IEICE TRANS. FUNDAMENTALS, VOL.E106–A, NO.3 MARCH 2023

PAPER Special Section on Information Theory and Its Applications

Multi-Designated Receiver Authentication Codes: Models and Constructions*

Yohei WATANABE[†a)], ***Member***, **Takenobu SEITO**[††b)], ***Nonmember***, ***and*** **Junji SHIKATA**[††,†††c)], ***Member***

SUMMARY An *authentication code* (A-code) is a two-party message authentication code in the information-theoretic security setting. One of the variants of A-codes is a *multi-receiver authentication code* (MRA-code), where there are a single sender and multiple receivers and the sender can create a single authenticator so that *all* receivers accepts it unless it is maliciously modified. In this paper, we introduce a *multi-designated receiver authentication code* (MDRA-code) with information-theoretic security as an extension of MRA-codes. The purpose of MDRA-codes is to securely transmit a message via a broadcast channel from a single sender to an *arbitrary subset* of multiple receivers that have been designated by the sender, and only the receivers in the subset (i.e., not all receivers) should accept the message if an adversary is absent. This paper proposes a model and security formalization of MDRA-codes, and provides constructions of MDRA-codes.

key words: *authentication codes, broadcast authentication, information theoretic security*

1. Introduction

An *authentication code* (A-code) [2], [3] provides a (virtual) authenticated channel between two users in the sense of information theoretic security, and is one of the unconditionally secure fundamental cryptographic primitives, which can provide security against quantum computers from the aspect of information theoretic security. A-codes and their variants have been investigated for almost half a century: A-codes and extended security notions [4]–[10]; multi-sender A-codes (MSA-codes) [11], [12]; multi-receiver A-codes (MRA-codes) [11], [13], [14]; and other extensions such as digital signatures and A-codes in the manual channel model [15]–[18].

This paper focuses on an extension of MRA-codes. In MRA-codes, a sender generates an authenticator (or a tag) for a message with sender's secret key, and the sender sends the message and authenticator via a broadcast channel; each receiver can check the validity of the message by using the attached authenticator and the receiver's secret key. It should be noted that the purpose of MRA-codes is to securely transmit a message from the single sender to *all receivers*, and all receivers should accept the message if an adversary is absent.

1.1 Our Contributions

In this paper, we consider and define a model of multi-designated receiver authentication codes (MDRA-codes) with information theoretic security. The purpose of MDRA-codes is to securely transmit a message from a single sender to *an arbitrary subset of receivers* that have been designated by the sender, and only the receivers in the subset (i.e., not all receivers) should accept the message if an adversary is absent. This type of authentication schemes can be regarded as a natural extension of MRA-codes, since MRA-codes are captured as a special case of the MDRA-codes where the sender selects the whole set of receivers.

Specifically, in Sect. 2, we extend security notions of (MR)A-codes and newly introduce a notion of anonymity, which guarantees secrecy of information on designated receivers.

We then propose two concrete MDRA-codes in Sect. 3. One is a simple generic construction from any A-codes and any MRA-codes. The other is a more efficient direct construction over finite fields.

In MDRA-codes, each receiver can judge whether the receiver is designated by the output of the verification algorithm, and it is the only means of checking the status. This is due to the anonymity notion; an authenticator leaks no information on designated receivers. In particular, non-designated receivers get a rejection symbol as the output of the verification algorithm regardless of whether an authenticator is forged. Namely, each non-designated receiver cannot distinguish the following two case: the receiver is undesignated; or the receiver is designated but the corresponding authenticator is forged. For this reason, in Sect. 4, we formalize an extended functionality, called *forgery detection*; it guarantees that a receiver can distinguish forged authenticators from honestly-generated ones even if the receiver is not designated. We show that our generic construction can be easily modified to meet the forgery detection functionality.

Manuscript received February 28, 2022.
Manuscript revised July 2, 2022.
Manuscript publicized September 30, 2022.

[†]The author is with the University of Electro-Communications, Chofu-shi, 182-8585 Japan.
[††]The authors are with Institute of Advanced Sciences, Yokohama National University, Yokohama-shi, 240-8501 Japan.
[†††]The author is with Graduate School of Environment and Information Sciences, Yokohama National University, Yokohama-shi, 240-8501 Japan.

*A preliminary version appeared at CISS 2022 [1]. This is a full version.

a) E-mail: watanabe@uec.ac.jp
b) E-mail: seito-takenobu-bk@ynu.ac.jp
c) E-mail: shikata-junji-rb@ynu.ac.jp

DOI: 10.1587/transfun.2022TAP0015

1.2 Related Work

In information-theoretically secure broadcast encryption (BE) [19]–[22], there are a single sender and multiple receivers, and the sender can specify an arbitrary subset of receivers who can decrypt a ciphertext sent via a broadcast channel. Hence, both MDRA-codes and BEs are regarded as being similar in the sense that a sender can give a certain type of functionality to an arbitrary subset of receivers, namely verification functionality in MDRA-codes and decryption functionality in BEs. However, authentication and encryption are quite different functionalities, and it is not trivial to construct MDRA-codes from BEs. To the best of our knowledge, there is no broadcast authentication schemes with information-theoretic security that enables a sender to specify an arbitrary subset from all receivers while keeping it secret. Recently, anonymous broadcast authentication (ABA) was proposed in [23], and one might think it is similar to our model. However, ABA is constructed based on (computationally secure) symmetric-key cryptography, and its model and security formalization is not given in the information-theoretic security setting. In addition, there are several schemes targeting one-to-many or many-to-many authenticated communications [24]–[28], however, those work is quite different from the MDRA-codes with information theoretic security.

Besides, MDRA-codes can also be viewed as an information-theoretically secure variant of *multi-designated verifier signatures* (MDVS) [29], which are digital signature schemes where a sender can designated multiple verifiers who can check the validity of signatures. Note that MDVS has been considered in the computational security setting, therefore it only provides security against probabilistic polynomial-time adversaries.

1.3 Motivating Scenario

MDRA-codes can be used for remotely controlling multiple devices as in ABA [23], which is a computationally secure analogue of MDRA-codes. Consider a system where multiple devices are involved and some of them are infected with malware. With MDRA-codes, a systems manager can bring the infected devices to a halt simultaneously; a systems manager designates the infected devices and generates an authenticator for a message of a 'kill' command, and all devices (including both designated and non-designated ones) check the validity of the authenticator. If a device accepts it, then it executes the command, i.e., it halts; otherwise, the device keeps working[†]. The systems manager just has to broadcast the authenticator of MDRA-codes to all devices, while traditional A-codes require one-to-one communications with each infected device. Moreover, the one-to-one communications obviously leak information on which devices are infected, which should be treated as sensitive information [30]. The anonymity notion of MDRA-codes masks such information. Although we have discussed only secure device halts, various commands, e.g., 'sleep' and 'wakeup,' can also be used in the above system.

[†]We here assume that the verification process is done in an isolated area from malware, e.g., an external module connected between a device and power source; when the module turns off itself, then the connected device is also powered off. Therefore, the malware cannot affect the verification process.

1.4 Refinements

A conference version of this paper appeared in [1]. This paper is the full version and includes the following refinements and improvements.

- First, we revisit definitions of correctness and security notions. In the proceedings version [1], we defined correctness and three security notions; (d, w, ε)-*security*, *anonymity*, and *consistency*. We revisit the definition of correctness and modify it so that it is parametarized by probability δ, which is called δ-correctness. Moreover, we figure out that δ-correctness and (d, w, ε)-security imply what the consistency property defined in [1], and omit the definition of consistency. Besides, we give a new definition of anonymity based on an existing anonymous encryption scheme with information theoretic security [31].
- Second, we revisit a generic construction from A-codes, which was proposed in [1]. The construction is insufficient for (d, w, ε)-security and we modify it by using an MRA-code as an additional building block.
- Third, we newly formalize the forgery detection functionality and show a generic construction of a forgery-detectable MDRA-code.

2. Model

In this section, we introduce MDRA-codes. As in papers on MRA-codes [11], [13], [14], throughout this paper, we consider a *one-time model*; a sender generates and sends an authenticator to receivers only once.

Notation. For any natural number $n \in \mathbb{N}$, we denote $\{1, \ldots, n\}$ by $[n]$.

2.1 Algorithms and Correctness

In MDRA-codes, there are $n + 2$ entities, $\mathsf{TA}, \mathsf{S}, \mathcal{R} := \{\mathsf{R}_1, \ldots, \mathsf{R}_n\}$, where $\mathcal{R}$ is a receiver set. At the beginning of the protocol, a trusted authority TA runs Gen algorithm and obtains $n+1$ secret keys $\mathsf{e}_\mathsf{S}, \mathsf{e}_1, \ldots, \mathsf{e}_n$, where e_S and e_i $(i \in [n])$ are secret keys for a sender S and receiver R_i, respectively. Those keys are sent to the corresponding entities via secure channels. After receiving e_S, S can designate an arbitrary subset $\mathcal{D}$ of all receivers $\mathcal{R}$ and run Auth algorithm to generate an authenticator (or a tag) $\tau_\mathcal{D}$ for a message $\mathsf{m} \in \mathcal{M}$ so that only receivers in $\mathcal{D}$ accept it. S broadcasts $(\mathsf{m}, \tau_\mathcal{D})$ to all

receivers via a broadcast channel. If R_i who has their secret key e_i is designated, i.e., $\mathsf{R}_i \in \mathcal{D}$, R_i can check the validity of $(\mathsf{m}, \tau_{\mathcal{D}})$. R_i accepts it unless the pair is (maliciously) modified. On the other hand, a non-designated receiver $\mathsf{R}_j \notin \mathcal{D}$ cannot check the validity with Vrfy algorithm. Namely, R_j does not accept $(\mathsf{m}, \tau_{\mathcal{D}})$ even if the pair does not modified.

Formally, we define MDRA-codes as follows.

Definition 1 (MDRA-codes). An MDRA-code $\Pi \coloneqq (\mathsf{Gen}, \mathsf{Auth}, \mathsf{Ver})$ with $n+2$ entities, $\mathsf{TA}, \mathsf{S}, \mathcal{R} \coloneqq \{\mathsf{R}_1, \ldots, \mathsf{R}_n\}$ and three finite spaces $\mathcal{M}, \mathcal{E}, \mathcal{T}$ is defined as follows.

Entities. There are $n+2$ entities: a trusted authority TA that generates secret information and securely sends it to the corresponding entities, a sender S, and n receivers $\mathcal{R} \coloneqq \{\mathsf{R}_1, \ldots, \mathsf{R}_n\}$, where $\mathcal{R}$ is a receiver set.

Spaces. $\mathcal{M}$, $\mathcal{E}$, and $\mathcal{T}$ are finite sets of messages, secret keys, and tags (or authenticators). More specifically, let $\mathcal{E}_{\mathsf{S}}$ and $\mathcal{E}_i$ ($i \in [n]$) be secret-key sets for S and R_i, respectively, and we define $\mathcal{E} \coloneqq \mathcal{E}_{\mathsf{S}} \times \mathcal{E}_1 \times \cdots \times \mathcal{E}_n$. They may be determined when Gen is executed.

Algorithms.

1. $(\mathsf{e}_{\mathsf{S}}, \mathsf{e}_1, \ldots, \mathsf{e}_n) \leftarrow \mathsf{Gen}(n, d, w)$: It is a probabilistic algorithm for setup and run by TA. It takes the number of receivers n, the number of designated receivers d, and the maximum number of receivers w that Π allows an adversary to corrupt as input, and outputs secret keys for each entity, where $\mathsf{e}_{\mathsf{S}} \in \mathcal{E}_{\mathsf{S}}$ and $\mathsf{e}_i \in \mathcal{E}_i$ are ones for S and R_i ($i \in [n]$), respectively.

