Josai Mathematical Monographs
vol. 7 (2014), pp. 85-110

Information-Theoretically Secure Anonymous Group Authentication with Arbitration: Formal Definition and Construction*

Takenobu Seito, Yohei Watanabe, Kazuyuki Kinose, Junji Shikata

Abstract. In cryptographic applications, there is often a need for protecting privacy of users besides integrity of message transmitted in a public channel. In information-theoretic (or unconditional) security setting, a model of GA-codes (Group Authentication codes) which can ensure both the integrity of the message and the anonymity for senders was proposed. In this model, there are multiple senders and a single receiver. And, one of the senders can generate an authenticated message anonymously. That is, the receiver can verify the validity of the authenticated message, but he cannot specify the sender of it. In GA-codes, it is assumed that both the sender and receiver are honest. However, it may be unnatural and an ideal assumption in several situations. In this paper, we remove the assumption and newly propose a formal definition (i.e., the model and security definitions) of GA^2-codes (Group Authentication codes with Arbitration). In GA^2-codes, it is assumed that the sender or the receiver can be dishonest and thus a dispute between them may occur. To resolve such a dispute, we introduce an honest arbiter in GA^2-codes. This model can be considered as natural extension of that of both the GA-codes and the traditional A^2-codes (Authentication codes with Arbitration). In addition, we propose a construction which meets our security definition of GA^2-codes by using polynomials over finite fields. We also consider the case that the arbiter is not always honest and call this model GA^3-codes (GA^2-codes with protection against arbiter's attack), which is further extension of GA^2-codes and be naturally considered from a similar setting of the traditional A^3-codes (A^2-code with protection against arbiter's attack).

1. Introduction

In order to theoretically show the security of cryptographic schemes, there are two types of approaches: The security relies on the computational infeasibility of breaking it (called computational security) or on the theoretical impossibility of breaking it, even by using unbounded computing power (called information-theoretic security or unconditional security). Since computational security is based on the assumptions of difficulty of intractable problems, it can only hold under assumptions on the adversary's computational resources (i.e., the adversary is assumed to be a polynomial-time Turing machine). In other words, the adversary

[*] The material in this paper was presented in part at the 3rd International Symposium on Engineering, Energy and Environment (3rd ISEEE), Bangkok, Thailand, November, 2013.

who has an unbounded computational power can break every scheme with computational security by at least exhaustive search over a key space (or by more efficient algorithms). In addition, it is known that quantum computers, if built, can solve the factoring and discrete logarithm problems in quantum-polynomial time [**8**]. On the other hand, information-theoretic security relies on no assumption of computationally intractable problems and specific computational models. Thus, even if algorithms and computer technologies are rapidly developed in the future, information-theoretically secure cryptographic schemes can still guarantee the security. From these points, we can find the advantage of information-theoretic security.

In cryptographic application, there is need for protecting privacy of users besides integrity of data transmitted in a public channel. In information-theoretic security setting, a model of GA-codes (Group Authentication codes) which can ensure both the integrity of the message and the anonymity for senders was proposed by Hanaoka et al [**5**]. In this model, it is assumed that both the sender and the receiver are mutually trusted. However, it may be unnatural and an ideal assumption in many situations. In this paper, we remove this assumption and newly propose a formal model. More specifically, we newly propose a model and a security definition of the GA^2-codes (GA-codes with Arbitration) in which a trusted arbiter is provided so that the arbiter can resolve a dispute between the sender and the receiver. This model can be considered as extension of both the GA-codes and the A^2-codes. In addition, we show a construction which meets our security definition of the GA^2-codes. Also, we consider the case that the arbiter is not always honest and call this model the GA^3-code (GA^2-code with protection against Arbiter's attack), which is similar to the setting of A^3-codes.

The rest of this paper is organized as follows: In Section 2, we survey the information-theoretically secure authentication code and its variants. In Section 3, we propose a model and a security definition of GA^2-codes. In Section 4, we give a construction of GA^2-codes by using polynomials over finite fields. Finally, in Section 5, we consider a security definition and a construction of GA^3-codes.

2. Authentication code and its Variants

2.1. A-codes

Authenticity (or integrity) is one of the fundamental and important cryptographic functions, and authentication/signature schemes are usually used for providing this function. In particular, A-code (Authentication-code) is the traditional authentication scheme with information-theoretic security which was originally proposed by Gilbert, McWilliams and Sloan [**3**], and later developed by Simmons [**9**].

For simplicity, throughout this paper, 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 [**6**]. The model of A-codes involves three participants, a sender S, a receiver R and a trusted initializer TI. The A-code Φ consists of a three-tuple of algorithms (*Gen*, *Tag*, *Ver*) with three spaces, $\mathcal{M}_A$, $\mathcal{A}$ and $\mathcal{K}$, where these three spaces are finite sets of possible messages, authenticators (or tags), and secret-keys, respectively. *Gen* is a key generation algorithm executed by TI, which takes a security parameter on input and outputs a secret-key k. For a communication, the sender S generates an authenticator by using *Tag* with the secret-key and a message. *Tag* is an algorithm for generating an authenticator. *Tag* takes a message $m \in \mathcal{M}_A$ and a secret-key $k \in \mathcal{K}$ on input and outputs an authenticator $\alpha \in \mathcal{A}$, and we write $\alpha = Tag(k, m)$ for it. Then, S sends the authenticated message (i.e., the pair of the message and authenticator) (m, α) to the receiver over a public channel.

