_S^{(j)}, m) \in \mathcal{A}$ by using a secret-key $e_S^{(j)}$ at the period j. Then, S sends the authenticated message with information on j, namely (α, j), to all receivers via a broadcast channel.

4. **Verification.** After receiving (α, j) from S, each receiver R_i can verify the validity of it by using secret-key e_i and $KVer$. If $KVer(e_i, \alpha, j) = \text{true}$, then R_i accepts (α, j) as valid, and rejects it otherwise.

In the model of KI-MRA, we require the following equation holds: for all possible $j \in \mathcal{T}$, $m \in \mathcal{M}$, $e_S^{(j)} \in \mathcal{E}_S^{(j)}$, and $e_i \in \mathcal{E}_i$, we have

$$KVer(e_i, KAuth(e_S^{(j)}, m), j) = true$$

The above requirement implies that any legal authenticated message can be accepted without error if entities correctly follows the specification of KI-MRA.

In addition, we define several notation as follows. Let ω be the number of possible colluders, and let γ be the number of possible periods at which sender's secret-keys may be exposed. And, for any set $\mathcal{Z}$ and any nonnegative integer z, let $\mathcal{P}(\mathcal{Z}, z) := \{Z \subset \mathcal{Z} || Z| \leq z\}$ be the family of all subsets of $\mathcal{Z}$ whose cardinality is less than or equal to z. And also, let $W := \{R_{i_1}, R_{i_2}, \ldots, R_{i_\omega}\} \in \mathcal{P}(R, \omega)$ be a set of possible colluders and $\mathcal{E}_W := \mathcal{E}_{i_1} \times \mathcal{E}_{i_2} \ldots \times \mathcal{E}_{i_\omega}$ be a set of possible secret-keys held by W. Furthermore, let $\Gamma := \{j_1, j_2, \ldots, j_\gamma\} \subset \mathcal{P}(\mathcal{T}, \gamma)$ be a set of periods at which sender's secret-keys are exposed, and $\mathcal{E}_\Gamma := \mathcal{E}_S^{(j_1)} \times \mathcal{E}_S^{(j_2)} \times \ldots \times \mathcal{E}_S^{(j_\gamma)}$ be a set of sender's secret-keys exposed. With these notation, we will discuss KI-MRA in the following sections.

2.2 Security Notions and Their Formalization

We now provide security notions and their formalization of KI-MRA in the one-time model based on key-insulated signature schemes with computational security [7] [8] and MRA-codes[17]. In MRA-codes, there are two kinds of attacks: *impersonation attack* and *substitution attacks* (see Appendix A for the detail of those attacks). Therefore, we consider similar attacks in KI-MRA. In the model of KI-MRA, we assume that the adversary can corrupt at most ω dishonest receivers among R, and we do not think about any attack by the sender, since he is assumed to be honest in the model as in that of MRA-codes. In addition, we need to consider the following two types of exposure as in [7] [8]:

- Type A: *Sender's secret-key exposure*, which models compromise of sender's secret-keys from the insecure device.
- Type B: *Master-key exposure*, which models compromise (robbery) of the secure device by physical means.

Therefore, by combining two kinds of attacks (i.e., impersonation and substitution attacks) in MRA-codes and two types of key-exposure (i.e., Types A and B) above, we consider four kinds of security notions of KI-MRA as follows.

Definition 2 (Security of KI-MRA). Let Π be a KI-MRA. The scheme Π is said to be an $(n, \omega; N, \gamma; \epsilon_A, \epsilon_B)$-*one-time secure* if $P_{\Pi,A} \leq \epsilon_A$ and $P_{\Pi,B} \leq \epsilon_B$, where $P_{\Pi,A}$ and $P_{\Pi,B}$ are defined as follows.

A-1) **Impersonation attack in the exposure type A.** The adversary who corrupts at most ω receivers tries to generate a fraudulent authenticated message at a period t, (α, t), that has not been legally generated by the sender S but will be accepted by a receiver R_i. Here, we assume that R_i is not included in the colluders, and the adversary can gather information by pooling secret-keys of corrupted receivers, at most γ sender's secret-keys exposed (but, the adversary cannot obtain the secret-key at the target period t). The success probability of this attack denoted by P_{Π,I_A} is defined as follows: For any set of colluders $W \in \mathcal{P}(R, \omega)$, any set of key-exposure periods $\Gamma \in \mathcal{P}(\mathcal{T}, \gamma)$, any targeted honest receiver $R_i \notin W$ and target period $t \notin \Gamma$, we define $P_{\Pi,I_A}(R_i, W, \Gamma, t)$ as

$$P_{\Pi,I_A}(R_i, W, \Gamma, t) := \max_{e_W} \max_{e_\Gamma} \max_{(\alpha,t)} \Pr(KVer(e_i, \alpha, t) = true | e_W, e_\Gamma),$$

where the probability is taken over random choice of KGen, and the maximum is taken over: all possible sets of the colluders' secret-keys $e_W \in \mathcal{E}_W$; all possible sets of sender's secret-keys $e_\Gamma \in \mathcal{E}_\Gamma$ exposed such that $e_S^{(t)} \notin e_\Gamma$; and all possible authenticated messages $(\alpha, t) \in \mathcal{A} \times \mathcal{T}$. Then, the probability P_{Π,I_A} is defined as $P_{\Pi,I_A} := \max_{R_i,W,\Gamma,t} P_{\Pi,I_A}(R_i, W, \Gamma, t)$.

A-2) **Substitution attack in the exposure type A.** The adversary who corrupts at most ω receivers tries to generate a fraudulent authenticated message at a period t, (α, t), that has not been legally generated by the sender S but will be accepted by a receiver R_i, after observing a valid authenticated message at the same period, (α', t). Here, we assume that R_i is not included in the colluders, and the adversary can gather information by pooling secret-keys of corrupted receivers, at most γ sender's secret-keys exposed (but, the adversary cannot obtain the secret-key at the target period t). The success probability of this attack denoted by P_{Π,S_A} is defined as follows: For any set of colluders $W \in \mathcal{P}(R, \omega)$, any set of key-exposure periods $\Gamma \in \mathcal{P}(\mathcal{T}, \gamma)$, any targeted honest receiver $R_i \notin W$ and target period $t \notin \Gamma$, we define $P_{\Pi,S_A}(R_i, W, \Gamma, t)$ as

$$P_{\Pi,S_A}(R_i, W, \Gamma, t) := \max_{e_W} \max_{e_\Gamma} \max_{(\alpha',t)} \max_{(\alpha,t)\neq(\alpha',t)} \Pr(KVer(e_i, \alpha, t) = true | e_W, e_\Gamma, (\alpha', t)),$$

where the probability is taken over random choice of KGen, and the maximum is taken over: all possible sets of the colluders' secret-keys $e_W \in \mathcal{E}_W$; all possible sets of sender's secret-keys exposed $e_\Gamma \in \mathcal{E}_\Gamma$ such that $e_S^{(t)} \notin e_\Gamma$; and all possible authenticated messages $(\alpha', t), (\alpha, t) \in \mathcal{A} \times \mathcal{T}$ such that $\alpha \neq \alpha'$. Then, the probability P_{Π,S_A} is defined as $P_{\Pi,S_A} := \max_{R_i,W,\Gamma,t} P_{\Pi,S_A}(R_i, W, \Gamma, t)$. And, we define $P_{\Pi,A} := \max(P_{\Pi,I_A}, P_{\Pi,S_A})$.