2. $\tau_{\mathcal{D}} \leftarrow \mathsf{Auth}(\mathsf{e}_{\mathsf{S}}, \mathsf{m}, \mathcal{D})$: It is an algorithm for authenticator generation and run by S. It takes S's secret key e_{S}, a message $\mathsf{m} \in \mathcal{M}$, and designated receivers $\mathcal{D} \subset \mathcal{R}$ such that $|\mathcal{D}| = d$ as input, and outputs an authenticator $\tau_{\mathcal{D}} \in \mathcal{T}$.

3. $\mathsf{ans} \leftarrow \mathsf{Ver}(\mathsf{e}_i, \mathsf{m}, \tau_{\mathcal{D}})$: It is a deterministic algorithm for verification and run by R_i. It takes R_i's secret key e_i, a message m, and an authenticator $\tau_{\mathcal{D}}$ as input, and outputs $\mathsf{ans} \in \{\mathtt{true}, \mathtt{false}\}$, where `true` and `false` indicate 'accept' and 'reject,' respectively.

We define the correctness property of MDRA-codes as follows.

Definition 2 (δ-correctness). Let Π be an MDRA-code. We say Π meets δ-correctness if for all $n, d, w \in \mathbb{N}$ s.t. $n \geq d$ and $n \geq w$, all $(\mathsf{e}_{\mathsf{S}}, \mathsf{e}_1, \ldots, \mathsf{e}_n) \leftarrow \mathsf{Gen}(n, d, w)$, all $\mathsf{m} \in \mathcal{M}$, and all $\mathcal{D} \subset \mathcal{R}$ s.t. $|\mathcal{D}| = d$, the following holds with probability at least δ:

$$\begin{cases} \mathsf{Ver}(\mathsf{e}_i, \mathsf{m}, \mathsf{Auth}(\mathsf{e}_{\mathsf{S}}, \mathsf{m}, \mathcal{D})) \rightarrow \mathtt{true} & \text{for every } \mathsf{R}_i \in \mathcal{D}, \\ \mathsf{Ver}(\mathsf{e}_i, \mathsf{m}, \mathsf{Auth}(\mathsf{e}_{\mathsf{S}}, \mathsf{m}, \mathcal{D})) \rightarrow \mathtt{false} & \text{for every } \mathsf{R}_i \notin \mathcal{D}. \end{cases}$$

2.2 Security Definitions

We consider security against impersonation attacks and substitution attacks as in the traditional A-codes [3] and MRA-codes [11], [13], [14]. In addition, we also consider *anonymity* as an additional security notion. We consider the anonymity notion as in ABA [23]. Anonymity guarantees that no information on (non-)designated receivers is leaked from an authenticator.

For simple description, we use the following notation: for any $\mathcal{X} = \{\mathsf{R}_{l_1}, \mathsf{R}_{l_2}, \ldots, \mathsf{R}_{l_\ell}\} \subset \mathcal{R}$, we define $\mathsf{e}_{\mathcal{X}} \coloneqq (\mathsf{e}_{l_1}, \mathsf{e}_{l_2}, \ldots, \mathsf{e}_{l_\ell}) \in \mathcal{E}_{\mathcal{X}}$, where $\mathcal{E}_{\mathcal{X}} \coloneqq \mathcal{E}_{l_1} \times \mathcal{E}_{l_2} \times \cdots \times \mathcal{E}_{l_\ell}$.

(d, w, ε)-security. We consider security against impersonation and substitution attacks.

Definition 3 ((d, w, ε)-security). Let Π be an MDRA-code in the one-time model. Π said to be (d, w, ε)-secure if it holds $\max\{P_{\mathsf{Imp}}, P_{\mathsf{Sub}}\} \leq \varepsilon$, where P_{Imp} and P_{Sub} are the success probabilities of the impersonation and substitution attacks, which are defined as follows.

Impersonation attacks. An adversary with at most w corrupted receivers tries to generate a fraudulent pair of a message m and an authenticator $\tau_{\mathcal{D}}$ for an arbitrary subset $\mathcal{D}$ of receivers so that some receiver $\mathsf{R}_i \in \mathcal{D} \setminus \mathcal{W}$ accepts the pair. For any $\mathcal{D} \subset \mathcal{R}$ such that $|\mathcal{D}| = d$, any $\mathcal{W} \subset \mathcal{R}$ such that $|\mathcal{W}| \leq w$, and any $\mathsf{R}_i \in \mathcal{D} \setminus \mathcal{W}$, the success probability of the impersonation attacks for $(\mathcal{D}, \mathcal{W}, i)$ denoted by $P_{\mathsf{Imp}}(\mathcal{D}, \mathcal{W}, i)$ is defined as

$$P_{\mathsf{Imp}}(\mathcal{D}, \mathcal{W}, i) \coloneqq \max_{(\mathsf{m}, \tau_{\mathcal{D}}) \in \mathcal{M} \times \mathcal{T}} \max_{\mathsf{e}_{\mathcal{W}} \in \mathcal{E}_{\mathcal{W}}} \Pr_{\mathsf{e}_i} \left\{ \mathsf{Ver}(\mathsf{e}_i, \mathsf{m}, \tau_{\mathcal{D}}) \neq \mathtt{false} \mid \mathsf{e}_{\mathcal{W}} \right\}.$$

We define $P_{\mathsf{Imp}} \coloneqq \max_{(\mathcal{D}, \mathcal{W}, i)} P_{\mathsf{Imp}}(\mathcal{D}, \mathcal{W}, i)$.

Substitution attacks. After observing a message m and an honestly-generated authenticator $\tau_{\mathcal{D}}$ for $\mathcal{D} \subset R$, an adversary with at most w corrupted receivers tries to generate a fraudulent pair of a message m' such that $\mathsf{m}' \neq \mathsf{m}$ and an authenticator $\tau'_{\mathcal{D}'}$ for an arbitrary subset $\mathcal{D}'$ of receivers so that some receiver $\mathsf{R}_i \in \mathcal{D}' \setminus \mathcal{W}$ accepts the pair. For any $\mathcal{D}, \mathcal{D}' \subset \mathcal{R}$ such that $|\mathcal{D}| = |\mathcal{D}'| = d$, any $\mathcal{W} \subset \mathcal{R}$ such that $|\mathcal{W}| \leq w$, and any $\mathsf{R}_i \in \mathcal{D}' \setminus \mathcal{W}$, the success probability of the substitution attacks for $(\mathcal{D}, \mathcal{D}', \mathcal{W}, i)$ denoted by $P_{\mathsf{Sub}}(\mathcal{D}, \mathcal{D}', \mathcal{W}, i)$ is defined as

$$P_{\mathsf{Sub}}(\mathcal{D}, \mathcal{D}', \mathcal{W}, i) \coloneqq \max_{(\mathsf{m}, \tau_{\mathcal{D}}) \in \mathcal{M} \times \mathcal{T}} \max_{\substack{(\mathsf{m}', \tau'_{\mathcal{D}'}) \in \mathcal{M} \times \mathcal{T} \\ \text{s.t. } (\mathsf{m}', \tau'_{\mathcal{D}'}) \neq (\mathsf{m}, \tau_{\mathcal{D}})}} \max_{\mathsf{e}_{\mathcal{W}} \in \mathcal{E}_{\mathcal{W}}} \Pr_{\mathsf{e}_i} \left\{ \mathsf{Ver}(\mathsf{e}_i, \mathsf{m}', \tau'_{\mathcal{D}'}) \neq \mathtt{false} \mid (\mathsf{m}, \tau_{\mathcal{D}}), \mathsf{e}_{\mathcal{W}} \right\}.$$

We define $P_{\mathsf{Sub}} \coloneqq \max_{(\mathcal{D}, \mathcal{D}', \mathcal{W}, i)} P_{\mathsf{Sub}}(\mathcal{D}, \mathcal{D}', \mathcal{W}, i)$.

Remark 1 (On the consistency property). We also consider a notion of *consistency*, which guarantees that if any designated receiver accepts an authenticator, then all of them do. We believe that this notion is important in terms of system management; thanks to consistency, S can easily confirm an authenticator has been successfully delivered by communicating only with one of designated receivers. Indeed, a similar notion has been considered in [32] in the context of (computationally secure) MDVS. Although we separately

defined (d, w, ε)-security and consistency in the conference version [1], the above (d, w, ε)-security (Def. 3) actually implies consistency; $\max\{P_{\mathsf{Imp}}, P_{\mathsf{Sub}}\} \leq \varepsilon$ means that an adversary cannot create any pair of a message and a fraudulent authenticator such that at least one receiver in $\mathcal{D}$ accepts it with probability more than ε. Therefore, (d, w, ε)-security guarantees that no honest receivers accept the forged pair (with probability more than ε) and so all of them reject it. Besides, the correctness property (Def. 2) guarantees that all honest receivers accepts an honestly-generated authenticator. For the above reason, we omit the consistency definition in this paper.

Anonymity. We also consider *anonymity*, meaning that an authenticator leaks no useful information on (non-)designated receivers. Namely, an adversary cannot get any information on which receivers (except for corrupted ones) are designated. Since the information on which receivers are designated may be sensitive one [30] (also see our motivating scenario in Sect. 1.3), we should consider anonymity. For instance, if a message is for receivers who have a certain privilege, such information on (non-)designated receivers should be treated as sensitive one.

Definition 4 (Anonymity). Let Π be an (d, w, ε)-secure MDRA-code in the one-time model. Π said to be anonymous if it satisfies the following property.

Anonymity. For any designated set $\mathcal{D} \subset \mathcal{R}$ such that $|\mathcal{D}| = d$ and any corrupted-receiver set $\mathcal{W} \subset \mathcal{R}$ such that $|\mathcal{W}| \leq w$, $\tau_{\mathcal{D}}$ leaks no information on $\mathcal{D} \setminus \mathcal{W}$ more than the sizes of the intersection of the designated and corrupted sets.

For any $\mathcal{W} \subset \mathcal{R}$ such that $|\mathcal{W}| \leq w$, any $(\mathsf{m}, \tau_{\mathcal{D}}) \in \mathcal{M} \times \mathcal{T}$, and any $\mathsf{e}_{\mathcal{W}} \in \mathcal{E}_{\mathcal{W}}$, it holds that

$$\Pr_{\substack{\mathcal{D} \text{ s.t.} \\ |\mathcal{D}|=d}} \{\mathcal{D} \setminus \mathcal{W} \mid (\mathsf{m}, \tau_{\mathcal{D}}), \mathsf{e}_{\mathcal{W}}\} = \Pr_{\substack{\mathcal{D} \text{ s.t.} \\ |\mathcal{D}|=d}} \{\mathcal{D} \setminus \mathcal{W}\}.$$

2.3 Discussion

On the range of designated-receiver sets. One may wonder why the above model focuses on the designated-receiver set $\mathcal{D}$ whose cardinality is exactly d, instead of flexible one (i.e., $|\mathcal{D}| \leq d$ or $|\mathcal{D}| \leq n$). In this work, we consider the simpler case, i.e., $|\mathcal{D}| = d$, since we follow previous research strategies on unconditionally secure BE [19] and key predistribution systems (KPS) [33]–[35], which can be seen as encryption and key-agreement variants of MDRA-codes, respectively. They are classified into two types: (t, ω)-secure and $(\leq n, \omega)$-secure ones. For instance, in (t, ω)-secure BE [20], [21], [36], [37], a sender can designate exact t receivers who can decrypt ciphertexts, while $(\leq n, \omega)$-secure BE [19], [38], [39] allows the sender to designate any subset of the receiver set. It is obvious that (t, ω)-secure schemes are easier to analyze than $(\leq n, \omega)$-secure ones since the latter can be realized a simple combination of (t, ω)-secure schemes for all $t \in [n]$[†]. Therefore, we began with (d, w, ε)-secure MDRA-codes, and leave an extension to $(\leq n, w, \varepsilon)$-secure schemes as an open problem.