On receiving (m, α), a receiver R can check the validity of it by using *Ver*. That is, the received authentication code originates from the sender and it has not been substituted during the transmission over the public channel. *Ver* takes the pair of the message and the authenticator (m, α) and a secret-key k on input, and outputs *valid* or *invalid*, and we write *valid* $=$ *Ver*$(k, (m, \alpha))$ or *invalid* $=$ *Ver*$(k, (m, \alpha))$ for it.

In A-codes, for simplicity we assume the following one-time model: it is allowed to generate an authenticator and transmit a pair of a message and an authenticator among senders only once; and the receiver is allowed to verify a pair of a message and an authenticator at most one time.

In A-codes, security under consideration is protection against an adversary, called opponent, who can impersonate the sender by inserting a message on the channel (Impersonation Attack), or can replace the pair of a message and an authenticator sent with another one (Substitution Attack). Formally, the security of A-codes is defined as follows.

Definition 1 (Security of A-code). *Let Φ be an A-code in the one-time model. The scheme Φ is said to be an ϵ-one-time secure A-code, if $P_O^{(A)} \le \epsilon$, where $P_O^{(A)}$ is defined by $P_O^{(A)} := \max(P_{I_O}^{(A)}, P_{S_O}^{(A)})$, and $P_{I_O}^{(A)}$ and $P_{S_O}^{(A)}$ are given as follows.*

Impersonation attack*: *The adversary O tries to generate a fraudulent pair of a message and an authenticator (m, α) that will be accepted by a receiver R. The success probability of this attack denoted by $P_{I_O}^{(A)}$ is defined as

$$P_{I_O}^{(A)} := \max_{(m,\alpha)} \Pr(R \textit{ accepts } (m, \alpha)).$$

Substitution attack*: *The adversary O can observe a transmitted pair of a message and an authenticator (m, α) which is generated by the sender S, and then tries to generate a fraudulent pair of a message and an authenticator (m', α') that will be accepted by a receiver R. The success probability of this

attack denoted by $P_{S_O}^{(A)}$ *is defined as*

$$P_{S_O}^{(A)} := \max_{(m',\alpha')} \max_{(m,\alpha)\neq(m',\alpha')} \Pr(R \textit{ accepts } (m',\alpha') \mid (m,\alpha)).$$

The traditional A-code is the most fundamental primitive for providing functionality of authenticity with information-theoretic security. Based on it, various extended models or variants of the A-code are proposed so far. We briefly explain the two major extension of the A-code, A^2-codes and A^3-codes, below.

2.2. A^2-codes and A^3-codes

In A-codes, since the two parties share a common secret-key, it must be assumed that they trust each other, or equivalently they are assumed to be honest players in each other. However, it may be unnatural and an ideal assumption in many situations. Therefore, an extension of A-code based on a more natural assumption, called A^2-code (Authentication code with Arbitration) is introduced by Simmons[**10, 11**]. In A^2-codes, the sender or the receiver can be dishonest. Thus, a dispute between them may occur, i.e., the sender denies a pair of messages and authenticators after having sent it, or the receiver forged a sender's authenticated massage and claims its validity. To solve the above dispute, the third participant, called an arbiter, is introduced in A^2-code. The arbiter is always honest and the sender and the receiver must trust the arbiter's honesty. The role of the arbiter is to solve the dispute between the sender and the receiver as a judge in the court. Following the above scenario, there are five kinds of attacks in this model: impersonation by the outsider, impersonation by the sender, impersonation by the receiver, substitution by the outsider, and substitution by the receiver.

The assumption of the arbiter's honestly in A^2-codes is very natural in several situations, however the opposite situation is pointed out in [**11**]. In order to remove the assumption that the arbiter is always honest, Brickell and Stinson [**1**] introduced the A^3-code (A^2-code with protecting against Arbiter's attack). Afterward, Safavi-Naini and Wang [**7**] introduced a more generic model of A^3-codes in which the arbiter can collude with a malicious entity. In the model of A^3-code, it is assumed that the arbiter is not always honest, which we call the arbiter being *semi-honest* in this paper. It means that the arbiter makes a judgment honestly in the case of a dispute, however he may take a fraudulent behavior in cooperation with some malicious entity. Intuitively, the semi-honest arbiter is like a judge who behaves honestly in the court, however he does not necessarily behave honestly outside of the court. And thus, it requires a weaker assumption and may be preferable in several situations.

We now summarize assumptions of participant's honesty in A-code, A^2-code and A^3-code in Table 1.

Next, we show the formal definitions of A^2-codes and A^3-codes.

	Assumptions of participant's honesty		
	Sender	Receiver	Arbiter
A-code	Honest	Honest	—
A^2-code	Dishonest	Dishonest	Honest
A^3-code	Dishonest	Dishonest	Semi-honest

Table 1. Assumptions of participant's honesty in A-code, A^2-code and A^3-code.