B-1) **Impersonation attack in the exposure type B.** The adversary who corrupts at most ω receivers tries to generate a fraudulent authenticated message (α, t) that has not been legally generated by the sender S but

will be accepted by a receiver R_i. Here, we assume that R_i is not included in the colluders, and the adversary can gather information by pooling secret-keys of corrupted receivers and a master-key exposed. The success probability of this attack denoted by P_{Π,I_B} is defined as follows: For any set of colluders $W \in \mathcal{P}(R,\omega)$, any targeted honest receiver $R_i \notin W$ and target period t, we define $P_{\Pi,I_B}(R_i,W,t)$ as

$$P_{\Pi,I_B}(R_i,W,t) := \max_{e_W} \max_{mk} \max_{(\alpha,t)} \Pr(KVer(e_i,\alpha,t) = true | e_W, mk),$$

where the probability is taken over random choice of KGen, and the maximum is taken over: all possible sets of the colluders' secret-keys $e_W \in \mathcal{E}_W$; all possible master-keys exposed $mk \in \mathcal{MK}$; and all possible authenticated messages $(\alpha,t) \in \mathcal{A} \times \mathcal{T}$. Then, the probability P_{Π,I_B} is defined as $P_{\Pi,I_B} := \max_{R_i,W,t} P_{\Pi,I_B}(R_i,W,t)$.

B-2) **Substitution attack in the exposure type B.** The adversary who corrupts at most ω receivers tries to generate a fraudulent authenticated message at a period t, (α,t), that has not been legally generated by the sender S but will be accepted by a receiver R_i, after observing a valid authenticated message at the same period, (α',t). Here, we assume that R_i is not included in the colluders, and the adversary can gather information by pooling secret-keys of corrupted receivers and a master-key exposed. The success probability of this attack denoted by P_{Π,S_B} is defined as follows: For any set of colluders $W \in \mathcal{P}(R,\omega)$, any targeted honest receiver $R_i \notin W$ and target period t, we define $P_{\Pi,S_B}(R_i,W,t)$ as

$$P_{\Pi,S_B}(R_i,W,t) := \max_{e_W} \max_{mk} \max_{(\alpha',t)} \max_{(\alpha,t)\neq(\alpha',t)} \Pr(KVer(e_i,\alpha,t) = true | e_W, mk, (\alpha',t)),$$

where the probability is taken over random choice of KGen, and the maximum is taken over: all possible sets of the colluders' secret-keys $e_W \in \mathcal{E}_W$; all possible master-keys exposed $mk \in \mathcal{MK}$; and all possible authenticated messages $(\alpha',t),(\alpha,t) \in \mathcal{A} \times \mathcal{T}$ such that $\alpha \neq \alpha'$. Then, the probability P_{Π,S_B} is defined as $P_{\Pi,S_B} := \max_{R_i,W,t} P_{\Pi,S_B}(R_i,W,t)$. And, we define $P_{\Pi,B} := \max(P_{\Pi,I_B}, P_{\Pi,S_B})$.

Instead of Definition 2, one can consider a more general attacking model as follows: in addition to information in Definition 2, the adversary may observe authenticated messages in all periods which are generated by the honest sender, since he can broadcast at most one authenticated message per period. However, this model is not so simple. Furthermore, even if we consider the general attacking model, we will obtain the very similar results (i.e., lower bounds and constructions) shown in Sections 2.3 and 3. Therefore, we consider the attacking model in Definition 2, since the purpose of this paper is to consider a simple and essential model of multireceiver authentication systems with key-insulated security.

2.3 Lower Bounds

In this section, we derive lower bounds of success probabilities of attacks and memory-sizes required for an $(n, \omega; N, \gamma; \epsilon_A, \epsilon_B)$-one-time secure KI-MRA. Let $\mathcal{A}^{(t)} := \{\alpha \in \mathcal{A} | KAuth(e_S^{(t)}, m) = \alpha \text{ for some } e_S^{(t)} \in \mathcal{E}_S^{(t)}, m \in \mathcal{M}\}$ be a set of possible authenticated messages which can be generated at a period t by the sender. Also, let $\mathcal{I}^{(h,j)} \subset \mathcal{I}$ be a finite set of possible key-updating information which is used for key-updating process from a period h to a period j. And, let $I^{(h,j)}$, E_W and E_Γ be random variables which take values on $\mathcal{I}^{(h,j)}$, $\mathcal{E}_W$ and $\mathcal{E}_\Gamma$, respectively. And also, let $(A^{(t)}, \tilde{A}^{(t)})$ be a joint random variable which takes values on the set $\mathcal{A}^{(t)} \times \mathcal{A}^{(t)}$ such that $A^{(t)} \neq \tilde{A}^{(t)}$.

We assume that there exist the following mappings in the model of KI-MRA, $\pi^{(j)} : \mathcal{E}_S^{(j)} \to \mathcal{E}_1^{(j)} \times \ldots \times \mathcal{E}_n^{(j)}$ and $f_i : \mathcal{E}_i \to \mathcal{E}_i^{(1)} \times \ldots \times \mathcal{E}_i^{(N)}$, where $\mathcal{E}_i^{(j)}$ is a set of possible R_i's keys which are actually used at the period j[2]. Note that the assumption is natural and not so strange, since we will actually see these mappings in our constructions in Section 3. In the following, let $E_i^{(j)}$ be a random variable which takes values on $\mathcal{E}_i^{(j)}$.

Then, we can derive lower bounds of success probabilities of attacks as follows. The proof of sketch is given in Appendix C.