On δ-correctness. Traditional A-codes and MRA-codes require perfect correctness; receivers accept any pair of a message and a correctly-generated authenticator with probability one (see Defs. 6 and 9 for detailed definitions). In this work, we require δ-correctness (Def. 2) for MDRA-codes, which holds with at least probability δ that all designated receivers accept any pair of a message and correctly-generated authenticator and all non-designated receivers reject the pair. Since it requires "correct rejection," we defined the correctness in a relaxed form. This relaxation stems from the intuition that adversary's success probability of forging authenticators in (MR)A-codes cannot be zero; there are at least one correct authenticator in the authenticator space and therefore a random guess works (with small probability). Namely, depending on MDRA-code constructions, a (correctly-generated) authenticator that some designated receiver accepts might also be accepted by some non-designated receiver. On the other hand, the correctness of MRA-codes guarantees that all receivers accept a correctly-generated authenticator. In that sense, the correctness for MDRA-codes seems more difficult to achieve than that for MRA-codes (and traditional A-codes). Indeed, our generic construction in Sect. 3.1 meets δ-correctness with $\delta < 1$, while our direct construction in Sect. 3.2 satisfies 1-correctness.

3. Constructions

In this section, we show two constructions of MDRA-codes. The first one is a simple generic construction from A-codes and MRA-codes, and the second one is a more efficient direct construction over finite fields.

3.1 Simple Generic Construction

We show a simple construction of an n-party MDRA-code from any two-party A-codes [3] and any n-party MRA-code [11]. To do so, we define A-codes and MRA-codes below.

A-codes [3]. We describe a syntax and security definition of A-codes.

Definition 5 (A-codes). An A-code $\Phi := (\mathsf{Setup}, \mathsf{Tag}, \mathsf{Vrfy})$ with three entities TA, S, and R and three finite spaces $\widetilde{\mathcal{M}}$, $\widetilde{\mathcal{K}}, \widetilde{\mathcal{T}}$ is defined as follows.

Entities. TA is a trusted authority that generates secret keys and securely distributes them to all other entities. S is a sender and R is a receiver.

Spaces. $\widetilde{\mathcal{M}}$, $\widetilde{\mathcal{K}}$, and $\widetilde{\mathcal{T}}$ are finite sets of messages, secret keys, and tags (or authenticators). They may be determined when Setup is executed.

Algorithms.

1. $\mathsf{k} \leftarrow \mathsf{Setup}()$: It is a probabilistic algorithm for setup and run by TA. It outputs a secret key k.

[†]Of course, this trivial construction may be redundant.

2. $\mathsf{tag} \leftarrow \mathsf{Tag}(\mathsf{k}, \mathsf{m})$: It is an algorithm for authenticator generation and run by S. It takes the secret key k and a message $\mathsf{m} \in \widetilde{\mathcal{M}}$ as input, and outputs an authenticator $\mathsf{tag} \in \widetilde{\mathcal{T}}$.

3. $\mathtt{ans} \leftarrow \mathsf{Vrfy}(\mathsf{k}, \mathsf{m}, \mathsf{tag})$: It is a deterministic algorithm for verification and run by R. It takes the secret key k, a message m, and an authenticator tag as input, and outputs $\mathtt{ans} \in \{\mathtt{true}, \mathtt{false}\}$, where `true` and `false` indicate 'accept' and 'reject,' respectively.

Definition 6 (Correctness of A-codes). For all $\mathsf{k} \leftarrow \mathsf{Setup}()$ and all $\mathsf{m} \in \widetilde{\mathcal{M}}$, it holds

$$\mathtt{true} \leftarrow \mathsf{Vrfy}(\mathsf{k}, \mathsf{m}, \mathsf{Tag}(\mathsf{k}, \mathsf{m})).$$

Definition 7 (Security of A-codes). Let Φ be an A-code in the one-time model. Φ said to be η-secure if it holds $\max\{\widetilde{P}_{\mathsf{Imp}}, \widetilde{P}_{\mathsf{Sub}}\} \leq \eta$, where $\widetilde{P}_{\mathsf{Imp}}$ and $\widetilde{P}_{\mathsf{Sub}}$ are the success probabilities of the attacks, which are defined as follows.

Impersonation attacks. The success probability of the impersonation attacks $\widetilde{P}_{\mathsf{Imp}}$ is defined as

$$\widetilde{P}_{\mathsf{Imp}} := \max_{(\mathsf{m},\mathsf{tag}) \in \widetilde{\mathcal{M}} \times \widetilde{\mathcal{T}}} \Pr_{\mathsf{k}}\{\mathsf{Vrfy}(\mathsf{k}, \mathsf{m}, \mathsf{tag}) \rightarrow \mathtt{true}\}.$$

Substitution attacks. The success probability of the substitution attacks denoted by $\widetilde{P}_{\mathsf{Sub}}$ is defined as

$$\widetilde{P}_{\mathsf{Sub}} := \max_{(\mathsf{m},\mathsf{tag}) \in \widetilde{\mathcal{M}} \times \widetilde{\mathcal{T}}} \max_{\substack{(\mathsf{m}',\mathsf{tag}') \in \widetilde{\mathcal{M}} \times \widetilde{\mathcal{T}} \\ \text{s.t. } (\mathsf{m}',\mathsf{tag}') \neq (\mathsf{m},\mathsf{tag})}} \Pr_{\mathsf{k}}\{\mathsf{Vrfy}(\mathsf{k}, \mathsf{m}', \mathsf{tag}') \rightarrow \mathtt{true} \mid (\mathsf{m}, \mathsf{tag})\}.$$

MRA-codes [11]. We describe a syntax and security definition of MRA-codes.

Definition 8 (MRA-codes). An MRA-code $\Psi := (\mathsf{MRGen}, \mathsf{MRAuth}, \mathsf{MRVer})$ with $n+2$ entities, TA, S, $\mathcal{R} = \{\mathsf{R}_1, \ldots, \mathsf{R}_n\}$ and three finite spaces $\widehat{\mathcal{M}}, \widehat{\mathcal{E}}, \widehat{\mathcal{T}}$ is defined as follows.

Entities. We consider the same entities as MDRA-codes, and so omit the details.

Spaces. $\widehat{\mathcal{T}}$, $\widehat{\mathcal{E}}$, and $\widehat{\mathcal{T}}$ are finite sets of messages, secret keys, and tags (or authenticators). More specifically, let $\widehat{\mathcal{E}}_{\mathsf{S}}$ and $\widehat{\mathcal{E}}_i$ ($i \in [n]$) be secret-key sets for S and R_i, respectively, and we define $\widehat{\mathcal{E}} := \widehat{\mathcal{E}}_{\mathsf{S}} \times \widehat{\mathcal{E}}_1 \times \cdots \times \widehat{\mathcal{E}}_n$. They may be determined when MRGen is executed.

Algorithms.

1. $(\widehat{\mathsf{e}}_{\mathsf{S}}, \widehat{\mathsf{e}}_1, \ldots, \widehat{\mathsf{e}}_n) \leftarrow \mathsf{MRGen}(n, w)$: It is a probabilistic algorithm for setup and run by TA. It takes the number of receivers n and the maximum number of receivers w that Ψ allows an adversary to corrupt as input, and outputs secret keys $(\widehat{\mathsf{e}}_{\mathsf{S}}, \widehat{\mathsf{e}}_1, \ldots, \widehat{\mathsf{e}}_n) \in \widehat{\mathcal{E}}$, where $\widehat{\mathsf{e}}_{\mathsf{S}}$ and $\widehat{\mathsf{e}}_i$ are secret keys for S and R_i ($i \in [n]$), respectively.

2. $\widehat{\tau} \leftarrow \mathsf{MRAuth}(\widehat{\mathsf{e}}_{\mathsf{S}}, \mathsf{m})$: It is an algorithm for authenticator generation and run by S. It takes the secret key $\widehat{\mathsf{e}}_{\mathsf{S}}$ and a message $\mathsf{m} \in \widehat{\mathcal{M}}$ as input, and outputs an authenticator $\widehat{\tau} \in \widehat{\mathcal{T}}$.

3. $\mathtt{ans} \leftarrow \mathsf{MRVer}(\widehat{\mathsf{e}}_i, \mathsf{m}, \widehat{\tau})$: It is a deterministic algorithm for verification and run by R_i. It takes the secret key $\widehat{\mathsf{e}}_i$, a message m, and an authenticator $\widehat{\tau}$ as input, and outputs $\mathtt{ans} \in \{\mathtt{true}, \mathtt{false}\}$, where `true` and `false` indicate 'accept' and 'reject,' respectively.

Definition 9 (Correctness of MRA-codes). For all $n, w \in \mathbb{N}$ s.t. $n \geq w$, all $(\widehat{\mathsf{e}}_{\mathsf{S}}, \widehat{\mathsf{e}}_1, \ldots, \widehat{\mathsf{e}}_n) \leftarrow \mathsf{MRGen}(n, w)$, all $\mathsf{m} \in \widehat{\mathcal{M}}$, and for all $i \in [n]$ it holds

$$\mathtt{true} \leftarrow \mathsf{MRVer}(\widehat{\mathsf{e}}_i, \mathsf{m}, \mathsf{MRAuth}(\widehat{\mathsf{e}}_{\mathsf{S}}, \mathsf{m})).$$

Definition 10 (Security of MRA-codes). Let Ψ be an MRA-code in the one-time model. Ψ said to be (w, μ)-secure if it holds $\max\{\widehat{P}_{\mathsf{Imp}}, \widehat{P}_{\mathsf{Sub}}\} \leq \mu$, where $\widehat{P}_{\mathsf{Imp}}$ and $\widehat{P}_{\mathsf{Sub}}$ are the success probabilities of the attacks, which are defined as follows.

Impersonation attacks. For any $\mathcal{W} \subset \mathcal{R}$ such that $|\mathcal{W}| \leq w$ and any $\mathsf{R}_i \in \mathcal{R} \setminus \mathcal{W}$, the success probability of the impersonation attacks for $(\mathcal{W}, i)$ denoted by $\widehat{P}_{\mathsf{Imp}}(\mathcal{W}, i)$ is defined as

$$\widehat{P}_{\mathsf{Imp}}(\mathcal{W}, i) := \max_{(\mathsf{m},\widehat{\tau}) \in \widehat{\mathcal{M}} \times \widehat{\mathcal{T}}} \max_{\widehat{\mathsf{e}}_{\mathcal{W}} \in \widehat{\mathcal{E}}_{\mathcal{W}}} \Pr_{\widehat{\mathsf{e}}_i}\{\mathsf{MRVer}(\widehat{\mathsf{e}}_i, \mathsf{m}, \widehat{\tau}) \rightarrow \mathtt{true} \mid \widehat{\mathsf{e}}_{\mathcal{W}}\}.$$

We define $\widehat{P}_{\mathsf{Imp}} := \max_{(\mathcal{W},i)} \widehat{P}_{\mathsf{Imp}}(\mathcal{W}, i)$.

Substitution attacks. For any $\mathcal{W} \subset \mathcal{R}$ such that $|\mathcal{W}| \leq w$, and any $\mathsf{R}_i \in \mathcal{R} \setminus \mathcal{W}$, the success probability of the substitution attacks for $(\mathcal{W}, i)$ denoted by $\widehat{P}_{\mathsf{Sub}}(\mathcal{W}, i)$ is defined as

$$\widehat{P}_{\mathsf{Sub}}(\mathcal{W}, i) := \max_{(\mathsf{m},\widehat{\tau}) \in \widehat{\mathcal{M}} \times \widehat{\mathcal{T}}} \max_{\substack{(\widehat{\tau}') \in \widehat{\mathcal{M}} \times \widehat{\mathcal{T}} \\ \text{s.t. } (\mathsf{m}',\widehat{\tau}') \neq (\mathsf{m},\widehat{\tau})}} \max_{\widehat{\mathsf{e}}_{\mathcal{W}} \in \widehat{\mathcal{E}}_{\mathcal{W}}} \Pr_{\widehat{\mathsf{e}}_i}\{\mathsf{MRVer}(\widehat{\mathsf{e}}_i, \mathsf{m}', \widehat{\tau}') \rightarrow \mathtt{true} \mid (\mathsf{m}, \widehat{\tau}), \widehat{\mathsf{e}}_{\mathcal{W}}\}.$$

We define $\widehat{P}_{\mathsf{Sub}} := \max_{(\mathcal{W},i)} \widehat{P}_{\mathsf{Sub}}(\mathcal{W}, i)$.