A^2-codes: Formally, A^2-codes are defined as follows. In A^2-codes, there are a sender S, a receiver R, an arbiter A, and a trusted initializer TI. The A^2-code Θ consists of a four-tuple of algorithms ($AGen$, *Auth*, *Vrfy*, *AVrfy*) with five spaces, $\tilde{\mathcal{M}}_A$, $\tilde{\mathcal{A}}$, $\mathcal{K}_S$, $\mathcal{K}_R$, and $\mathcal{K}_A$, where $\tilde{\mathcal{M}}_A$ is a finite set of possible messages, $\tilde{\mathcal{A}}$ is a finite set of possible authenticators, and $\mathcal{K}_S$, $\mathcal{K}_R$, and $\mathcal{K}_A$ are finite sets of possible secret keys of the sender S, the receiver R, and the arbiter A, respectively. $AGen$ is a key generation algorithm executed by TI, which takes a security parameter on input and outputs secret-keys k_S, k_R, and k_A for S, R, and A, respectively. For a communication, the sender S generates an authenticator by using *Auth* with the secret-key and a message. *Auth* takes a message $m \in \tilde{\mathcal{M}}_A$ and a secret-key $k_S \in \mathcal{K}_S$ on input and outputs an authenticator $\alpha \in \tilde{\mathcal{A}}$, and we write $\alpha = Auth(k_S, m)$ for it. On receiving (m, α), a receiver R can check the validity of it by using *Vrfy*. That is, *Vrfy* takes the pair of the message and the authenticator (m, α) and a secret-key $k_R \in \mathcal{K}_R$ on input, and outputs *valid* or *invalid*, and we write *valid* $= Vrfy(k_R, (m, \alpha))$ or *invalid* $= Vrfy(k_R, (m, \alpha))$ for it. If a dispute between S and R occurs, A can resolve the dispute based on the following judgment by using his secret key k_A.

(1) R ascribes an authenticated message (m, α) to S_i, but S denies it. Then, S or R asks for arbitration.

- R wins if A accepts (m, α) (i.e. $AVrfy(k_A, (m, \alpha)) = valid$).
- R loses otherwise.

(2) S produces (m, α) such that R will accept it. After having sent it to R, S attempts to deny having created (m, α). Then, S or R asks for arbitration.

- S wins if A rejects (m, α) (i.e. $AVrfy(k_A, (m, \alpha)) = invalid$).
- S loses otherwise.

(3) After knowing that R rejected (m, α), S claims that (m, α) is valid. Then, S or R asks for arbitration.

- S wins if A accepts (m, α) (i.e. $AVrfy(k_A, (m, \alpha)) = valid$).
- S loses otherwise.

In A^2-codes, for simplicity we assume the following one-time model as in the model of A-codes: the sender is allowed to generate an authenticator and transmit an authenticated message only once; each of the arbiter and the receiver is allowed to verify an authenticated message at most one time.

Next, we define the security definition of A^2-codes. In A^2-codes, an adversary can perform impersonation attacks, substitution attacks, denial attacks, and claim attacks. Impersonation attacks and substitution attacks are the same as those in A-codes. In denial attacks, the adversary produces an authenticated message (i.e., a pair of messages and authenticators) such that R will accept it, but attempts to deny the authenticated message after having sent it. In claim attacks, after knowing that R rejected an authenticated message, the adversary claims that it is valid. The aim of this attack is to compel R to accept the authenticated message even if R rejected it.

We now classify the attacks according to adversary's types: an outsider O who can only have access to public information, a dishonest sender S, a dishonest receiver R, or possible collusion of them. Then, the security definition of A^2-codes is defined as follows.

Definition 2 (Security of A^2-code). *Let Θ be an A^2-code in the one-time model. The scheme Θ is said to be δ-one-time secure, if* $\max(P_O^{(A^2)}, P_S^{(A^2)}, P_R^{(A^2)}) \leq \delta$*, where $P_O^{(A^2)}$ is the same as $P_O^{(A)}$ in Definition 1, and $P_S^{(A^2)}$ and $P_R^{(A^2)}$ are defined as follows.*

(i) ***Attacks by** S**:** Let $P_S^{(A^2)} := \max(P_D^{(A^2)}, P_C^{(A^2)})$, where $P_D^{(A^2)}$ and $P_C^{(A^2)}$ are given as follows.*

(1) Denial attack: After sending an authenticated message to the receiver R, the dishonest sender S tries to deny having sent it. S tries to generate (m, α) such that R accepts it and A rejects it (i.e., S wins in the arbitration). The success probability of this attack denoted by $P_D^{(A^2)}$ is defined as

$$P_D^{(A^2)} := \max_{k_S} \max_{(m,\alpha)} \Pr(R \textit{ accepts } (m, \alpha) \wedge A \textit{ rejects } (m, \alpha) \mid k_S).$$

(2) Claim attack: After knowing that the receiver R has rejected an authenticated message, S tries to claim that it is valid. S tries to generate (m, α) such that R rejects it and the arbiter A accepts it (i.e., S wins in the arbitration). The success probability of this attack denoted by $P_C^{(A^2)}$ is defined as

$$P_C^{(A^2)} := \max_{k_S} \max_{(m,\alpha)} \Pr(R \textit{ rejects } (m, \alpha) \wedge A \textit{ accepts } (m, \alpha) \mid k_S).$$

(ii) ***Attacks by*** *R: The dishonest receiver R tries to trump up an authenticated message from the sender. Let $P_R^{(A^2)} := \max(P_{I_R}^{(A^2)}, P_{S_R}^{(A^2)})$, where $P_{I_R}^{(A^2)}$ and $P_{S_R}^{(A^2)}$ are given as follows.*

Impersonation attack: *R tries to generate a fraudulent authenticated message (m, α) such that the arbiter A accepts it. The success probability of this attack denoted by $P_{I_R}^{(A^2)}$ is defined as*

$$P_{I_R}^{(A^2)} := \max_{k_R} \max_{(m,\alpha)} \Pr(A \textit{ accepts } (m,\alpha) \mid k_R).$$