Theorem 1. *For any $i \in \{1, 2, \ldots, n\}$, any colluding group W with $R_i \notin W$, any $t \in \mathcal{T}$, and any set of key-exposed time periods Γ with $t \notin \Gamma$, we have the following inequalities:*

1. $P_{\Pi,I_A}(R_i, W, \Gamma, t) \geq 2^{-I(A^{(t)}; E_i^{(t)} | E_W, E_\Gamma)}$,
2. $P_{\Pi,S_A}(R_i, W, \Gamma, t) \geq 2^{-I(\tilde{A}^{(t)}; E_i^{(t)} | E_W, E_\Gamma, A^{(t)})}$,
3. $P_{\Pi,I_B}(R_i, W, t) \geq 2^{-I(A^{(t)}; E_i^{(t)} | E_W, MK)}$,
4. $P_{\Pi,S_B}(R_i, W, t) \geq 2^{-I(\tilde{A}^{(t)}; E_i^{(t)} | E_W, MK, A^{(t)})}$,

where $I(X; Y|Z)$ means the conditional mutual information of random variables X and Y given Z.

We next show lower bounds of memory-sizes of entities in KI-MRA. From Theorem 1, we obtain the following lower bounds of memory-sizes.

Theorem 2. *Let Π be an $(n, \omega; N, \gamma; \epsilon, \epsilon)$-one-time secure KI-MRA. Let $q := \epsilon^{-1}$. Then, for any $i \in \{1, 2, \ldots, n\}$, $j \in \mathcal{T}$ and $h \in \tilde{\mathcal{T}}$, we have*: (i) $|\mathcal{E}_S^{(j)}| \geq q^{2(\omega+1)}$; (ii) $|\mathcal{E}_i| \geq q^{2(\gamma+1)}$; (iii) $|\mathcal{MK}| \geq q^{2\gamma(\omega+1)}$; (iv) $|\mathcal{I}^{(h,j)}| \geq q^{2(\omega+1)}$; and (v) $|\mathcal{A}^{(j)}| \geq 2^{H(M)} q^{\omega+1}$. *In particular, if $\Pr_M$ is the uniform distribution, $|\mathcal{A}^{(j)}| \geq q^{\omega+1} |\mathcal{M}|$.*

Proof. The proof is given in Appendix B.

As we will see in the next section, the above lower bounds are tight. Therefore, we define optimality of constructions of KI-MRA as follows.

[2] Note that, $e_i^{(j)}$, a R_i's key actually used for a period j, may be a part of an entire key e_i or may be equal to the entire key itself.

Definition 3. A construction of $(n, \omega; N, \gamma; \epsilon, \epsilon)$-one-time secure KI-MRA is said to be *optimal* if it meets all the inequalities (i)-(v) in Theorem 2 with equalities.

3 Constructions

In this section, we propose two kinds of constructions of KI-MRA, direct and generic constructions.

3.1 Direct Construction

We provide a direct construction which is one-time secure KI-MRA in our model by using polynomials over finite fields. In addition, it is shown that the direct construction meets the lower bounds of key-sizes with equalities. Therefore, it turns out that the direct construction is optimal. The construction is given as follows.

1. **Key Generation Algorithm *KGen*.** For a security parameter 1^k, the algorithm *KGen* outputs matching secret-keys $e_S^{(0)}, mk, e_i (1 \leq i \leq n)$ for S, H, $R_i (1 \leq i \leq n)$ as follows. *KGen* picks a k-bit prime power q, where $q > \max(n, N)$, and constructs the finite field F_q with q elements. We assume that the identity of each receiver R_i is also denoted by R_i and that $R_i \subset F_q \setminus \{0\}$. Also, we assume $M \subset F_q \setminus \{0\}$, $\mathcal{T} = \{1, 2, \ldots, N\} \subset F_q \setminus \{0\}$ and $\tilde{\mathcal{T}} := \mathcal{T} \cup \{0\} \subset F_q$ by using appropriate encoding. And, *KGen* takes two random polynomials over F_q:

$$F(x, z) = \sum_{i=0}^{\omega} \sum_{k=0}^{1} a_{i,0,k} x^i z^k$$

$$mk(x, y, z) = \sum_{i=0}^{\omega} \sum_{j=1}^{\gamma} \sum_{k=0}^{1} a_{i,j,k} x^i y^j z^k,$$

   where each coefficient $a_{i,j,k}$ is chosen uniformly at random from F_q, and we define $x^0 = z^0 = 1$. *KGen* also computes $n + 1$ polynomials $e_S^{(0)}(x, z) := F(x, z)$ and $e_i(y, z) := F(x, z)|_{x=R_i} + mk(x, y, z)|_{x=R_i}$ $(1 \leq i \leq n)$. Then, the algorithm *KGen* outputs secret-keys $e_S^{(0)} := e_S^{(0)}(x, z)$, $mk := mk(x, y, z)$ and $e_i := e_i(y, z)$ $(1 \leq i \leq n)$ for S, H and R_i, respectively.
2. **Device Key-Updating Algorithm *KUpd** and Sender's Key-Updating Algorithm *KUpd*.** For two periods $h \in \tilde{\mathcal{T}}$, $j \in \mathcal{T}$ and $mk = mk(x, y, z)$, the algorithm *KUpd** generates a polynomial $mk^{(h,j)}(x, z) := mk(x, y, z)|_{y=j} - mk(x, y, z)|_{y=h}$. Then, *KUpd** outputs key-updating information $mk^{(h,j)} := mk^{(h,j)}(x, z)$. For $mk^{(h,j)}$ and $e_S^{(h)} := e_S^{(h)}(x, z)$, the algorithm *KUpd* generates the polynomial $e_S^{(j)}(x, z) := e_S^{(h)}(x, z) + mk^{(h,j)}(x, z)$. Then, *KUpd* outputs the secret-key at the period j, $e_S^{(j)} := e_S^{(j)}(x, z)$.

3. **Authentication Algorithm *KAuth*.** For a message $m \in F_q$ and $e_S^{(j)} = e_S^{(j)}(x,z)$, the algorithm *KAuth* generates the polynomial $\alpha(x) := e_S^{(j)}(x,z)|_{z=m}$, and outputs the authenticated message at the period j, $\alpha := (m, \alpha(x))$.
4. **Verification Algorithm *KVer*.** For an authenticated message at a period t, (α, t) $(\alpha = \alpha(x))$, and $e_i = e_i(y,z)$, the algorithm *KVer* outputs *true* if $\alpha(x)|_{x=R_i} = e_i(y,z)|_{y=t,z=m}$ holds, and otherwise outputs *false*.

We can show security of the above construction as follows. The proof of sketch is given in Appendix C.