Now we are ready to show our simple construction of an MDRA-code $\Pi = (\mathsf{Gen}, \mathsf{Auth}, \mathsf{Ver})$ from any A-code $\Phi = (\mathsf{Setup}, \mathsf{Tag}, \mathsf{Vrfy})$ and any MRA-code $\Psi = (\mathsf{MRGen}, \mathsf{MRAuth}, \mathsf{MRVer})$. Note that our construction requires both of A-codes and MRA-codes as building blocks and enables one to set any $d \in [n]$ and any $w \in [n-1]$.

$\mathsf{Gen}(n, d, w)$. Run Setup n times to get n secret keys $\mathsf{k}_1, \ldots, \mathsf{k}_n$. Run MRGen to obtain $(\widehat{\mathsf{e}}_{\mathsf{S}}, \widehat{\mathsf{e}}_1, \ldots, \widehat{\mathsf{e}}_n)$. Output $\mathsf{e}_{\mathsf{S}} := (\mathsf{k}_1, \ldots, \mathsf{k}_n, \widehat{\mathsf{e}}_{\mathsf{S}})$ and $\mathsf{e}_i := (\mathsf{k}_i, \widehat{\mathsf{e}}_i)$.

$\mathsf{Auth}(\mathsf{e}_{\mathsf{S}}, \mathsf{m}, \mathcal{D})$. Parse $\mathsf{e}_{\mathsf{S}} = (\mathsf{k}_1, \ldots, \mathsf{k}_n, \widehat{\mathsf{e}}_{\mathsf{S}})$. Suppose $\mathcal{D} = \{\mathsf{R}_{i_1}, \ldots, \mathsf{R}_{i_d}\}$. For every $j \in [d]$, run $\mathsf{Tag}(\mathsf{k}_{i_j}, \mathsf{m})$ and get tag_{i_j}. Run $\mathsf{MRAuth}(\widehat{\mathsf{e}}_{\mathsf{S}}, (\mathsf{m}, \mathsf{tag}_{\sigma(i_1)}, \ldots, \mathsf{tag}_{\sigma(i_d)}))$ to compute $\widehat{\tau}$, where $\sigma : [d] \rightarrow [d]$ is a random permutation. Output $\tau_{\mathcal{D}} := (\mathsf{tag}_{\sigma(i_1)}, \ldots, \mathsf{tag}_{\sigma(i_d)}, \widehat{\tau})$.

$\mathsf{Ver}(\mathsf{e}_i, \mathsf{m}, \tau_{\mathcal{D}})$. Parse $\mathsf{e}_i = (\mathsf{k}_i, \widehat{\mathsf{e}}_i)$ and $\tau_{\mathcal{D}} = (\mathsf{tag}_{l_1}, \ldots, \mathsf{tag}_{l_d}, \widehat{\tau})$, respectively. Run $\mathsf{MRVer}(\widehat{\mathsf{e}}_i, (\mathsf{m}, \mathsf{tag}_{l_1}, \ldots, \mathsf{tag}_{l_d}), \widehat{\tau})$. If the output is `false`, output `false`; otherwise, run $\mathsf{Vrfy}(\mathsf{k}_i, \mathsf{m}, \mathsf{tag}_{l_j})$ for every $j \in [d]$. If there exists at least one index j such that $\mathtt{true} \leftarrow \mathsf{Vrfy}(\mathsf{k}_i, \mathsf{m}, \mathsf{tag}_{l_j})$, output `true`; otherwise, output `false`.

Theorem 1. If the underlying A-code Φ is η-secure, the underlying MRA-code Ψ is (w, μ)-secure, and σ is a random permutation, an MDRA-code Π constructed above meets δ-correctness, (d, w, ε)-security, and anonymity, where $\delta \geq 1 - d(n-d)\eta$, $w \leq n-1$, and $\varepsilon \leq d \cdot \mu \cdot \eta$.

Proof. We show the above scheme satisfies δ-correctness, (d, w, ε)-security, and anonymity.

δ-correctness. First, $\mathsf{MRVer}(\widehat{\mathsf{e}}_i, (\mathsf{m}, \mathsf{tag}_{l_1}, \ldots, \mathsf{tag}_{l_d}), \widehat{\tau})$ outputs `true` due to the correctness property of the underlying MRA-code. It is obvious that every designated receiver $\mathsf{R}_i \in \mathcal{D}$ can obtain at least one $\mathtt{true} \leftarrow \mathsf{Vrfy}(\mathsf{k}_i, \mathsf{m}, \mathsf{tag}_{l_\ell})$ due to the correctness property of the underlying A-code. On the other hand, every non-designated receiver $\mathsf{R}_j \notin \mathcal{D}$ might obtain `true` since Vrfy might output `true` for invalid A-code authenticators. For any $\mathcal{D} \subset \mathcal{R}$ such that $|\mathcal{D}| = d$, the probability $P'(\mathcal{D})$ that at least one non-designated receiver gets at least one `true` is

$$
\begin{aligned}
&P'(\mathcal{D}) \\
&\leq \max_{(\mathsf{m}, \mathsf{tag}_{l_1}, \ldots, \mathsf{tag}_{l_d})} \\
&\quad \Pr_{\{\mathsf{k}_j\}_{\mathsf{R}_j \in \mathcal{R} \setminus \mathcal{D}}} \left\{ \bigvee_{\mathsf{R}_j \in \mathcal{R} \setminus \mathcal{D}} \left(\bigvee_{\ell \in [d]} \mathsf{Vrfy}(\mathsf{k}_j, \mathsf{m}, \mathsf{tag}_{l_\ell}) \rightarrow \mathtt{true} \right) \right\} \\
&\leq \max_{(\mathsf{m}, \mathsf{tag}_{l_1}, \ldots, \mathsf{tag}_{l_d})} \\
&\quad \sum_{\mathsf{R}_j \in \mathcal{R} \setminus \mathcal{D}} \Pr_{\mathsf{k}_j} \left\{ \bigvee_{\ell \in [d]} \left(\mathsf{Vrfy}(\mathsf{k}_j, \mathsf{m}, \mathsf{tag}_{l_\ell}) \rightarrow \mathtt{true} \right) \right\} \qquad (1) \\
&\leq \max_{(\mathsf{m}, \mathsf{tag}_{l_1}, \ldots, \mathsf{tag}_{l_d})} \\
&\quad \sum_{\mathsf{R}_j \in \mathcal{R} \setminus \mathcal{D}} \sum_{\ell \in [d]} \Pr_{\mathsf{k}_j} \left\{ \mathsf{Vrfy}(\mathsf{k}_j, \mathsf{m}, \mathsf{tag}_{l_\ell}) \rightarrow \mathtt{true} \right\} \qquad (2) \\
&\leq \sum_{\mathsf{R}_j \in \mathcal{R} \setminus \mathcal{D}} \sum_{\ell \in [d]} \max_{(\mathsf{m}, \mathsf{tag}_{l_\ell})} \Pr_{\mathsf{k}_j} \left\{ \mathsf{Vrfy}(\mathsf{k}_j, \mathsf{m}, \mathsf{tag}_{l_\ell}) \rightarrow \mathtt{true} \right\} \\
&\leq d(n-d)\eta,
\end{aligned}
$$

where Eqs. (1) and (2) follow from the union bound and the last inequality follows from η-security of the underlying A-code.

Since the above holds for any $\mathcal{D}$ such that $|\mathcal{D}| = d$, we have $\delta \geq 1 - P'(\mathcal{D}) \geq 1 - d(n-d)\eta$.

(d, w, ε)-security. First, we show the above construction is secure against impersonation attacks. Since each k_i is independent of each other, the corresponding tags tag_i is also independent of each other. Therefore, due to η-security of the A-code, an adversary who has at most w A-code keys $\mathsf{k}_{l_1}, \ldots, \mathsf{k}_{l_w}$ cannot compute a valid authenticator tag_i for any honest receiver R_i. Moreover, due to (w, μ)-security of the MRA-code, it is difficult to create a valid authenticator $\widehat{\tau}$ even if the adversary has at most w MRA-code secret keys $\widehat{\mathsf{e}}_{l_1}, \ldots, \widehat{\mathsf{e}}_{l_w}$.

To show the proof as simple as possible, we use the following notations. For any $\mathcal{X} = \{\mathsf{R}_{l_1}, \mathsf{R}_{l_2}, \ldots, \mathsf{R}_{l_\ell}\} \subset \mathcal{R}$, we define $\widehat{\mathsf{e}}_{\mathcal{X}} := (\widehat{\mathsf{e}}_{l_1}, \widehat{\mathsf{e}}_{l_2}, \ldots, \widehat{\mathsf{e}}_{\ell}) \in \widehat{\mathcal{E}}_{\mathcal{X}}$ and $\mathsf{k}_{\mathcal{X}} := (\mathsf{k}_{l_1}, \mathsf{k}_{l_2}, \ldots, \mathsf{k}_{\ell}) \in \widetilde{\mathcal{K}}_{\mathcal{X}}$, where $\widehat{\mathcal{E}}_{\mathcal{X}} := \widehat{\mathcal{E}}_{l_1} \times \widehat{\mathcal{E}}_{l_2} \times \cdots \times \widehat{\mathcal{E}}_{l_\ell}$ and $\widetilde{\mathcal{K}}_{\mathcal{X}} := \widetilde{\mathcal{K}}_{l_1} \times \widetilde{\mathcal{K}}_{l_2} \times \cdots \times \widetilde{\mathcal{K}}_{l_\ell}$, respectively. Let $\widehat{\mathsf{m}} := (\mathsf{m}, \mathsf{tag}_1, \ldots, \mathsf{tag}_d)$.

Now we are ready to show the proof. Let $\mathsf{Suc}_{i,j}$ be an event that for any fixed $\mathcal{D}, \mathcal{W} \subset \mathcal{R}$, an honest receiver $\mathsf{R}_i \in \mathcal{D} \setminus \mathcal{W}$ gets $\mathsf{Vrfy}(\mathsf{k}_i, \mathsf{m}, \mathsf{tag}_j) = \mathtt{true}$ for some $\mathsf{R}_j \in \mathcal{D}$. For any $\mathcal{D} \subset \mathcal{R}$ s.t. $|\mathcal{D}| = d$, any $\mathcal{W} \subset \mathcal{R}$ s.t. $|\mathcal{W}| \leq n-1$, and any $\mathsf{R}_i \in \mathcal{D} \setminus \mathcal{W}$, we have

$$
\begin{aligned}
&P_{\mathsf{Imp}}(\mathcal{D}, \mathcal{W}, i) \\
&= \max_{(\mathsf{m}, \tau_{\mathcal{D}}) \in \mathcal{M} \times \mathcal{T}} \max_{\mathsf{e}_{\mathcal{W}} \in \mathcal{E}_{\mathcal{W}}} \\
&\quad \Pr_{\widehat{\mathsf{e}}_i, \mathsf{k}_i} \left\{ \mathsf{MRVer}(\widehat{\mathsf{e}}_i, \widehat{\mathsf{m}}, \widehat{\tau}) = \mathtt{true} \wedge \mathsf{Suc}_{i,j} \mid \mathsf{e}_{\mathcal{W}} \right\} \\
&= \max_{(\mathsf{m}, \tau_{\mathcal{D}}) \in \mathcal{M} \times \mathcal{T}} \max_{(\mathsf{k}_{\mathcal{W}}, \widehat{\mathsf{e}}_{\mathcal{W}}) \in \widetilde{\mathcal{K}}_{\mathcal{W}} \times \widehat{\mathcal{E}}_{\mathcal{W}}} \\
&\quad \Pr_{\widehat{\mathsf{e}}_i} \left\{ \mathsf{MRVer}(\widehat{\mathsf{e}}_i, \widehat{\mathsf{m}}, \widehat{\tau}) = \mathtt{true} \mid \widehat{\mathsf{e}}_{\mathcal{W}} \right\} \\
&\qquad\qquad \cdot \Pr_{\mathsf{k}_i} \left\{ \mathsf{Suc}_{i,j} \mid \mathsf{k}_{\mathcal{W}} \right\}, \qquad (3) \\
&\leq \max_{(\mathsf{m}, \tau_{\mathcal{D}}) \in \mathcal{M} \times \mathcal{T}} \max_{(\mathsf{k}_{\mathcal{W}}, \widehat{\mathsf{e}}_{\mathcal{W}}) \in \widetilde{\mathcal{K}}_{\mathcal{W}} \times \widehat{\mathcal{E}}_{\mathcal{W}}} \\
&\quad \Pr_{\widehat{\mathsf{e}}_i} \left\{ \mathsf{MRVer}(\widehat{\mathsf{e}}_i, \widehat{\mathsf{m}}, \widehat{\tau}) = \mathtt{true} \mid \widehat{\mathsf{e}}_{\mathcal{W}} \right\} \\
&\qquad \cdot \sum_{\mathsf{R}_j \in \mathcal{D}} \Pr_{\mathsf{k}_i} \left\{ \mathsf{Vrfy}(\mathsf{k}_i, \mathsf{m}, \mathsf{tag}_j) = \mathtt{true} \mid \mathsf{k}_{\mathcal{W}} \right\}, \qquad (4) \\
&\leq d \cdot \mu \cdot \eta,
\end{aligned}
$$

where Eqs. (3) and (4) follow from independence of secret keys and the union bound, and the last inequality follows from η-security of the underlying A-code and (w, μ)-security of the underlying MRA-code. Therefore, we have

$$
P_{\mathsf{Imp}} = \max_{(\mathcal{D}, \mathcal{W}, i)} P_{\mathsf{Imp}}(\mathcal{D}, \mathcal{W}, i) \leq d \cdot \mu \cdot \eta.
$$