Substitution attack: *R can observe a transmitted authenticated message (m, α) which is generated by S, and then tries to generate a fraudulent one (m', α') such that the arbiter A accepts it and $(m', \alpha') \neq (m, \alpha)$. The success probability of this attack denoted by $P_{S_R}^{(A^2)}$ is defined as*

$$P_{S_R}^{(A^2)} := \max_{k_R} \max_{(m',\alpha')} \max_{(m,\alpha)\neq(m',\alpha')} \Pr(A \textit{ accepts } (m',\alpha') \mid k_R, (m,\alpha)).$$

A^3-codes: In this paper, we consider the security of the *traditional* A^3-code in [**1**]. Formally, the A^3-code, which is the A^2-code without the assumption that the arbiter is always honest, is defined as follows.

Definition 3 (Security of A^3-code). *Let Θ be a δ-one-time secure A^2-code. The scheme Θ is said to be a δ-one-time secure A^3-code, if $P_A^{(A^3)}$ is at most δ, where $P_A^{(A^3)}$ is defined as follows.*

- ***Attacks by*** *A: The malicious arbiter A tries to trump up an authenticated message from the sender. Let $P_A^{(A^3)} := \max(P_{I_A}^{(A^3)}, P_{S_A}^{(A^3)})$, where $P_{I_A}^{(A^3)}$ and $P_{S_A}^{(A^3)}$ are given as follows.*

  Impersonation attack: *A tries to generate a fraudulent authenticated message (m, α) such that the receiver R will accept it. The success probability of this attack denoted by $P_{I_A}^{(A^3)}$ is defined as*

$$P_{I_A}^{(A^3)} := \max_{k_A} \max_{(m,\alpha)} \Pr(R \textit{ accepts } (m,\alpha) \mid k_A).$$

  Substitution attack: *A can observe a transmitted authenticated message (m, α) which is generated by S, and then tries to generate a fraudulent one (m', α') such that the receiver R will accept it and $(m', \alpha') \neq (m, \alpha)$. The*

	Number of Sender	Number of Receiver	Additional Property
A-code	Single	Single	—
GA-code	Multiple	Single	Anonymity of Senders

Table 2. The model and additional property of A-codes and GA-codes.

success probability of this attack denoted by $P_{S_A}^{(A^3)}$ *is defined as*

$$P_{S_A}^{(A^3)} := \max_{k_A} \max_{(m',\alpha')} \max_{(m,\alpha)\neq(m',\alpha')} \Pr(R \textit{ accepts } (m',\alpha') \mid k_A, (m,\alpha)).$$

2.3. GA-codes

In several cryptographic applications (e.g., e-voting and electronic bidding), there is a need for protecting users' privacy (anonymity) besides integrity of data transmitted in a public channel. The group signature scheme introduced by Chaum and Van Heyst proposed the scheme which can satisfy both requirements [**2**]. This scheme allows a group member to sign (authenticate) a message anonymously on behalf of the group. However, in the case of dispute between members of the groups, the identity of a sender of a signed message can be revealed only by a privileged participant, called a group manager. Group signatures have mainly been studied from a viewpoint of computational security so far. The extension of A-codes, called GA-codes (Group Authentication codes) was proposed by Hanaoka et al. [**5**]. The GA-code is an information-theoretically secure authentication code with anonymity whose function is similar to that of computationally secure group signatures. In the model of GA-codes, there are multiple senders, a single receiver and a group authority. For communication, one of the senders can anonymously send an authenticated message to the receiver. And then, the receiver can verify the validity of it, however, he cannot specify the sender of the authenticated message by himself. If the receiver wants to reveal the identity of the sender, he can only obtain it by cooperating with the group authority. In GA-code, it is assumed that the receiver is honest, and there are four kinds of attacks: impersonation by the outsider, impersonation by a collusion group of malicious senders, substitution by the outsider, and substitution by a collusion group of malicious senders. Here, we summarize the features of A-codes and GA-codes in Table 2.

Formally, the model of GA-codes is as follows. The model of GA-codes involves $n+3$ participants, n senders $S_1, \ldots, S_n$, a receiver R, a group authority G, and a trusted initializer TI. For convenience, for each sender $S_i \in \{S_1, S_2, \ldots, S_n\}$ we use the same symbol S_i to denote the identity of the sender. The GA-code Φ consists of a four-tuple of algorithms (*KGen*, *Sign*, *GVrfy*, *Open*) with $n+4$ spaces, $\mathcal{M}_G$, $\mathcal{A}_G$, $\mathcal{AK}_1, \ldots, \mathcal{AK}_n$, $\mathcal{VK}$, and $\mathcal{GK}$, where they are finite sets of possible messages, possible authenticators (or tags), possible secret-keys of senders $S_1, \ldots, S_n$, possible secret-keys of the receiver, and possible secret-keys of the group authority, respectively. *KGen* is a key generation algorithm executed by TI, which takes a security parameter on input and outputs secret-keys $ak_1, \ldots, ak_n, vk, gk$ for $S_1, \ldots, S_n, R, G$, respectively. For a communication, the sender S_i generates an authenticator by using *Sign* with the secret-key and a message. *Sign* takes a message $m \in \mathcal{M}_G$ and an S_i's secret-key $ak_i \in \mathcal{AK}_i$ on input and outputs an authenticator $\sigma \in \mathcal{A}_G$, and we write $\sigma = \mathit{Sign}(ak_i, m)$ for it. Then, S_i sends the authenticated message (m, σ) to the receiver over a public channel. On receiving (m, σ), a receiver R can check the validity of it by using *GVrfy*. *GVrfy* takes an authenticated message (m, σ) and an R's secret-key vk on input, and outputs *valid* or *invalid*, and we write $\mathit{valid} = \mathit{GVrfy}(vk, (m, \sigma))$ or $\mathit{invalid} = \mathit{GVrfy}(vk, (m, \sigma))$ for it.