Theorem 3. *The resulting KI-MRA by the above construction is* $(n, w; N, \gamma; \frac{1}{q}, \frac{1}{q})$*-one-time secure. Furthermore, the required memory-sizes of secret-keys and the size of authenticated messages are given as follows.*

$$|\mathcal{E}_S^{(j)}| = q^{2(\omega+1)}, \quad |\mathcal{E}_i| = q^{2(\gamma+1)}, \quad |\mathcal{MK}| = q^{2\gamma(\omega+1)}$$
$$|\mathcal{I}^{(h,j)}| = q^{2(\omega+1)}, \quad |A^{(j)}| = q^{\omega+1}|M|.$$

Therefore, the above construction is optimal.

3.2 Generic Construction

We propose a generic construction (i.e., a black box construction) of one-time secure KI-MRA by using CFFs (cover free families) and MRA-codes. In general, the merit to consider a generic construction lies in that it is possible to take general settings of parameters in the construction starting from underlying primitives, though it is often the case that generic constructions are inefficient compared to direct constructions. From this point of view, we propose a generic construction of KI-MRA by using both CFFs and MRA-codes. As we will see, our construction is simple and better CFFs and MRA-codes lead to better KI-MRAs. We start with describing the definition of CFF and the model of MRA-codes as follows.

Definition 4 (CFF[9]). Let $\mathcal{L} := \{l_1, l_2, \ldots, l_d\}$ be a universal set and $\mathcal{F} := \{F_1, F_2, \ldots, F_N\}$ be a family of subsets of $\mathcal{L}$. Then, we call it (d, N, γ)*-CFF (Cover Free Family)* if $F_{i_0} \not\subset F_{i_1} \cup F_{i_2} \cup \ldots \cup F_{i_\gamma}$ for all $F_{i_0}, F_{i_1} \ldots, F_{i_\gamma} \in \mathcal{F}$ where $F_{i_j} \neq F_{i_k}$ if $j \neq k$.

A trivial CFF is the family consisting of single-elements subsets, in which we have $N = d$ i.e., $\mathcal{L} = \{1, 2, \ldots, d\}$ and $\mathcal{F} = \{\{1\}, \{2\}, \ldots, \{d\}\}$. We note that there exist non-trivial constructions of CFFs. The constructions of CFFs are studied in various areas in mathematics such as finite geometry, design theory and probability theory. We also note that concrete methods for generating CFFs are given in [9][15]. Next, we describe a model of MRA-codes in [17].

MRA-codes. We consider the scenario where there are $n + 1$ entities, a sender $\tilde{S}$ and n receivers $\tilde{R}_1, \ldots, \tilde{R}_n$. The MRA-code $\tilde{\Pi}$ consists of a three-tuple of algorithms (*MGen*, *MAuth*, *MVer*) with four spaces, $\tilde{\mathcal{M}}$, $\mathcal{D}$, $\mathcal{U}$ and $\mathcal{V}$, where $\tilde{\mathcal{M}}$

is a finite set of possible messages, $\mathcal{D}$ is a finite set of possible authenticated messages, $\mathcal{U}$ and $\mathcal{V}$ are finite sets of possible secret-keys for the sender and receivers, respectively. *MGen* is a key generation algorithm, which takes security parameter on input and outputs matching keys $u \in \mathcal{U}$ and $v_i \in \mathcal{V}$ $(i = 1, 2, \ldots, n)$, where u and v_i are secret-keys for $\tilde{S}$ and $\tilde{R}_i$, respectively. *MAuth* is an algorithm for generating an authenticated message, and it is used when the sender wants to broadcast the authenticated message to all verifiers via an insecure broadcast channel. *MAuth* takes a secret-key $u \in \mathcal{U}$ and message $m \in \tilde{\mathcal{M}}$ on input and outputs an authenticated message $\delta \in \mathcal{D}$, and we write $\delta = MAuth(u, m)$ for it. On receiving δ, the receiver $\tilde{R}_i$ can check the validity of it by using *MVer*. *MVer* takes a secret-key $v_i \in \mathcal{V}$ and an authenticated message $\delta \in \mathcal{D}$ on input, and outputs *true* or *false*, where *true* is output if and only if δ is valid, and we write $true = MVer(v_i, \delta)$ or $false = MVer(v_i, \delta)$ for it. In MRA-codes, there are two kinds of attacks: the *impersonation attack* and *substitution attack*. The formal definitions of those attacks are given in Appendix A.

Our generic construction of KI-MRA is given as follows.

1. **Key Generation Algorithm *KGen*.** For a security parameter 1^k, the algorithm *KGen* outputs matching secret-keys for S, H $R_1, \ldots, R_n$ as follows. *KGen* generates (d, N, γ)-*CFF* $\mathcal{L} := \{l_1, \ldots, l_d\}$ and $\mathcal{F} := \{F_1, \ldots, F_N\}$, and makes them public to all entities. And *KGen* calls *MGen* N times with taking on input the security parameter 1^k. Let $(u_0^{(j)}, v_{1,0}^{(j)}, \ldots, v_{n,0}^{(j)})$ be the j-th output from *MGen* $(1 \leq j \leq N)$. Similarly, *KGen* calls *MGen* d times, and let $(u_1^{(l_j)}, v_{1,1}^{(l_j)}, \ldots, v_{n,1}^{(l_j)})$ be the j-th output $(1 \leq j \leq d)$[3]. Also, it sets $U^{(0)} := \emptyset$. Then, the algorithm *KGen* outputs secret-keys $e_S^{(0)} := (u_0^{(1)}, u_0^{(2)}, \ldots, u_0^{(N)}, U^{(0)})$, $mk := (u_1^{(l_1)}, u_1^{(l_2)}, \ldots, u_1^{(l_d)})$ and $e_i := (v_{i,0}^{(1)}, v_{i,0}^{(2)}, \ldots, v_{i,0}^{(N)}, v_{i,1}^{(l_1)}, v_{i,1}^{(l_2)}, \ldots, v_{i,1}^{(l_d)})$ for S, H and R_i, respectively.
2. **Device Key-Updating Algorithm *KUpd** and Sender's Key-Updating Algorithm *KUpd*.** For two periods $h \in \tilde{\mathcal{T}}$, $j \in \mathcal{T}$ and $mk = (u_1^{(l_1)}, \ldots, u_1^{(l_d)})$, *KUpd** generates $U^{(j)} := \{u_1^{(l)} | l \in F_j\}$. Then, *KUpd** outputs the key-updating information $mk^{(h,j)} := U^{(j)}$.