We can show security against substitution attacks in a similar way.

Anonymity. It is clear that each secret key k_i is randomly generated by Setup and hence independent of receivers' identities. It is inherited by A-code authenticators tag_i. Moreover, the order of authenticators of the underlying A-code in $\tau_{\mathcal{D}}$ is randomized by the random permutation σ. Therefore, the adversary obtains no information on $\mathcal{D}$ from $\widehat{\tau}$, which is an MRA-code authenticator for $(\mathsf{m}, \mathsf{tag}_{\sigma(i_1)}, \ldots, \mathsf{tag}_{\sigma(i_d)})$. Note that MRA-code secret keys $\widehat{\mathsf{e}}_1, \ldots, \widehat{\mathsf{e}}_n$ are generated before designating $\mathcal{D}$, and hence they include no information on $\mathcal{D}$. Thus, our construction obviously satisfies anonymity. □

3.2 Efficient Direct Construction

Though the generic construction in the previous section is simple, the size of S's secret key e_S depends on the number of all receivers, i.e., $O(n)$. In this section, we propose a more efficient construction of an MDRA-code over finite fields. Specifically, the second construction achieves the size $O(\max\{n-d, w\})$ of S's secret key (see the next section for the detailed efficiency comparison).

Formally, our second construction of an MDRA-code $\Pi = (\mathsf{Gen}, \mathsf{Auth}, \mathsf{Ver})$ is given as follows.

$\mathsf{Gen}(n, d, w)$. Let $\lambda := n - d$, and let $\mathbb{F}_q$ be a finite field, where q is the power of prime such that $q \geq n$. Assume that $[n] \subset \mathbb{F}_q$, i.e., every $i \in [n]$ is appropriately encoded into an element of $\mathbb{F}_q$. Randomly choose the following polynomials:

$$C(x) := \sum_{i=0}^{w} a_i x^i \in \mathbb{F}_q[X],$$

$$G(x) := r + \sum_{i=1}^{\lambda} b_i x^i \in \mathbb{F}_q[X],$$

$$F_t(x, y) := \sum_{j=0}^{1} \left(\sum_{i=0}^{w} c_{i,j}^{(t)} x^i \right) y^j \in \mathbb{F}_q[X, Y] \text{ for } t \in \{0, 1\}.$$

Compute

$$\sigma(x, z) := F_0(x, r) + z \cdot F_1(x, r).$$

For all $i \in [n]$, set

$$v_i := C(i), \;\; \gamma_i := G(v_i), \;\; \sigma_i(y, z) := F_0(i, y) + z \cdot F_1(i, y).$$

Output $(\mathsf{e}_\mathsf{S}, \mathsf{e}_1, \ldots, \mathsf{e}_n)$, where

$$\mathsf{e}_\mathsf{S} := (C(x), G(x), \sigma(x, z)), \;\; \mathsf{e}_i := (\gamma_i, \sigma_i(y, z)) \text{ for } i \in [n].$$

$\mathsf{Auth}(\mathsf{e}_\mathsf{S}, \mathsf{m}, \mathcal{D})$. Parse e_S as $(C(x), G(x), \sigma(x, z))$. Compute

$$\widehat{\sigma}(x) := \sigma(x, \mathsf{m}), \;\; \Gamma := \{G(C(i_j)) \mid \mathsf{R}_{i_j} \in \mathcal{R} \setminus \mathcal{D})\}.$$

Output $\tau_\mathcal{D} := (\widehat{\sigma}(x), \Gamma)$.

$\mathsf{Ver}(\mathsf{e}_i, \mathsf{m}, \tau_\mathcal{D})$. Parse

$$\mathsf{e}_i = (\gamma_i, \sigma_i(y, z)), \;\; \tau_\mathcal{D} = (\widehat{\sigma}'(x), \Gamma'),$$

respectively. Output `false` if it holds that $\gamma_i \in \Gamma'$. Otherwise, reconstruct $G(x)$ from γ_i $(= G(v_i))$ and Γ' via Lagrange interpolation and output `true` if it holds that

$$\widehat{\sigma}'(i) = \sigma_i(G(0), \mathsf{m}).$$

Otherwise, output `false`.

Theorem 2. An MDRA-code Π constructed above meets δ-correctness, (d, w, ε)-security, and anonymity, where $\delta = 1$ and $\varepsilon = 1/q$.

Proof. We show the above scheme satisfies the correctness, (d, w, ε)-security, and anonymity.

δ-correctness. Suppose $\mathsf{R}_i \in \mathcal{D}$. Since we have

$$\widehat{\sigma}(i) = \sigma(i, \mathsf{m}) = F_0(i, r) + \mathsf{m} \cdot F_1(i, r),$$
$$\sigma_i(G(0), \mathsf{m}) = F_0(i, G(0)) + \mathsf{m} \cdot F_1(i, G(0)),$$

$\mathsf{Vrfy}(\mathsf{e}_i, \mathsf{m}, \tau_\mathcal{D})$ outputs `true` if it reconstructs $G(x)$ correctly. Since each receiver $\mathsf{R}_i \in \mathcal{D}$ can reconstruct $G(x)$ from their share $G(v_i)$ and $n - d$ shares from Γ, it is clear that R_i can reconstruct it. On the other hand, $G(v_j) \in \Gamma$ holds if $\mathsf{R}_j \notin \mathcal{D}$. Therefore, Vrfy outputs `false`. Hence, the proposed scheme satisfies δ-correctness, where $\delta = 1$.

(d, w, ε)-security. We describe the proof for security against substitution attacks, which implies the proof for security against impersonation attacks. Without loss of generality, we suppose w receivers $\mathcal{W} = \{\mathsf{R}_{\ell_1}, \ldots, \mathsf{R}_{\ell_w}\}$ are corrupted and t corrupted receivers are designated, say, $\mathcal{D} \cap \mathcal{W} = \{\mathsf{R}_{\ell_1}, \ldots, \mathsf{R}_{\ell_t}\}$. The adversary that corrupts $\mathcal{W}$ has $\{(\gamma_{\ell_j}, \sigma_{\ell_j}(y, z))\}_{j=1}^{w}$ and $\tau_\mathcal{D} = (\widehat{\sigma}(x), \Gamma = \{\gamma_j \mid \mathsf{R}_j \in \mathcal{R} \setminus \mathcal{D}\})$.

The adversary with $\mathcal{W}$ outputs $(\mathsf{m}', \tau'_{\mathcal{D}'})$ for $\mathcal{D}' \subset \mathcal{R}$ after observing $(\mathsf{m}, \tau_\mathcal{D})$, where $\tau'_{\mathcal{D}'} = (\widehat{\sigma}'(x), \Gamma')$ and $\tau_\mathcal{D} = (\widehat{\sigma}(x), \Gamma)$. $\mathcal{W}$ wins if it holds $\mathsf{Vrfy}(\mathsf{e}_{i^\star}, \mathsf{m}', \tau'_{\mathcal{D}'}) = \mathtt{true}$ for some $\mathsf{R}_{i^\star} \in \mathcal{D}' \setminus \mathcal{W}$. Here, we should consider two cases: $\mathcal{D} = \mathcal{D}'$ and $\mathcal{D} \neq \mathcal{D}'$. However, in the above setting, i,e., $\mathcal{D} \cap \mathcal{W} \neq \emptyset$, there are no differences between them since the adversary can reconstruct r in both cases and eventually get the same information from $\mathcal{W}$. Therefore, in the following, we assume $\mathcal{D} = \mathcal{D}'$ for simplicity.

Let us start the proof. The adversary tries to output $(\mathsf{m}', \tau'_\mathcal{D} = (\widehat{\sigma}'(x), \Gamma'))$ such that $(\mathsf{m}', \widehat{\sigma}'(x), \Gamma') \neq (\mathsf{m}, \widehat{\sigma}(x), \Gamma)$ and $\mathsf{Vrfy}(\mathsf{e}_{i^\star}, \mathsf{m}'(\widehat{\sigma}'(x), \Gamma')) \to \mathtt{true}$ for some $\mathsf{R}_{i^\star} \in \mathcal{D} \setminus \mathcal{W}$.

As described above, the adversary knows $\tau_\mathcal{D} = (\widehat{\sigma}(x), \Gamma)$, which is broadcast to all receivers, where

$$\begin{aligned}
\widehat{\sigma}(x) &= F_0(x, r) + \mathsf{m} \cdot F_1(x, r) \\
&= \sum_{j=0}^{1} \left(\sum_{i=0}^{w} c_{i,j}^{(0)} x^i \right) r^j + \mathsf{m} \cdot \left(\sum_{j=0}^{1} \left(\sum_{i=0}^{w} c_{i,j}^{(1)} x^i \right) r^j \right) \\
&= \sum_{i=0}^{w} \left(c_{i,0}^{(0)} + \mathsf{m} \cdot c_{i,0}^{(1)} + r \cdot c_{i,1}^{(0)} + \mathsf{m} \cdot r \cdot c_{i,1}^{(1)} \right) x^i, \\
&= \sum_{i=0}^{w} s_i x^i, \qquad (5)
\end{aligned}$$

where $s_i := c_{i,0}^{(0)} + \mathsf{m} \cdot c_{i,0}^{(1)} + r \cdot c_{i,1}^{(0)} + \mathsf{m} \cdot r \cdot c_{i,1}^{(1)}$. Note that the adversary can reconstruct r from Γ and at least one share γ_{ℓ_i} of $\mathsf{R}_{\ell_i} \in \mathcal{D} \cap \mathcal{W}$.

On the other hand, the adversary corrupts $\mathcal{W}$ and knows their keys $\mathsf{e}_\ell = (G(v_{\ell_j}), \sigma_{\ell_j}(y, z))$ for $j \in [w]$, where

$$\begin{aligned}
\sigma_{\ell_j}(y, z) &= F_0(\ell_j, y) + z \cdot F_1(\ell_j, y) \\
&= \varphi_{\ell_j,0}^{(0)} + \varphi_{\ell_j,1}^{(0)} y + \varphi_{\ell_j,0}^{(1)} z + \varphi_{\ell_j,1}^{(1)} yz, \qquad (6)
\end{aligned}$$

where $\varphi_{\ell_j,b}^{(\beta)} := \sum_{i=0}^{w} c_{i,b}^{(\beta)} \ell_j^i$ for every $b, \beta \in \{0, 1\}$.