In GA-codes, an adversary can perform impersonation attacks or substitution attacks, which is the same situation as that of A-codes. We classify the attacks according to adversary's types: an outsider O who can only have access to public information, and a group of k malicious senders. Here, we assume that a group authority and the receiver are honest. Also, we denote a group of k $(1 \leq k \leq n-1)$ malicious senders by $S(i_1, \ldots, i_k) := \{S_{i_1}, \ldots, S_{i_k}\}$ and their secret information by $e_{S(i_1, \ldots, i_k)}$. Also let $\tilde{\mathcal{W}} := \{S(i_1, \ldots, i_k) \mid S(i_1, \ldots, i_k) \subset \mathcal{S}\}$. Then, security of GA-codes is defined as follows.

Definition 4 (Security of GA-code). *Let Ψ be a GA-code in the one-time model. The scheme Ψ is said to be a (p, k, n)-one-time secure GA-code, if the following conditions are satisfied.*

1) *Each of R and G obtains no information on the identity of the sender from an authenticated message alone. Namely, for any $i \in \{1, 2, \ldots, n\}$, we have*

   a) $\max_{(m,\sigma)} \max_{vk} |\Pr(S_i \mid vk, (m, \sigma)) - \Pr(S_i \mid vk)| = 0$*; and*

   b) $\max_{(m,\sigma)} \max_{gk} |\Pr(S_i \mid gk, (m, \sigma)) - \Pr(S_i \mid gk)| = 0.$

   The above equations mean that, after distributing secret-keys vk and gk, any authenticated message (m, σ) will reveal no information on the identity of senders. Note that the above σ is taken such that $\sigma = \mathit{Sign}(ak_i, m)$ for some ak_i and m.

2) *No information on the identity of the sender of (m, σ) is leaked from (m, σ) itself against malicious senders $S(i_1, \ldots, i_k)$. Namely, for any $S(i_1, \ldots, i_k) \in \tilde{\mathcal{W}}$ and $S_i \in \mathcal{S} \setminus S(i_1, \ldots, i_k)$, we have*

$$\max_{(m,\sigma)} \max_{ak_{S(i_1,\ldots,i_k)}} \left| \Pr(S_i \mid ak_{S(i_1,\ldots,i_k)}, (m, \sigma)) - \Pr(S_i \mid ak_{S(i_1,\ldots,i_k)}) \right| = 0,$$

   This equation means that, after distributing secret-keys $ak_{S(i_1,\ldots,i_k)}$, any authenticated message (m, σ) will reveal no information on the identity of senders.

3) All of the success probabilities of the following attacks, $P_O^{(GA)}$ and $P_S^{(GA)}$, are at most $p \in [0,1]$.

(i) ***Attacks by** O**:** The outsider O tries to trap the receiver R. Let $P_O^{(GA)} := \max(P_{I_O}^{(GA)}, P_{S_O}^{(GA)})$, where $P_{I_O}^{(GA)}$ and $P_{S_O}^{(GA)}$ are given as follows.*

Impersonation attack**:** *O tries to generate a fraudulent authenticated message (m,σ) that will be accepted by a receiver R. The success probability of this attack denoted by $P_{I_O}^{(GA)}$ is defined as*

$$P_{I_O}^{(GA)} := \max_{(m,\sigma)} \Pr(R \textit{ accepts } (m,\sigma)).$$

Substitution attack**:** *O can observe a transmitted authenticated message (m,σ) which is generated by one of the senders S_i, and then tries to generate a fraudulent authenticated message $(m',\sigma') \neq (m,\sigma)$ that will be accepted by a receiver R. The success probability of this attack denoted by $P_{S_O}^{(GA)}(S_i)$ is defined as*

$$P_{S_O}^{(GA)}(S_i) := \max_{(m',\sigma')} \max_{(m,\sigma)\neq(m',\sigma')} \Pr(R \textit{ accepts } (m',\sigma') \mid (m,\sigma)).$$

Then, $P_{S_O}^{(GA)}$ is defined as $P_{S_O}^{(GA)} := \max_{S_i \in \mathcal{S}} P_{S_O}^{(GA)}(S_i)$.