   For $mk^{(h,j)}$ and $e_S^{(h)} = (u_0^{(1)}, \ldots, u_0^{(N)}, U^{(h)})$, *KUpd* generates the secret-key at the period j, $e_S^{(j)} := (u_0^{(1)}, \ldots, u_0^{(N)}, U^{(j)})$, and outputs it.
3. **Authentication Algorithm *KAuth*.** For a message $m \in M$ and $e_S^{(j)} = (u_0^{(1)}, \ldots, u_0^{(N)}, U^{(j)})$, *KAuth* generates the authenticated message at the period j, $\alpha := (m, \delta_0^{(j)}, \delta_{i_1}^{(j)}, \ldots, \delta_{i_{|F_j|}}^{(j)})$, where $\delta_0^{(j)} := MAuth(u_0^{(j)}, m)$ and $\delta_{i_g}^{(j)} := MAuth(u_1^{(i_g)}, m)$ for all $i_g \in F_j$. *KAuth* then outputs α.
4. **Verification Algorithm *KVer*.** For an authenticated message at a period j, (α, j), where $\alpha = (m, \delta_0^{(j)}, \delta_{l_1}^{(j)}, \ldots, \delta_{l_{|F_j|}}^{(j)})$ and $e_i = (v_{i,0}^{(1)}, \ldots, v_{i,0}^{(N)}, v_{i,1}^{(l_1)}, \ldots, v_{i,1}^{(l_d)})$, *KVer* outputs *true* if $MVer(v_{i,0}^{(j)}, \delta_0^{(j)}) = true$ and $MVer(v_{i,1}^{(l_g)}, \delta_{l_g}^{(j)}) = true$ for all $l_g \in F_j$, and otherwise outputs *false*.

[3] We note that $(u_1^{(l_j)}, v_{1,1}^{(l_j)}, \ldots, v_{n,1}^{(l_j)})$ is corresponding to $l_j \in \mathcal{L}$.

The security of the above generic construction is shown as follows. The proof of sketch is given in Appendix C.

Theorem 4. *Given a (d, N, γ)-CFF $\mathcal{F}$ and an (n, ω, ϵ)-secure MRA-code $\tilde{\Pi}$, then the KI-MRA Π formed by the above construction based on the CFF and $\tilde{\Pi}$ is $(n, \omega; N, \gamma; \epsilon_A, \epsilon_B)$-one-time secure, where $\epsilon_A \leq \epsilon^{\phi}$ and $\epsilon_B \leq \epsilon$. Here, $\phi := \min(|F_{i_0} - \{F_{i_1} \cup \ldots \cup F_{i_\gamma}\}|)$, where the minimum is taken over all F_{i_0}, F_{i_1}, ..., $F_{i_\gamma} \in \mathcal{F}$. Furthermore, required memory-sizes of authenticated messages and secret-keys are given as follows*:

$$|\mathcal{E}_S^{(j)}| = (N + |F_j|)|\mathcal{U}|, \quad |\mathcal{E}_i| = (N + d)|\mathcal{V}|, \quad |\mathcal{MK}| = d|\mathcal{U}|$$
$$|\mathcal{I}^{(h,j)}| = |F_j||\mathcal{U}|, \quad |A^{(j)}| = (|F_j| + 1)|\mathcal{D}|.$$

Remark 1. In [17], the generic construction of MRA-codes by combining CFFs and A-codes [10][21] is proposed. Therefore, by combining our generic construction and the one in [17], KI-MRA can be constructed by using two kinds of simple primitives, CFFs and A-codes.

4 Concluding Remarks

In this paper, we studied information-theoretically secure authentication schemes with key-insulated security. Specifically, we introduced a model of information-theoretically secure multireceiver authentication codes (KI-MRA), and proposed security notions and their formalizations in our model. In addition, we derived tight lower bounds of memory-sizes required for the KI-MRA. Furthermore, we provided two kinds of constructions: direct and generic constructions which were provably secure in our security definition. In particular, It was shown that the direct construction was optimal.

In this paper, for simplicity, we discussed the one-time model of KI-MRA. However, it would be interesting to extend our one-time model to the multi-use model of KI-MRA. Also, it would be a future research to study information-theoretically secure key-insulated signature schemes which have security notions stronger than those of KI-MRAs.

Acknowledgements

We would like to thank anonymous referees for helpful and valuable comments.

References

1. Anderson, R.: Two remarks on public key cryptology. In: ACM CCCS (1997) (invited Lecture), `http://www.cl.cam.ac.uk/users/rja14/`
2. Bellare, M., Miner, S.K.: A Forward-Secure Digital Signature Scheme. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 431–448. Springer, Heidelberg (1999)

3. Canetti, R., Goldwasser, S.: An efficient threshold public-key cryptosystem secure against adaptive chosen-ciphertext attack. In: Stern, J. (ed.) EUROCRYPT 1999. LNCS, vol. 1592, pp. 90–106. Springer, Heidelberg (1999)
4. Canneti, R., Halevi, S., Katz, J.: A forward secure public key encryption scheme. J. Cryptology 20(3), 265–294 (2007)
5. Desmedt, Y., Frankel, Y.: Threshold cryptosystems. In: Brassard, G. (ed.) CRYPTO 1989. LNCS, vol. 435, pp. 307–315. Springer, Heidelberg (1990)
6. Desmedt, Y., Frankel, Y., Yung, M.: Multi-receiver/Multi-sender network security: efficient authenticated multicast/feedback. In: Proc. of IEEE Inforcom 1992, pp. 2045–2054 (1992)
7. Dodis, Y., Katz, J., Xu, S., Yung, M.: Key-Insulated Public-Key Cryptosystems. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 65–82. Springer, Heidelberg (2002)
8. Dodis, Y., Katz, J., Xu, S., Yung, M.: Strong Key-Insulated Signature Schemes. In: Desmedt, Y.G. (ed.) PKC 2003. LNCS, vol. 2567, pp. 130–144. Springer, Heidelberg (2002)
9. Erdös, P., Frankl, P., Furedi, Z.: Families of finite sets in which no sets is covered by the union of r others. Israel Journal of Mathematics 51, 79–89 (1985)
10. Gilbert, E.N., MacWilliams, F.J., Sloane, N.J.A.: Codes which detect deception. Bell System Technical Journal 53, 405–425 (1974)
11. Hanaoka, Y., Hanaoka, G., Shikata, J., Imai, H.: Information-Theoretically Secure Key Insulated Encryption: Models, Bounds and Constructions. IEICE Trans. Fundamentals E.87-A(10), 2521–2532 (2004)
12. Hanaoka, G., Shikata, J., Zheng, Y., Imai, H.: Unconditionally secure digital signature schemes admitting transferability. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 130–142. Springer, Heidelberg (2000)
13. Itkis, G., Reyzin, L.: SiBIR: Signer-Base Intrusion-Resilient Signatures. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 499–514. Springer, Heidelberg (2002)
14. Johansson, T.: Further results on asymmetric authentication schemes. Information and Computation 151, 100–133 (1999)
15. Kumar, R., Rajagopalan, S., Sahai, A.: Coding constructions for blacklisting problems without computational assumptions. In: Wiener, M. (ed.) CRYPTO 1999. LNCS, vol. 1666, pp. 609–623. Springer, Heidelberg (1999)
16. Rivest, R.: Unconditionally secure commitment and oblivious transfer schemes using private channels and a trusted initializer (1999) (manuscript), `http://people.csail.mit.edu/rivest/Rivest-commitment.pdf`
17. Safavi-Naini, R., Wang, H.: Multireceiver authentication codes: model, bounds, constructions and extensions. Information and Computation 151, 148–172 (1999)
18. Shikata, J., Hanaoka, G., Zheng, Y., Imai, H.: Security Notions for Unconditionally Secure Signature Schemes. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 434–449. Springer, Heidelberg (2002)
19. Shor, P.W.: Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM J. Compt. 26(5), 1484–1509 (1997)
20. Shoup, V., Gennaro, R.: Securing threshold cryptosystems against chosen-ciphertext attack. In: Nyberg, K. (ed.) EUROCRYPT 1998. LNCS, vol. 1403, pp. 1–16. Springer, Heidelberg (1998)
21. Simmons, G.J.: Authentication theory/coding theory. In: Blakely, G.R., Chaum, D. (eds.) CRYPTO 1984. LNCS, vol. 196, pp. 411–431. Springer, Heidelberg (1985)