From Eqs. (5) and (6), we have

$$\begin{bmatrix} c_{0,0}^{(0)} & c_{0,0}^{(1)} & c_{0,1}^{(0)} & c_{0,1}^{(1)} \\ c_{1,0}^{(0)} & c_{1,0}^{(1)} & c_{1,1}^{(0)} & c_{1,1}^{(1)} \\ \vdots & \vdots & \vdots & \vdots \\ c_{w,0}^{(0)} & c_{w,0}^{(1)} & c_{w,1}^{(0)} & c_{w,1}^{(1)} \end{bmatrix} \begin{bmatrix} 1 \\ \mathsf{m} \\ r \\ \mathsf{m} \cdot r \end{bmatrix} = \begin{bmatrix} s_0 \\ s_1 \\ \vdots \\ s_w \end{bmatrix},$$

and

$$\begin{bmatrix} 1 & \ell_1 & \cdots & \ell_1^w \\ 1 & \ell_2 & \cdots & \ell_2^w \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \ell_w & \cdots & \ell_w^w \end{bmatrix} \begin{bmatrix} c_{0,0}^{(0)} & c_{0,0}^{(1)} & c_{0,1}^{(0)} & c_{0,1}^{(1)} \\ c_{1,0}^{(0)} & c_{1,0}^{(1)} & c_{1,1}^{(0)} & c_{1,1}^{(1)} \\ \vdots & \vdots & \vdots & \vdots \\ c_{w,0}^{(0)} & c_{w,0}^{(1)} & c_{w,1}^{(0)} & c_{w,1}^{(1)} \end{bmatrix} = \begin{bmatrix} \varphi_{\ell_1,0}^{(0)} & \varphi_{\ell_1,0}^{(1)} & \varphi_{\ell_1,1}^{(0)} & \varphi_{\ell_1,1}^{(1)} \\ \varphi_{\ell_2,0}^{(0)} & \varphi_{\ell_2,0}^{(1)} & \varphi_{\ell_2,1}^{(0)} & \varphi_{\ell_2,1}^{(1)} \\ \vdots & \vdots & \vdots & \vdots \\ \varphi_{\ell_w,0}^{(0)} & \varphi_{\ell_w,0}^{(1)} & \varphi_{\ell_w,1}^{(0)} & \varphi_{\ell_w,1}^{(1)} \end{bmatrix}.$$

We write the above two equations as

$$\mathbf{Cm} = \mathbf{s}, \tag{7}$$
$$\mathbf{LC} = \mathbf{P}, \tag{8}$$

where

$$\mathbf{m} = \begin{bmatrix} 1 \\ \mathsf{m} \\ r \\ \mathsf{m} \cdot r \end{bmatrix}, \quad \mathbf{C} = \begin{bmatrix} c_{0,0}^{(0)} & c_{0,0}^{(1)} & c_{0,1}^{(0)} & c_{0,1}^{(1)} \\ c_{1,0}^{(0)} & c_{1,0}^{(1)} & c_{1,1}^{(0)} & c_{1,1}^{(1)} \\ \vdots & \vdots & \vdots & \vdots \\ c_{w,0}^{(0)} & c_{w,0}^{(1)} & c_{w,1}^{(0)} & c_{w,1}^{(1)} \end{bmatrix},$$

$$\mathbf{s} = \begin{bmatrix} s_0 \\ s_1 \\ \vdots \\ s_w \end{bmatrix}, \quad \mathbf{L} = \begin{bmatrix} 1 & \ell_1 & \cdots & \ell_1^w \\ 1 & \ell_2 & \cdots & \ell_2^w \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \ell_w & \cdots & \ell_w^w \end{bmatrix},$$

$$\mathbf{P} = \begin{bmatrix} \varphi_{\ell_1,0}^{(0)} & \varphi_{\ell_1,0}^{(1)} & \varphi_{\ell_1,1}^{(0)} & \varphi_{\ell_1,1}^{(1)} \\ \varphi_{\ell_2,0}^{(0)} & \varphi_{\ell_2,0}^{(1)} & \varphi_{\ell_2,1}^{(0)} & \varphi_{\ell_2,1}^{(1)} \\ \vdots & \vdots & \vdots & \vdots \\ \varphi_{\ell_w,0}^{(0)} & \varphi_{\ell_w,0}^{(1)} & \varphi_{\ell_w,1}^{(0)} & \varphi_{\ell_w,1}^{(1)} \end{bmatrix}.$$

We can prove the following lemma as in [14, Lemma 1].

Lemma 1. There exist q different matrices $\mathbf{C}$ such that $\mathbf{Cm} = \mathbf{s}$ and $\mathbf{LC} = \mathbf{P}$.

The adversary tries to guess $\sigma_{i^\star}(y,z) = \varphi_{i^\star,0}^{(0)} + \varphi_{i^\star,1}^{(0)} y + \varphi_{i^\star,0}^{(1)} z + \varphi_{i^\star,1}^{(1)} yz$ contained in $\mathsf{R}_{i^\star}$'s secret key $\mathsf{e}_{i^\star}$ and find $\widehat{\sigma}'(x) = \sum_{i=0}^{w} s_i' x^i$ such that

$$\sum_{i=0}^{w} s_i' (i^\star)^i = \varphi_{i^\star,0}^{(0)} + \varphi_{i^\star,1}^{(0)} r + \varphi_{i^\star,0}^{(1)} \mathsf{m}' + \varphi_{i^\star,1}^{(1)} r \cdot \mathsf{m}'.$$

Let

$$\mathbf{i}^\star := \begin{bmatrix} 1 & i^\star & \cdots & (i^\star)^w \end{bmatrix},$$
$$\mathbf{p}^\star := \begin{bmatrix} \varphi_{i^\star,0}^{(0)} & \varphi_{i^\star,1}^{(0)} & \varphi_{i^\star,0}^{(1)} & \varphi_{i^\star,1}^{(1)} \end{bmatrix}.$$

We then write the above equation as

$$\mathbf{i}^\star \mathbf{s} = \mathbf{p}^\star \mathbf{m}, \tag{9}$$

and we can restate the aim of the adversary is to find $\mathbf{s}$ satisfying Eq. (9).

From Lemma 1, there are q different matrices $\mathbf{C}_1, \mathbf{C}_2, \ldots, \mathbf{C}_q$ such that it holds $\mathbf{LC}_1 = \cdots = \mathbf{LC}_q = \mathbf{P}$. Therefore, for any two matrices $\mathbf{C}_i, \mathbf{C}_j$ of them, we have

$$\begin{bmatrix} \mathbf{L} \\ \mathbf{i}^\star \end{bmatrix} \mathbf{C}_i = \begin{bmatrix} \mathbf{P} \\ \mathbf{p}_i^\star \end{bmatrix} \text{ and } \begin{bmatrix} \mathbf{L} \\ \mathbf{i}^\star \end{bmatrix} \mathbf{C}_j = \begin{bmatrix} \mathbf{P} \\ \mathbf{p}_j^\star \end{bmatrix},$$

where $\mathbf{p}_i^\star := \mathbf{i}^\star \mathbf{C}_i$ and $\mathbf{p}_j^\star := \mathbf{i}^\star \mathbf{C}_j$. Since $\mathbf{C}_i \neq \mathbf{C}_j$ holds and $\begin{bmatrix} \mathbf{L} \\ \mathbf{i}^\star \end{bmatrix}$ is a Vandermonde matrix and invertible, we have $\mathbf{p}_i^\star \neq \mathbf{p}_j^\star$. Hence, there are q different vectors $\mathbf{p}_1^\star, \mathbf{p}_2^\star, \ldots, \mathbf{p}_q^\star$ from the adversary's view.

We next show that there are also q candidates of $\mathbf{s}$. From Lemma 1, we obtain the following corollary.

Corollary 1. There exist q different matrices $\mathbf{C}$ such that $\mathbf{Pm} = \mathbf{Ls}$.

Proof. Left multiply Eq. (7) by $\mathbf{L}$ and obtain $\mathbf{LCm} = \mathbf{Ls}$, which implies $\mathbf{Pm} = \mathbf{Ls}$ from Eq. (8). □

As shown above, there are q different vectors $\mathbf{p}_1^\star, \mathbf{p}_2^\star, \ldots, \mathbf{p}_q^\star$ such that it holds that $\mathbf{p}_i^\star \neq \mathbf{p}_j^\star$ for any distinct $i, j \in [q]$. Since it holds that $\mathbf{p}_i^\star \mathbf{m} \neq \mathbf{p}_j^\star \mathbf{m}$ for any $\mathbf{m}$, we have

$$\mathbf{i}^\star \mathbf{s}_i \neq \mathbf{i}^\star \mathbf{s}_j, \tag{10}$$

where $\mathbf{i}^\star \mathbf{s}_i := \mathbf{p}_i^\star \mathbf{m}$ and $\mathbf{i}^\star \mathbf{s}_j := \mathbf{p}_j^\star \mathbf{m}$. From Eq. (10), we have $\mathbf{s}_i \neq \mathbf{s}_j$ for any distinct $i, j \in [q]$. Thus, there are q different values of $\mathbf{s}$ and the probability that the adversary with $\mathcal{W}$ guesses $\widehat{\sigma}'(x)$ satisfying Eq. (9) is $1/q$.

Anonymity. $\mathcal{W}$ has at most w values related to $v_i = C(i)$ (i.e., $G(u_i)$), $\mathcal{W}$ cannot reconstruct the polynomial $C(x)$ since its degree is at most w. More specifically, we have $\mathbf{La} = \mathbf{v}$, where

$$\mathbf{a} := \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_w \end{bmatrix} \text{ and } \mathbf{v} = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_w \end{bmatrix}.$$

Let $\mathbf{i} := [1\ i\ \cdots\ i^w]$ for any $\mathsf{R}_i \in \mathcal{R} \setminus \mathcal{W}$. Then, we have $\begin{bmatrix} \mathbf{L} \\ \mathbf{i} \end{bmatrix} \mathbf{a} = \begin{bmatrix} \mathbf{v} \\ v_i \end{bmatrix}$. Since $\begin{bmatrix} \mathbf{L} \\ \mathbf{i} \end{bmatrix}$ is a Vandermonde matrix and invertible, there is q candidates of v_i that all are equally likely to appear. Therefore, each v_i is independent of its index i, and therefore the proposed construction meets anonymity. □

Table 1 Efficiency comparison between our constructions. $|\mathsf{x}|$ denotes the number of elements in finite field $\mathbb{F}_q$ contained in x, where q is the power of prime such that $q \geq n$.

Schemes	$\lvert\mathsf{e}_\mathsf{S}\rvert$	$\lvert\mathsf{e}_i\rvert$	$\lvert\tau_\mathcal{D}\rvert$	$\delta \geq$	$\varepsilon \leq$
Generic Construction in § 3.1	$2n + 2(w+1)(d+1)$	$2d+4$	$d + (w+1)(d+1)$	$1 - d(n-d)/q$	d/q^2
Direct Construction in § 3.2	$n - d + 3w + 4$	$2w+3$	$w + 1 + n - d + 1$	1	$1/q$

3.3 Efficiency Comparison

We give efficiency comparison between the proposed schemes in Table 1. To give a fair comparison, we instantiate our generic construction with optimal constructions of A-codes and MRA-codes[†]. Note that since MRAuth is used to generate an MRA-code authenticator for a message $(\mathsf{m}, \mathsf{tag}_{i_1}, \ldots, \mathsf{tag}_{i_d}) \in \mathbb{F}_q^{d+1}$, we require large MRA-code secret keys and authenticators.

As can be seen in Table 1, the direct construction achieves smaller sizes of secret keys and authenticators and better correctness parameter δ, though they also depend on values of n, d, and w.