(ii) ***Attacks by** $S(i_1,\ldots,i_k)$**:** In this attack, a group of malicious senders $S(i_1,\ldots,i_k)$ tries to trump up an authenticated message from the sender $S_i \in \mathcal{S} \setminus S(i_1,\ldots,i_k)$. Let $P_S^{(GA)} := \max(P_{I_S}^{(GA)}, P_{S_S}^{(GA)})$, where $P_{I_S}^{(GA)}$ and $P_{S_S}^{(GA)}$ are given as follows.*

Impersonation attack**:** *$S(i_1,\ldots,i_k)$ tries to generate a fraudulent authenticated message (m,σ) such that the receiver R accepts it and someone in $\mathcal{S} \setminus S(i_1,\ldots,i_k)$ is detected as the sender of it. The success probability of this attack is denoted by $P_{I_S}^{(GA)}$ is defined as*

$$P_{I_S}^{(GA)}(S(i_1,\ldots,i_k)) := \max_{ak_{S(i_1,\ldots,i_k)}} \max_{(m,\sigma)} \Pr(R \textit{ accepts } (m,\sigma) \ \wedge \textit{someone in } \mathcal{S} \setminus S(i_1,\ldots,i_k) \textit{ is detected as the sender of } (m,\sigma) \mid ak_{S(i_1,\ldots,i_k)}).$$

Then, we define $P_{I_S}^{(GA)} := \max_{S(i_1,\ldots,i_k)\in\tilde{\mathcal{W}}} P_{I_S}^{(GA)}(S(i_1,\ldots,\, i_k))$.

Substitution attack**:** *$S(i_1,\ldots,i_k)$ can observe a transmitted authenticated message (m,σ) which is generated by $S_i \in \mathcal{S} \setminus S(i_1,\ldots,i_k)$, and then tries to generate a fraudulent one (m',σ') such that the receiver R accepts it and someone in $\mathcal{S} \setminus S(i_1,\ldots,i_k)$ is detected as* *the sender of it. The success probability of this attack is denoted by* $P_{S_S}^{(GA)}(S(i_1,\ldots,i_k),S_i)$ *is defined as*

$$P_{S_S}^{(GA)}(S(i_1,\ldots,i_k),S_i) := \max_{ak_{S(i_1,\ldots,i_k)}} \max_{(m',\sigma')} \max_{(m,\sigma)\neq(m',\sigma')} \Pr(R \textit{ accepts } (m',\sigma') \ \wedge \textit{someone in } \mathcal{S}\setminus S(i_1,\ldots,i_k) \textit{ is detected as the sender of } (m',\sigma') \mid ak_{S(i_1,\ldots,i_k)},(m,\sigma)).$$

Then, $P_{S_S}^{(GA)}$ *is defined as*

$$P_{S_S}^{(GA)} := \max_{S(i_1,\ldots,i_k)\in\tilde{\mathcal{W}}} \max_{S_i\in\mathcal{S}\setminus S(i_1,\ldots,i_k)} P_{S_S}^{(GA)}(S(i_1,\ldots,i_k),S_i).$$

As in A-codes, in GA-codes it must be assumed that all entities are honest players, however, it may be unnatural and an ideal assumption in many situations. In the next section, we will propose an extension of GA-codes based on a more natural assumption, and we call it GA^2-code (GA-code with Arbitration).

3. GA^2-codes: The Model and Security Definition

3.1. The model

In this section, we introduce a model of GA^2-codes. In GA^2-codes, there are the following entities: n senders S_1, S_2, …, S_n, a receiver R, a group authority G, an arbiter A, and a trusted initializer TI, where n is a positive integer. For convenience, as in GA-codes, for each sender $S_i \in \{S_1,S_2,\ldots,S_n\}$ we use the same symbol S_i to denote the identity of the sender. Once being given secret information, S_i can generate an authenticator by using his secret information and a message, and R can verify it by using his secret information. Additionally, by cooperating with G, R can obtain the identity of the sender of it. In the case of dispute between S_i and R, A can resolve the dispute by using his secret information. A formal definition is given as follows.

Definition 5 (GA^2-code). *A GA^2-code (GA-code with Arbitration)* Π *involves* $n+4$ *entities,* TI*,* S_1*,* S_2*, …,* S_n*,* R*,* G *and* A*, and consists of six algorithms (GGen, GSign, GVer, GOpen, AVer, AOpen) with* $n+5$ *spaces* $\mathcal{M}$*,* $\mathcal{E}_{S_1}$*, …,* $\mathcal{E}_{S_n}$*,* $\mathcal{E}_R$*,* $\mathcal{E}_G$*,* $\mathcal{E}_A$*, and* Σ*, where all of the above algorithms except GGen are deterministic and all of the above spaces are finite. In addition,* Π *is executed with five phases as follows.*

– *Notation.*

  - *Entities:* TI *is a trusted initializer,* S_i $(1 \le i \le n)$ *is a sender. Let* $\mathcal{S} := \{S_1,S_2,\ldots,S_n\}$ *be a set of senders. And,* R *is a receiver,* G *is a group authority,* A *is an arbiter.*

- *Spaces: $\mathcal{M}$ is a finite set of possible messages, $\mathcal{E}_{S_1}, \ldots, \mathcal{E}_{S_n}$ are finite sets of possible keys of senders $S_1, \ldots, S_n$, respectively. $\mathcal{E}_R$ is a finite set of possible receiver's secret keys, $\mathcal{E}_G$ is a finite set of possible group authority's secret keys, and $\mathcal{E}_A$ is a finite set of possible arbiter's secret keys. Σ is a finite set of possible authenticators.*
- *Algorithms: GGen is a key generation algorithm, GSign: $\mathcal{E}_{S_i} \times \mathcal{M} \to \Sigma$ is an authenticator generation algorithm which outputs an authenticator message, and GVer: $\mathcal{E}_R \times \mathcal{M} \times \Sigma \to \{valid, invalid\}$ is a verification algorithm for the receiver. GOpen: $\mathcal{E}_R \times \mathcal{E}_G \times \mathcal{M} \times \Sigma \to \mathcal{S} \cup \{\perp\}$ is an open algorithm for the group authority and the receiver, where $\perp$ implies the invalid symbol, AVer: $\mathcal{E}_A \times \mathcal{M} \times \Sigma \to \{valid, invalid\}$ is a verification algorithm for the arbiter, and AOpen: $\mathcal{E}_A \times \mathcal{E}_G \times \mathcal{M} \times \Sigma \to \mathcal{S} \cup \{\perp\}$ is an open algorithm for the group authority and the arbiter.*