Appendix A: Security Notions of MRA-Codes

We describe the security notions of MRA-codes shown in [6], [17], [14]. In MRA-codes, two kinds of attacks are considered: *impersonation attack* and *substitution attack*. We describe the formal definitions of those security notions as follows.

Definition 5. [17] *Let $\tilde{\Pi}$ be a MRA-codes. The scheme $\tilde{\Pi}$ said to be $(\tilde{n}, \tilde{\omega}, \tilde{\epsilon})$-secure if* $\max(P_{\tilde{\Pi},I}, P_{\tilde{\Pi},S}) \leq \tilde{\epsilon}$ *where $P_{\tilde{\Pi},I}$ and $P_{\tilde{\Pi},S}$ are defined as follows.*

1) ***Impersonation Attack:*** *The adversary who corrupts at most $\tilde{\omega}$ receivers tries to generate a fraudulent authenticated message δ that has not been legally generated by the sender $\tilde{S}$ but will be accepted by a receiver $\tilde{R}_i$. Here, we assume that $\tilde{R}_i$ is not included in the colluders, and the adversary can obtain information by pooling secret-keys of corrupted receivers. Success probability of this attack denoted by $P_{\tilde{\Pi},I}$ is defined as follows. For any $\tilde{W} \in \mathcal{P}(\tilde{R}, \tilde{\omega})$ and $\tilde{R}_i \notin \tilde{W}$, we define $P_{\tilde{\Pi},I}(\tilde{R}_i, \tilde{W})$ as follows.*

$$P_{\tilde{\Pi},I}(\tilde{R}_i, \tilde{W}) := \max_{e_{\tilde{W}}} \max_{\delta} \Pr(MVer(v_i, \delta) = true | e_{\tilde{W}})$$

where the probability is taken over random choice of MGen, and the maximum is taken over: all possible sets of the colluders' secret-keys $e_{\tilde{W}} \in \mathcal{E}_{\tilde{W}}$; and all possible authenticated messages $\delta \in \mathcal{D}$. Then, the probability $P_{\tilde{\Pi},I}$ is defined as $P_{\tilde{\Pi},I} := \max_{\tilde{R}_i, \tilde{W}}(\tilde{R}_i, \tilde{W})$.

2) ***Substitution Attack:*** *The adversary who corrupts at most $\tilde{\omega}$ receivers tries to generate a fraudulent authenticated message δ that has not been legally generated by the sender $\tilde{S}$ but will be accepted by a receiver $\tilde{R}_i$, after observing the transmitted authenticated message δ'. Here, we assume that $\tilde{R}_i$ is not included in the colluders, and the adversary can obtain information by pooling secret-keys of corrupted receivers. Success probability of this attack denoted by $P_{\tilde{\Pi},S}$ is defined as follows. For any $\tilde{W} \in \mathcal{P}(\tilde{R}, \tilde{\omega})$ and $\tilde{R}_i \notin \tilde{W}$, we define $P_{\tilde{\Pi},S}(\tilde{R}_i, \tilde{W})$ as follows.*

$$P_{\tilde{\Pi},S}(\tilde{R}_i, \tilde{W}) := \max_{e_{\tilde{W}}} \max_{\delta'} \max_{\delta \neq \delta'} \Pr(MVer(v_i, \delta) = true | e_{\tilde{W}}, \delta')$$

where the probability is taken over random choice of MGen, and the maximum is taken over: all possible sets of the colluders' secret-keys $e_{\tilde{W}} \in \mathcal{E}_{\tilde{W}}$; and all possible authenticated messages $\delta', \delta \in \mathcal{D}$ such that $\delta \neq \delta'$. Then, the probability $P_{\tilde{\Pi},S}$ is defined as $P_{\tilde{\Pi},S} := \max_{\tilde{R}_i, \tilde{W}}(\tilde{R}_i, \tilde{W})$.

Appendix B: Proof of Theorem 2

The proof of Theorem 2 follows from Lemmas 2-6 below.

Lemma 1. Let R_i be a receiver and t be a period. For any $W \in \mathcal{P}(\mathcal{R}, \omega)$ and any $\Gamma \in \mathcal{P}(\mathcal{T}, \gamma)$ such that $R_i \notin W$ and $t \notin \Gamma$, we have $P_{\Pi,S_A}(R_i, W, \Gamma, t) \geq 2^{-H(E_i^{(t)}|E_W, E_\Gamma, A^{(t)})}$.

Proof. The lemma follows from Theorem 1 straightforwardly, since $I(\tilde{A}^{(t)}; E_i^{(t)} \mid E_W,\ E_\Gamma,\ A^{(t)}) = H(E_i^{(t)}|E_W,\ E_\Gamma, A^{(t)}) - H(E_i^{(t)} \mid E_W,\ E_\Gamma,\ \tilde{A}^{(t)},\ A^{(t)}) \leq H(E_i^{(t)}|E_W,\ E_\Gamma, A^{(t)})$. □

Lemma 2. $|\mathcal{E}_S^{(j)}| \geq q^{2(\omega+1)}$ for any $j \in \tilde{\mathcal{T}}$.