4. Forgery-Detectable MDRA-Codes

As can be seen above, MDRA-codes enable a sender to create an authenticator for an arbitrary subset $\mathcal{D} \subset \mathcal{R}$ such that $|\mathcal{D}| = d$ and detect impersonation and substitution attacks. However, honest receivers have no means of distinguishing valid authenticators from invalid ones. Specifically, δ-correctness (Def. 2) guarantees non-designated receivers obtain `false` as the output of Ver algorithm, while due to (d, w, ε)-security (Def. 3), any receivers get `false` as the output of Ver algorithm if authenticators are forged. Furthermore, if MDRA-codes meet anonymity (Def. 4), then any receiver cannot obtain any information on other receivers[††]. It would be convenient in practice if non-designated receivers can detect forged authenticators.

4.1 Forgery Detection

In this section, we consider an extended functionality called *forgery detection*. MDRA-codes with forgery-detection functionality, which we call *forgery-detectable MDRA-codes*, enable receivers to detect forgery *even if they are not designated*.

Definition 11 (Forgery Detection). Suppose the verification algorithm in Def. 1 in the following extended form:

- $\mathsf{ans} \leftarrow \mathsf{Ver}(\mathsf{e}_i, \mathsf{m}, \tau_\mathcal{D})$: It is a deterministic algorithm for verification. It takes R_i's secret key e_i, a message m, and an authenticator $\tau_\mathcal{D}$ as input, and outputs $\mathsf{ans} \in \{\mathtt{true}, \mathtt{false}, \perp\}$, where `true`, `false`, and $\perp$ indicate 'accept,' 'reject,' and 'undesignated,' respectively.

Then, an MDRA-code Π is said to be forgery-detectable if it satisfies δ-strong correctness and strong (d, w, ε)-security, which are defined as follows.

δ-strong correctness. Let Π be an MDRA-code. We say Π meets δ-strong correctness if for all $n, d, w \in \mathbb{N}$ s.t. $n \geq d$ and $n \geq w$, all $(\mathsf{e}_\mathsf{S}, \mathsf{e}_1, \ldots, \mathsf{e}_n) \leftarrow \mathsf{Gen}(n, w)$, all $\mathsf{m} \in \mathcal{M}$, and all $\mathcal{D} \subset \mathcal{R}$ s.t. $|\mathcal{D}| = d$, the following holds with probability at least δ:

$$\begin{cases} \mathsf{Ver}(\mathsf{e}_i, \mathsf{m}, \mathsf{Auth}(\mathsf{e}_\mathsf{S}, \mathsf{m}, \mathcal{D})) = \mathtt{true} & \text{for every } \mathsf{R}_i \in \mathcal{D}, \\ \mathsf{Ver}(\mathsf{e}_i, \mathsf{m}, \mathsf{Auth}(\mathsf{e}_\mathsf{S}, \mathsf{m}, \mathcal{D})) = \perp & \text{for every } \mathsf{R}_i \notin \mathcal{D}. \end{cases}$$

Strong (d, w, ε)-security. Π said to be strong (d, w, ε)-secure if it holds $\max\{P^+_{\mathsf{Imp}}, P^+_{\mathsf{Sub}}\} \leq \varepsilon$, where P^+_{Imp} and P^+_{Sub} are the success probabilities of the following extended impersonation and substitution attacks.

Extended impersonation attacks. For any $\mathcal{D} \subset \mathcal{R}$ such that $|\mathcal{D}| = d$, any $\mathcal{W} \subset \mathcal{R}$ such that $|\mathcal{W}| \leq w$, and any $\mathsf{R}_i \in \mathcal{R} \setminus \mathcal{W}$ (*not* $\mathsf{R}_i \in \mathcal{D} \setminus \mathcal{W}$), we consider the success probability $P_{\mathsf{Sub}}(\mathcal{D}, \mathcal{W}, i)$ of the impersonation attacks for $(\mathcal{D}, \mathcal{W}, i)$, and define $P^+_{\mathsf{Imp}} := \max_{(\mathcal{D}, \mathcal{W}, i)} P_{\mathsf{Imp}}(\mathcal{D}, \mathcal{W}, i)$.

Extended substitution attacks. For any $\mathcal{D}, \mathcal{D}' \subset \mathcal{R}$ such that $|\mathcal{D}| = |\mathcal{D}'| = d$, any $\mathcal{W} \subset \mathcal{R}$ such that $|\mathcal{W}| \leq w$, and any $\mathsf{R}_i \in \mathcal{R} \setminus \mathcal{W}$ (*not* $\mathsf{R}_i \in \mathcal{D}' \setminus \mathcal{W}$), the success probability $P_{\mathsf{Sub}}(\mathcal{D}, \mathcal{D}', \mathcal{W}, i)$ of the substitution attacks for $(\mathcal{D}, \mathcal{D}', \mathcal{W}, i)$, and we define $P^+_{\mathsf{Sub}} := \max_{(\mathcal{D}, \mathcal{D}', \mathcal{W}, i)} P_{\mathsf{Sub}}(\mathcal{D}, \mathcal{D}', \mathcal{W}, i)$.

The above strong correctness definition guarantees Ver never outputs `false` as long as an authenticator is correctly generated. Moreover, in the above extended attacks, the range of target receivers are extended from $\mathcal{D} \setminus \mathcal{W}$ to $\mathcal{R} \setminus \mathcal{W}$ in order to guarantee that non-designated receivers can detect forgery by checking the output of Ver.

4.2 Forgery-Detectable Construction

We show that our generic construction in Sect. 3.1 can be easily modified to have the forgery-detectable functionality as follows.

$\mathsf{Gen}(n, d, w)$. Same as the original construction.

$\mathsf{Auth}(\mathsf{e}_\mathsf{S}, \mathsf{m}, \mathcal{D})$. Same as the original construction.

$\mathsf{Ver}(\mathsf{e}_i, \mathsf{m}, \tau_\mathcal{D})$. Parse $\mathsf{e}_i = (\mathsf{k}_i, \widehat{\mathsf{e}}_i)$ and $\tau_\mathcal{D} = (\mathsf{tag}_{l_1}, \ldots, \mathsf{tag}_{l_d}, \widehat{\tau})$, respectively. Run $\mathsf{MRVer}(\widehat{\mathsf{e}}_i, (\mathsf{m}, \mathsf{tag}_{l_1}, \ldots, \mathsf{tag}_{l_d}), \widehat{\tau})$. If the output is also `false`, output `false`; otherwise, run $\mathsf{Vrfy}(\mathsf{k}_i, \mathsf{m}, \mathsf{tag}_{l_j})$ for every $j \in [d]$. If there exists at least one index j such that $\mathtt{true} \leftarrow \mathsf{Vrfy}(\mathsf{k}_i, \mathsf{m}, \mathsf{tag}_{l_j})$, output `true`;

[†]We give the details in Appendix.

[††]Anonymity guarantees that any corrupted receivers $\mathcal{W}$ cannot get any information on $\mathcal{D} \setminus \mathcal{W}$ (except for the size $|\mathcal{D}| = d$), which also means $\mathcal{W}$ cannot obtain any information on $(\mathcal{R} \setminus \mathcal{D}) \setminus \mathcal{W}$. Therefore, considering $\mathcal{W} \in \mathcal{R}$ s.t. $|\mathcal{W}| = 1$, it means that any receiver does not know who are designated or not.

otherwise, output $\perp$.

Theorem 3. If the underlying A-code Φ is η-secure, the underlying MRA-code Ψ is (w,μ)-secure, and σ is a random permutation, an MDRA-code Π constructed above meets δ-strong correctness, strong (d,w,ε)-security, and anonymity, where $\delta \geq 1 - d(n-d)\eta$, $w \leq n-1$, and $\varepsilon \leq \mu$.

Proof. We show the above scheme satisfies strong (d,w,ε)-security. We omit the proofs of δ-strong correctness and anonymity since they can be proved in the same way as Theorem 1.

We show the above modified construction is secure against extended impersonation attacks. We consider $P_{\mathsf{Imp}}(\mathcal{D},\mathcal{W},i)$ as in the proof of Theorem 1, and have $P_{\mathsf{Imp}}(\mathcal{D},\mathcal{W},i) \leq \ell \cdot \mu \cdot \eta$ for any $\mathsf{R}_i \in \mathcal{D} \setminus \mathcal{W}$. We here analyze $P_{\mathsf{Imp}}(\mathcal{D},\mathcal{W},i)$ for $\mathsf{R}_i \in \mathcal{R} \setminus (\mathcal{D} \cup \mathcal{W})$. In this case, an adversary aims to generate $(\mathsf{m},(\mathsf{tag}_{l_1},\ldots,\mathsf{tag}_{l_d},\widehat{\tau}))$ so that R_i accepts a pair $((\mathsf{m},\mathsf{tag}_{l_1},\ldots,\mathsf{tag}_{l_d}),\widehat{\tau})$ and rejects $(\mathsf{m},\mathsf{tag}_{l_i})$ for all $i \in [d]$. Therefore, the aim of the adversary is just to break (w,μ)-security of the underlying MRA-code. Hence, for any $\mathcal{D} \subset \mathcal{R}$ s.t. $|\mathcal{D}| = d$, any $\mathcal{W} \subset \mathcal{R}$ s.t. $|\mathcal{W}| \leq n-1$, and any $\mathsf{R}_i \in \mathcal{R} \setminus (\mathcal{D} \cup \mathcal{W})$, we have $P_{\mathsf{Imp}}(\mathcal{D},\mathcal{W},i) \leq \mu$.

Thus, we have

$$P^{+}_{\mathsf{Imp}} = \max_{(\mathcal{D},\mathcal{W},i)} P_{\mathsf{Imp}}(\mathcal{D},\mathcal{W},i) \leq \mu.$$

We can show security against extended substitution attacks in a similar way. □

5. Conclusion

In this paper, we proposed multi-designated receiver authentication codes (MDRA-codes) with information-theoretic security, which is an authentication system to securely transmit a message from a single sender to an arbitrary subset of receivers that have been designated by the sender. In particular, we proposed the formal model of MDRA-codes and formalized security against impersonation and substitution attacks and anonymity. We then showed two constructions of MDRA-codes: a simple generic construction based on traditional A-codes and MRA-codes, and an efficient direct construction based on polynomials over a finite field. In particular, the latter is more efficient than the former in terms of the sizes of tags and keys of the sender and receivers. We also showed how to achieve forgery-detection functionality; we defined it and provided a construction of a forgery-detectable MDRA-code by modifying the proposed generic construction. Our future work includes an optimal construction of MDRA-codes in terms of tag-size and key-size by deriving tight lower bounds on the tag size and the secret-key sizes of the sender and receivers.

Acknowledgments

This research was conducted under a contract of "Research and development on IoT malware removal/make it non-functional technologies for effective use of the radio spectrum" among "Research and Development for Expansion of Radio Wave Resources (JPJ000254)", which was supported by the Ministry of Internal Affairs and Communications, Japan.