1. ***Key Generation and Distribution by** TI. In the initial phase, TI generates the following keys by using GGen: a secret key $e_{S_i} \in \mathcal{E}_{S_i}$ for S_i $(1 \leq i \leq n)$, a secret key $e_R \in \mathcal{E}_R$ for R, a secret key $e_G \in \mathcal{E}_G$ for G, and a secret key $e_A \in \mathcal{E}_A$ for A. These keys are distributed to corresponding entities via secure channels. After distributing these keys, TI deletes these keys from his memory, and each entity keeps his own key secret.*

2. ***Authenticator Generation.** In order to send a message $m \in \mathcal{M}$ to R with authenticity and anonymity, $S_i \in \mathcal{S}$ generates an authenticator σ by using his key e_{S_i} and m, that is $\sigma = GSign(e_{S_i}, m)$, and transmits (m, σ) to R.*

3. ***Verification.** R verifies the validity of (m, σ) by using e_R. If $GVer(e_R, (m, \sigma)) = valid$ then R accepts it, and otherwise R rejects it.*

4. ***Tracing.** If R wants to reveal the identity of the sender of (m, σ), R can obtain it by cooperating with G if G approves R's request, that is $GOpen(e_R, e_G, (m, \sigma)) = S_i$, where $\sigma = GSign(e_{S_i}, m)$.*

5. ***Arbitration.** In the case of dispute between S_i and R, A can resolve the dispute based on the following judgment by using his secret key e_A.*

   (1) Cooperating with G, R ascribes an authenticated message (m, σ) to S_i, but S_i denies it. Then, S_i or R asks for arbitration.

   - *R wins if A accept (i.e. $AVer(e_A, (m, \sigma)) = valid$) and can reveal the identity of the sender S_i from (m, σ) by cooperating with G (i.e. $AOpen(e_A, e_G, (m, \sigma)) = S_i$).*
   - *R loses otherwise.*

   (2) S_i produces (m, σ) such that R will accept it. After having sent it to R, S_i attempts to deny having created (m, σ). Then, S_i or R asks for arbitration.

- *S_i wins if A rejects (m,σ) (i.e. $AVer(e_A,(m,\sigma)) = invalid$).*
- *S_i loses otherwise.*

(3) After knowing that R rejected (m,σ), S_i claims that (m,σ) is valid. Then, S_i or R asks for arbitration.

- *S_i wins if A accepts (m,σ) (i.e. $AVer(e_A,(m,\sigma)) = valid$).*
- *S_i loses otherwise.*

In the above model, for simplicity we assume the following conditions: it is allowed to generate an authenticator and transmit an authenticated message among senders only once; both the receiver and the arbiter are allowed to verify an authenticated message at most one time; and the group authority is allowed to reply to a request only at most one time.

3.2. Adversarial model and security definition

In this section, we define a security definition of GA^2-codes. In GA^2-codes, the arbiter is assumed to be always honest. As in A^2-codes, an adversary can perform impersonation attacks, substitution attacks, denial attacks or claim attacks by creating a fraudulent an authenticated message. These attacks are the same as those in A^2-codes. We now classify the attacks according to adversary's types: An outsider O who can only have access to public information, a group of k malicious senders, a dishonest receiver R and possible collusion of them. Here, we assume that a group authority is honest, and we do not consider colluding attacks including the outsider, because the outsider has no secret-key information. As in GA-codes, we denote a group of k $(1 \le k \le n-1)$ malicious senders by $S(i_1,\ldots,i_k) := \{S_{i_1},\ldots,S_{i_k}\}$ and their secret information by $e_{S(i_1,\ldots,i_k)}$. Also let $\mathcal{W} := \{S(i_1,\ldots,i_k) \mid S(i_1,\ldots,i_k) \subset \mathcal{S}\}$. Then, we give a formal security definition of GA^2-code below.

Definition 6 (Security of GA^2-code). *Let Π be a GA^2-code in the one-time model. The scheme Π is said to be (p,k,n)-one-time secure, if the following conditions are satisfied.*

1) Each of R, A and G obtains no information on the identity of the sender from an authenticated message alone. Namely, the following conditions are satisfied: For any $i \in \{1,2,\ldots,n\}$, we have

$$a)\ \max_{(m,\sigma)} \max_{e_R} |\Pr(S_i \mid e_R,(m,\sigma)) - \Pr(S_i \mid e_R)| = 0;$$

$$b)\ \max_{(m,\sigma)} \max_{e_A} |\Pr(S_i \mid e_A,(m,\sigma)) - \Pr(S_i \mid e_A)| = 0; \textit{and}$$

$$c)\ \max_{(m,\sigma)} \max_{e_G} |\Pr(S_i \mid e_G,(m,\sigma)) - \Pr(S_i \mid e_G)| = 0.$$