Proof. We first prove that $H(E_S^{(j)}|E_\Gamma) \geq 2(\omega+1)\log q$ for any $\Gamma \in \mathcal{P}(\mathcal{T}, \gamma)$ and $j \in \mathcal{T}$ with $j \notin \Gamma$. Let $W_i := \{R_1, \ldots, R_{i-1}, R_{i+1}, \ldots, R_{\omega+1}\}$. Then, for any $\Gamma \in \mathcal{P}(\mathcal{T}, \gamma)$ and $j \in \mathcal{T}$ with $j \notin \Gamma$, we have

$$\prod_{i=1}^{\omega+1} P_{\Pi,I_A}(R_i, W_i, \Gamma, j) P_{\Pi,S_A}(R_i, W_i, \Gamma, j) \geq 2^{-\sum_{i=1}^{\omega+1} H(E_i^{(j)}|E_1^{(j)},\ldots,E_{i-1}^{(j)},E_\Gamma)} \quad (1)$$

$$= 2^{-H(E_1^{(j)},\ldots,E_{\omega+1}^{(j)}|E_\Gamma)}$$

$$\geq 2^{-H(E_S^{(j)}|E_\Gamma)}, \quad (2)$$

where (1) follows from Theorem 1 and Lemma 1, and (2) is shown by considering the mapping $\pi^{(j)} : \mathcal{E}_S^{(j)} \to \mathcal{E}_1^{(j)} \times \ldots \times \mathcal{E}_n^{(j)}$.

Since $\prod_{i=1}^{\omega+1} P_{\Pi,I_A}(R_i, W_i, \Gamma, j) P_{\Pi,S_A}(R_i, W_i, \Gamma, j) \leq \prod_{i=1}^{\omega+1} (\frac{1}{q})^2 = (\frac{1}{q})^{2(\omega+1)}$, we obtain $2^{-H(E_S^{(j)}|E_\Gamma)} \leq (\frac{1}{q})^{2(\omega+1)}$ and hence $H(E_S^{(j)}|E_\Gamma) \geq 2(\omega+1)\log q$. Therefore, we have $|\mathcal{E}_S^{(j)}| \geq q^{2(\omega+1)}$, since $H(E_S^{(j)}|E_\Gamma) \leq \log|\mathcal{E}_S^{(j)}|$. □

Lemma 3. $|\mathcal{E}_i| \geq q^{2(\gamma+1)}$ for any $i \in \{1, 2, \ldots, n\}$.

Proof. Let $\Gamma_j := \{1, \ldots, j-1, j+1, \ldots, \gamma+1\}$. Then, for $W = \emptyset$, we have

$$\prod_{j=1}^{\gamma+1} P_{\Pi,I_A}(R_i, W, \Gamma_j, j) P_{\Pi,S_A}(R_i, W, \Gamma_j, j) \geq \prod_{j=1}^{\gamma+1} 2^{-H(E_i^{(j)}|E_S^{(1)},\ldots,E_S^{(j-1)})} \quad (3)$$

$$\geq \prod_{j=1}^{\gamma+1} 2^{-H(E_i^{(j)}|E_i^{(1)},\ldots,E_i^{(j-1)})} \quad (4)$$

$$= 2^{-H(E_i^{(1)},\ldots,E_i^{(\gamma+1)})}$$

$$\geq 2^{-H(E_i)}. \quad (5)$$

In the above expressions, (3) follows from Theorem 1 and Lemma 1, (4) is shown by considering the mapping $p_i^{(k)} \circ \pi^{(k)} : \mathcal{E}_S^{(k)} \to \mathcal{E}_i^{(k)}$ for $1 \leq k \leq j-1$, where $p_i^{(k)} : \mathcal{E}_1^{(k)} \times \ldots \times \mathcal{E}_n^{(k)} \to \mathcal{E}_i^{(k)}$ is the i-th projection, and (5) is shown by considering the mapping $f_i : \mathcal{E}_i \to \mathcal{E}_i^{(1)} \times \ldots \times \mathcal{E}_i^{(N)}$.

Since $\prod_{i=1}^{\gamma+1} P_{\Pi,I_A}(R_i, W, \Gamma_j, j) P_{\Pi,S_A}(R_i, W, \Gamma_j, j) \leq \prod_{i=1}^{\gamma+1} (\frac{1}{q})^2 = (\frac{1}{q})^{2(\gamma+1)}$, we obtain $|\mathcal{E}_i| \geq 2^{H(E_i)} \geq q^{2(\gamma+1)}$. □

Lemma 4. $|\mathcal{MK}| \geq q^{2\gamma(\omega+1)}$.

Proof. For any $\Gamma = \{k_1, k_2, \ldots, k_\gamma\} \in \mathcal{P}(\mathcal{T}, \gamma)$ with $|\Gamma| = \gamma$, and $j \in \mathcal{T}$ such that $j \notin \Gamma$, we have

$$\begin{aligned} H(MK) &\geq H(MK|E_S^{(j)}) \\ &\geq I(E_S^{(k_1)}, \ldots, E_S^{(k_\gamma)}; MK|E_S^{(j)}) \\ &= H(E_S^{(k_1)}, \ldots, E_S^{(k_\gamma)}|E_S^{(j)}) \\ &= \sum_{i=1}^{\gamma} H(E_S^{(k_i)}|E_S^{(j)}, E_S^{(k_1)}, \ldots, E_S^{(k_{i-1})}) \\ &\geq 2\gamma(\omega+1)\log q, \end{aligned} \tag{6}$$

where (6) follows from the proof of Lemma 2. Therefore, we have $|\mathcal{MK}| \geq 2^{H(MK)} \geq q^{2\gamma(\omega+1)}$. □

Lemma 5. $|\mathcal{I}^{(h,j)}| \geq q^{2(\omega+1)}$ for any $h \in \tilde{\mathcal{T}}$ and $j \in \mathcal{T}$.

Proof. From the deterministic algorithm (i.e., mapping) $KUpd$: $\mathcal{E}_S \times \mathcal{I} \to \mathcal{E}_S$, it follows that $H(I^{(h,j)}|E_S^{(h)}) \geq H(E_S^{(j)}|E_S^{(h)})$. Thus, we have

$$H(I^{(h,j)}) \geq H(I^{(h,j)}|E_S^{(h)}) \geq H(E_S^{(j)}|E_S^{(h)}) \geq 2(\omega+1)\log q,$$

where the last inequality follows from the proof of Lemma 2. Therefore, we have $|\mathcal{I}^{(h,j)}| \geq 2^{H(I^{(h,j)})} \geq q^{2(\omega+1)}$. □

Lemma 6. $|\mathcal{A}^{(j)}| \geq 2^{H(M)} q^{\omega+1}$ *for any* $j \in \mathcal{T}$. In particular, if $\Pr_M$ is the uniform distribution, we have $|\mathcal{A}^{(j)}| \geq q^{\omega+1}|M|$ *for any* $j \in \mathcal{T}$.