References

[1] T. Seito, J. Shikata, and Y. Watanabe, "Multi-designated receiver authentication-codes with information-theoretic security," 56th Annual Conference on Information Science and Systems, CISS 2022, pp.84–89, IEEE, 2022.
[2] E.N. Gilbert, F.J. MacWilliams, and N.J.A. Sloane, "Codes which detect deception," Bell Syst. Tech. J., vol.53, no.3, pp.405–424, 1974.
[3] G.J. Simmons, "Authentication theory/coding theory," Advances in Cryptology – CRYPTO'84, Lecture Notes in Computer Science, vol.196, pp.411–431, Springer Berlin Heidelberg, 1985.
[4] E. Brickell and D. Stinson, "Authentication codes with multiple arbiters," Advances in Cryptology – EUROCRYPT'88, D. Barstow, W. Brauer, P. Brinch Hansen, D. Gries, D. Luckham, C. Moler, A. Pnueli, G. Seegmüller, J. Stoer, N. Wirth, and C. Günther, eds., Lecture Notes in Computer Science, vol.330, pp.51–55, Springer Berlin Heidelberg, 1988.
[5] G. Hanaoka, J. Shikata, Y. Hanaoka, and H. Imai, "The role of arbiters in asymmetric authentication schemes," Information Security, C. Boyd and W. Mao, eds., Lecture Notes in Computer Science, vol.2851, pp.428–441, Springer Berlin Heidelberg, 2003.
[6] G.J. Simmons, "Message authentication with arbitration of transmitter/receiver disputes," Advances in Cryptology – EUROCRYPT'87, D. Chaum and W. Price, eds., Lecture Notes in Computer Science, vol.304, pp.151–165, Springer Berlin Heidelberg, 1988.
[7] G.J. Simmons, "A cartesian product construction for unconditionally secure authentication codes that permit arbitration," J. Cryptology, vol.2, no.2, pp.77–104, 1990.
[8] K. Kurosawa, "New bound on authentication code with arbitration," Advances in Cryptology – CRYPTO'94, Lecture Notes in Computer Science, vol.839, pp.140–149, Springer, 1994.
[9] R. Safavi-Naini and P. Wild, "Information theoretic bounds on authentication systems in query model," IEEE Trans. Inf. Theory, vol.54, no.6, pp.2426–2436, June 2008.
[10] J. Shikata, "Tighter bounds on entropy of secret keys in authentication codes," IEEE Information Theory Workshop, ITW 2017, pp.259–263, 2017.
[11] Y. Desmedt, Y. Frankel, and M. Yung, "Multi-receiver/multi-sender network security: Efficient authenticated multicast/feedback," INFOCOM'92. Eleventh Annual Joint Conference of the IEEE Computer and Communications Societies, IEEE, vol.3, pp.2045–2054, 1992.
[12] T. Hwang and W. Chih-Hung, "Arbitrated unconditionally secure authentication scheme with multi-senders," Information Processing Letters, vol.65, no.4, pp.189–193, 1998.
[13] K. Kurosawa and S. Obana, "Characterization of (k,n) multi-receiver authentication," Information Security and Privacy, ACISP'97, LNCS 1270, pp.205–215, Springer, 1997.
[14] R. Safavi-Naini and H. Wang, "New results on multi-receiver authentication codes," Advances in Cryptology – EUROCRYPT'98, K. Nyberg, ed., Lecture Notes in Computer Science, vol.1403, pp.527–541, Springer Berlin Heidelberg, 1998.
[15] J. Shikata, G. Hanaoka, Y. Zheng, and H. Imai, "Security notions for unconditionally secure signature schemes," Advances in Cryptology – EUROCRYPT 2002, L. Knudsen, ed., Lecture Notes in Computer Science, vol.2332, pp.434–449, Springer Berlin Heidelberg, 2002.
[16] G. Hanaoka, J. Shikata, Y. Zheng, and H. Imai, "Efficient and unconditionally secure digital signatures and a security analysis of a multi-receiver authentication code," Public Key Cryptography, D. Naccache and P. Paillier, eds., Lecture Notes in Computer Science,

vol.2274, pp.64–79, Springer Berlin Heidelberg, 2002.
[17] S. Wang and R. Safavi-Naini, "New results on unconditionally secure multi-receiver manual authentication," Information Theoretic Security, ICITS 2007, Y. Desmedt, ed., Lecture Notes in Computer Science, vol.4883, pp.115–132, Springer Berlin Heidelberg, 2009.
[18] M. Naor, G. Segev, and A. Smith, "Tight bounds for unconditional authentication protocols in the manual channel and shared key models," IEEE Trans. Inf. Theory, vol.54, no.6, pp.2408–2425, 2008.
[19] A. Fiat and M. Naor, "Broadcast encryption," Advances in Cryptology – CRYPTO'93, Lecture Notes in Computer Science, vol.773, pp.480–491, Springer Berlin Heidelberg, 1994.
[20] C. Blundo, L. Mattos, and D. Stinson, "Trade-offs between communication and storage in unconditionally secure schemes for broadcast encryption and interactive key distribution," Advances in Cryptology – CRYPTO'96, Lecture Notes in Computer Science, vol.1109, pp.387–400, Springer Berlin Heidelberg, 1996.
[21] K. Kurosawa, T. Yoshida, Y. Desmedt, and M. Burmester, "Some bounds and a construction for secure broadcast encryption," Advances in Cryptology – ASIACRYPT'98, Lecture Notes in Computer Science, vol.1514, pp.420–433, Springer Berlin Heidelberg, 1998.
[22] Y. Watanabe and J. Shikata, "Unconditionally secure broadcast encryption schemes with trade-offs between communication and storage," IEICE Trans. Fundamentals, vol.E99-A, no.6, pp.1097–1106, June 2016.
[23] Y. Watanabe, N. Yanai, and J. Shikata, "Anonymous broadcast authentication for securely remote-controlling IoT devices," Advanced Information Networking and Applications, L. Barolli, I. Woungang, and T. Enokido, eds., Cham, pp.679–690, Springer International Publishing, 2021.
[24] H. Chan and A. Perrig, "Round-efficient broadcast authentication protocols for fixed topology classes," Proc. IEEE S&P 2010, pp.257–272, IEEE, 2010.
[25] A. Perrig, "The BiBa one-time signature and broadcast authentication protocol," Proc. CCS 2001, pp.28–37, ACM, 2001.
[26] A. Perrig, R. Canetti, J.D. Tygar, and D. Song, "Efficient authentication and signing of multicast streams over lossy channels," Proc. IEEE S&P 2000, pp.56–73, IEEE, 2000.
[27] K.A. Shim, "Basis: A practical multi-user broadcast authentication scheme in wireless sensor networks," IEEE Trans. Inf. Forensics Security, vol.12, no.7, pp.1545–1554, 2017.
[28] R. Safavi-Naini and H. Wang, "Broadcast authentication for group communication," Theoretical Computer Science, vol.269, no.1-2, pp.1–21, 2001.
[29] F. Laguillaumie and D. Vergnaud, "Multi-designated verifiers signatures," ICICS 2004, J. Lopez, S. Qing, and E. Okamoto, eds., Berlin, Heidelberg, pp.495–507, Springer Berlin Heidelberg, 2004.
[30] Y. Zhauniarovich, I. Khalil, T. Yu, and M. Dacier, "A survey on malicious domains detection through dns data analysis," ACM Computing Surveys, vol.51, no.4, pp.1–36, 2018.
[31] G. Hanaoka, J. Shikata, Y. Hanaoka, and H. Imai, "Unconditionally secure anonymous encryption and group authentication," The Computer Journal, vol.49, no.3, pp.310–321, 2006.
[32] I. Damgård, H. Haagh, R. Mercer, A. Nitulescu, C. Orlandi, and S. Yakoubov, "Stronger security and constructions of multi-designated verifier signatures," Theory of Cryptography, TCC 2020, R. Pass and K. Pietrzak, eds., Cham, pp.229–260, Springer International Publishing, 2020.
[33] R. Blom, "An optimal class of symmetric key generation systems," Advances in Cryptology – EUROCRYPT'84, T. Beth, N. Cot, and I. Ingemarsson, eds., Lecture Notes in Computer Science, vol.209, pp.335–338, Springer, 1985.
[34] T. Matsumoto and H. Imai, "On the key predistribution system: A practical solution to the key distribution problem," Advances in Cryptology – CRYPTO'87, Lecture Notes in Computer Science, vol.293, pp.185–193, Springer, 1988.
[35] C. Blundo, A. Santis, A. Herzberg, S. Kutten, U. Vaccaro, and M. Yung, "Perfectly-secure key distribution for dynamic conferences," Advances in Cryptology – CRYPTO'93, E. Brickell, ed., Lecture Notes in Computer Science, vol.740, pp.471–486, Springer, 1993.
[36] H. Chen, S. Ling, C. Padró, H. Wang, and C. Xing, "Key predistribution schemes and one-time broadcast encryption schemes from algebraic geometry codes," Cryptography and Coding, M. Parker, ed., Lecture Notes in Computer Science, vol.5921, pp.263–277, Springer, 2009.
[37] M. Luby and J. Staddon, "Combinatorial bounds for broadcast encryption," Advances in Cryptology – EUROCRYPT'98, K. Nyberg, ed., Lecture Notes in Computer Science, vol.1403, pp.512–526, Springer, 1998.
[38] C. Blundo and A. Cresti, "Space requirements for broadcast encryption," Advances in Cryptology – EUROCRYPT'94, A. Santis, ed., Lecture Notes in Computer Science, vol.950, pp.287–298, Springer, 1995.
[39] C. Padró, I. Gracia, and S. Martín, "Improving the trade-off between storage and communication in broadcast encryption schemes," Discrete Applied Mathematics, vol.143, no.1-3, pp.213–220, 2004.

Appendix: Constructions of Building Blocks

Optimal construction of an A-code. An well-known optimal construction of an A-code is as follows:

1. $\mathsf{Setup}()$: Let $\mathbb{F}_q$ is a finite field, where q is the power of prime. Randomly choose a, b from $\mathbb{F}_q$ and output $\mathsf{k} := (a, b)$.
2. $\mathsf{Tag}(\mathsf{k}, \mathsf{m})$: Output $\mathsf{tag} := a \cdot \mathsf{m} + b$.
3. $\mathsf{Vrfy}(\mathsf{k}, \mathsf{m}, \mathsf{tag})$: Check if it holds $\mathsf{tag} = a \cdot \mathsf{m} + b$. If so, output `true`; otherwise, output `false`.

The above construction meets $1/q$-security.

Optimal construction of an MRA-code. An optimal construction of an MRA-code [11] is as follows:

1. $\mathsf{MRGen}(n, w)$: Let $\mathbb{F}_q$ is a finite field, where q is the power of prime. Randomly choose two polynomials $f(x), g(x) \in \mathbb{F}_q[X]$ with the degree at most w. Output $\widehat{\mathsf{e}}_\mathsf{S} := (f(x), g(x))$ and $\widehat{\mathsf{e}}_i := (f(i), g(i))$ for all $i \in [n]$.
2. $\mathsf{MRAuth}(\widehat{\mathsf{e}}_\mathsf{S}, \mathsf{m})$: Output $\widehat{\tau}(x) := f(x) \cdot \mathsf{m} + g(x)$.
3. $\mathsf{MRVer}(\widehat{\mathsf{e}}_i, \mathsf{m}, \widehat{\tau})$: Check if it holds $\widehat{\tau}(i) = f(i) \cdot \mathsf{m} + g(i)$. If so, output `true`; otherwise, output `false`.

The above construction meets $(w, 1/q)$-security.

Yohei Watanabe received the B.E., M.E., and Ph.D. degrees in information science from Yokohama National University in 2011, 2013, and 2016, respectively. He is currently Assistant Professor at the University of Electro-Communications, and also serves as Invited Adviser at NICT, Collaborative Researcher at AIST, and Research Fellow at Japan Datacom, Co., Ltd. His research interests include cryptography and information security. He is a member of IEICE, IPSJ, IEEE, and IACR.

Takenobu Seito received the Ph.D. degrees in engineering from Yokohama National University in 2011. He has been working mainly on business applications of information security technologies at a financial institution and auditing firm in Japan. He also currently serves Assistant Professor at Institute of Advanced Sciences, Yokohama National University, Japan.

Junji Shikata received the B.S. and M.S. degrees in mathematics from Kyoto University, Kyoto, Japan, in 1994 and 1997, respectively, and the Ph.D. degree in mathematics from Osaka University, Osaka, Japan, in 2000. From 2000 to 2002 he was a Postdoctoral Fellow at the Institute of Industrial Science, the University of Tokyo, Tokyo, Japan. Since 2002 he has been with the Graduate School of Environment and Information Sciences, Yokohama National University, Yokohama, Japan. From 2008 to 2009, he was a visiting researcher at the Department of Computer Science, Swiss Federal Institute of Technology (ETH), Zurich, Switzerland. Currently, he is a Professor of Yokohama National University. His research interests include cryptology, information theory, theoretical computer science, and computational number theory. Dr. Shikata received several awards including the 19th TELECOM System Technology Award from the Telecommunications Advancement Foundation in 2004, the Wilkes Award 2006 from the British Computer Society, and the Young Scientists' Prize, the Commendation for Science and Technology by the Minister of Education, Culture, Sports, Science and Technology in Japan in 2010.