Proof. For any $j \in \mathcal{T}$ and any $\Gamma \in \mathcal{P}(\mathcal{T}, \gamma)$ such that $j \notin \Gamma$, we have $I(A^{(j)}; E_S|E_\Gamma) \geq I(A^{(j)}; E_1, \ldots, E_{\omega+1}|E_\Gamma)$ by considering the mapping $\pi : \mathcal{E}_S \to \mathcal{E}_1 \times \cdots \times \mathcal{E}_n$. Let $W_i := \{R_1, R_2, \ldots, R_{i-1}\}$. Then, we have

$$\begin{aligned} 2^{-I(A^{(j)};E_S|E_\Gamma)} &\leq 2^{-I(A^{(j)};E_1,\ldots,E_{\omega+1}|E_\Gamma)} \\ &= 2^{-\sum_{i=1}^{\omega+1} I(A^{(j)};E_i|E_1,\ldots,E_{i-1},E_\Gamma)} \\ &\leq \prod_{i=1}^{\omega+1} 2^{-I(A^{(j)};E_i^{(j)}|E_1,\ldots,E_{i-1},E_\Gamma)} \qquad (7) \\ &\leq \prod_{i=1}^{\omega+1} P_{\Pi,I_A}(R_i, W_i, \Gamma, j) \qquad (8) \\ &\leq (P_{\Pi,A})^{\omega+1} \leq \left(\frac{1}{q}\right)^{\omega+1}, \end{aligned}$$

where (7) is shown by considering the mapping $f_i : \mathcal{E}_i \to \mathcal{E}_i^{(1)} \times \ldots \times \mathcal{E}_i^{(N)}$, and (8) follows from Theorem 1. In addition, for $\Gamma = \emptyset$, we have

$$2^{-I(A^{(j)};E_S|E_\Gamma)} = 2^{-H(A^{(j)})+H(A^{(j)}|E_S)} \geq \frac{2^{H(M)}}{|\mathcal{A}^{(j)}|},$$

where the last inequality follows from the deterministic algorithm $KAuth$: $\mathcal{E}_S \times \mathcal{M} \to \mathcal{A}$. Therefore, we obtain $|\mathcal{A}^{(j)}| \geq 2^{H(M)} q^{\omega+1}$. □

Appendix C: Sketch Proofs

Sketch Proof of Theorem 1. The proof can be shown in a way similar to the proof of Theorem 3.2 in [17]. Here, we only show a sketch proof of the first inequality. We define a characteristic function $\mathcal{X}_{I_A}$ as follows.

$$\mathcal{X}_{I_A}((\alpha,t), e_i^{(t)}, e_W, e_\Gamma) = \begin{cases} 1 \text{ if } KVer(e_i, \alpha, t) = true \wedge \Pr((\alpha,t), e_i^{(t)}, e_W, e_\Gamma) \neq 0 \\ 0 \text{ otherwise.} \end{cases}$$

Then, from Definition 2, we can express $P_{\Pi,I_A}(R_i, W, \Gamma, t)$ as

$$P_{\Pi,I_A}(R_i, W, \Gamma, t) = \max_{e_W} \max_{e_\Gamma} \max_{(\alpha,t)} \sum_{e_i^{(t)}} \mathcal{X}_{I_A}((\alpha,t), e_i^{(t)}, e_W, e_\Gamma) \Pr(e_i^{(t)} | e_W, e_\Gamma).$$

By a way similar to the proof of Theorem 3.2 in [17], we have $P_{\Pi,I_A}(R_i, W, \Gamma, t) \geq 2^{-I(A^{(t)}; E_i^{(t)} | E_W, E_\Gamma)}$. Similarly, other inequalities can also be proved. □

Sketch Proof of Theorem 3. The proof can be directly shown as in the proofs of constructions of MRA (For example, see [17] [14]). Here, we only describe the outline of the proof of $P_{\Pi,S} \leq \frac{1}{q}$, since other ones can be shown by a similar idea. To succeed in the substitution attack in the exposure type A, the adversary will generate a fraudulent authenticated message at a period t (α, t), where $\alpha = (m, \alpha(x))$, under the following conditions: the adversary can obtain γ exposed secret-keys for the sender, ω secret-keys for corrupted receivers and a valid authenticated message at the same period (α', t), where $\alpha' \neq \alpha$. However, the degrees of $F(x,z) + mk(x,y,z)$ with respect to x, y and z are at most ω, γ and 1, respectively. Thus, for the message m, the adversary cannot guess the polynomial $\alpha(x) = F(x,m) + mk(x,t,m)$ with probability more than $1/q$. Therefore, we have $P_{\Pi,S_A} \leq \frac{1}{q}$. In a manner similar to this, we can prove that $P_{\Pi,I_A} \leq \frac{1}{q}$. Thus, we have $P_{\Pi,A} = \max(P_{\Pi,I_A}, P_{\Pi,S_A}) \leq \frac{1}{q}$. Similarly, we can also prove that $P_{\Pi,B} = \max(P_{\Pi,I_B}, P_{\Pi,S_B}) \leq \frac{1}{q}$. Furthermore, it is straightforward to evaluate memory-sizes required in the construction. □

Sketch Proof of Theorem 4. The proof of security can be directly shown by the definition of CFF and security of MRA. Here, we only describe the outline of the proof of $P_{\Pi,S_A} \leq \epsilon^\phi$, since other ones can be shown by a similar idea. The adversary can know γ sets $U^{(1)}, U^{(2)}, \ldots, U^{(\gamma)}$ from γ exposed secret-keys for the sender. However, from the definition of CFF, the adversary cannot obtain at least ϕ elements of the set $U^{(t)} = \{u_1^{(l)} | l \in F_t\}$. Therefore, the adversary needs to forge at least ϕ authenticated messages of the underlying MRA-code. Thus, we have $P_{\Pi,S_A} \leq \epsilon^\phi$. In a manner similar to this, we can prove that $P_{\Pi,I_A} \leq \epsilon^\phi$. Thus, we have $P_{\Pi,A} = \max(P_{\Pi,I_A}, P_{\Pi,S_A}) \leq \epsilon^\phi$. Similarly, we can also prove that $P_{\Pi,B} = \max(P_{\Pi,I_B}, P_{\Pi,S_B}) \leq \epsilon$. Furthermore, it is straightforward to evaluate memory-sizes required in the construction. □