The above equations mean that, after distributing secret-keys e_R, e_A, e_G, each *of R, A and G obtains no information on the identity of the sender from arbitrary (m, σ), where σ is taken such that $\sigma = GSign(e_{S_i}, m)$ for some e_{S_i} and m.*

2) No information on the identity of the sender of (m, σ) is leaked from (m, σ) itself against the following adversaries: (i) malicious senders $S(i_1, \ldots, i_k)$; and (ii) the collusion between malicious senders $S(i_1, \ldots, i_k)$ and the malicious receiver R. Namely, for any $S(i_1, \ldots, i_k) \in \mathcal{W}$ and $S_i \in \mathcal{S} \setminus S(i_1, \ldots, i_k)$, we have

a) $\max\limits_{(m,\sigma)} \max\limits_{e_{S(i_1,\ldots,i_k)}} \left| \Pr(S_i \mid e_{S(i_1,\ldots,i_k)}, (m, \sigma)) - \Pr(S_i \mid e_{S(i_1,\ldots,i_k)}) \right| = 0;$ *and*

b) $\max\limits_{(m,\sigma)} \max\limits_{e_{S(i_1,\ldots,i_k)}} \max\limits_{e_R} \left| \Pr(S_i \mid e_{S(i_1,\ldots,i_k)}, e_R, (m, \sigma)) - \Pr(S_i \mid e_{S(i_1,\ldots,i_k)}, e_R) \right| = 0.$

3) All of the success probabilities of the following attacks, $P_O^{(GA^2)}, P_S^{(GA^2)}, P_D^{(GA^2)}, P_C^{(GA^2)}, P_R^{(GA^2)}$ and $P_{SR}^{(GA^2)}$, are at most $p \in [0, 1]$.

(i) ***Attacks by*** O*: In this attack, the outsider O tries to trap the receiver R. Let $P_O^{(GA^2)} := \max(P_{I_O}^{(GA^2)}, P_{S_O}^{(GA^2)})$, where $P_{I_O}^{(GA^2)}$ and $P_{S_O}^{(GA^2)}$ are given as follows.*

Impersonation attack**:** *O tries to generate a fraudulent authenticated message (m, σ) that will be accepted by a receiver R. The success probability of this attack denoted by $P_{I_O}^{(GA^2)}$ is defined as*

$$P_{I_O}^{(GA^2)} := \max_{(m,\sigma)} \Pr(R \textit{ accepts } (m, \sigma)).$$

Substitution attack**:** *O can observe a transmitted authenticated message (m, σ) which is generated by one of the senders S_i, and then tries to generate a fraudulent one $(m', \sigma') \neq (m, \sigma)$ that will be accepted by a receiver R. The success probability of this attack denoted by $P_{S_O}^{(GA^2)}(S_i)$ is defined as*

$$P_{S_O}^{(GA^2)}(S_i) := \max_{(m',\sigma')} \max_{(m,\sigma) \neq (m',\sigma')} \Pr(R \textit{ accepts } (m', \sigma') \mid (m, \sigma)).$$

Then, $P_{S_O}^{(GA^2)}$ is defined as $P_{S_O}^{(GA^2)} := \max\limits_{S_i \in \mathcal{S}} P_{S_O}^{(GA^2)}(S_i)$.

(ii) ***Attacks by*** $S(i_1, \ldots, i_k)$*: In this attack, we consider the following three cases.*

(1) A group of malicious senders $S(i_1, \ldots, i_k)$ tries to trump up an authenticated message from some honest sender $S_i \in \mathcal{S} \setminus S(i_1, \ldots, i_k)$.

Let $P_S^{(GA^2)} := \max(P_{I_S}^{(GA^2)}, P_{S_S}^{(GA^2)})$*, where* $P_{I_S}^{(GA^2)}$ *and* $P_{S_S}^{(GA^2)}$ *are given as follows.*

Impersonation attack: $S(i_1, \ldots, i_k)$ *tries to generate a fraudulent authenticated message* (m, σ) *such that both* R *and* A *accept it and someone in* $\mathcal{S} \setminus S(i_1, \ldots, i_k)$ *is detected as the sender of it. The success probability of this attack is denoted by* $P_{I_S}^{(GA^2)}$ *is defined as*

$$P_{I_S}^{(GA^2)}(S(i_1, \ldots, i_k)) := \max_{e_{S(i_1,\ldots,i_k)}} \max_{(m,\sigma)}$$

$$\Pr(R \textit{ and } A \textit{ accept } (m, \sigma) \ \wedge \textit{someone in } \mathcal{S} \setminus S(i_1, \ldots, i_k)$$
$$\textit{is detected as the sender of } (m, \sigma) \mid e_{S(i_1,\ldots,i_k)}).$$

Then, we define $P_{I_S}^{(GA^2)} := \max_{S(i_1,\ldots,i_k) \in \mathcal{W}} P_{I_S}^{(GA^2)}(S(i_1, \ldots, i_k))$.

Substitution attack: $S(i_1, \ldots, i_k)$ *can observe a transmitted authenticated message* (m, σ) *which is generated by* $S_i \in \mathcal{S} \setminus S(i_1, \ldots, i_k)$*, and then tries to generate a fraudulent one* (m', σ') *such that both* R *and* A *accept it and someone in* $\mathcal{S} \setminus S(i_1, \ldots, i_k)$ *is detected as the sender of it. The success probability of this attack is denoted by* $P_{S_S}^{(GA^2)}(S(i_1, \ldots, i_k), S_i)$ *is defined as*

$$P_{S_S}^{(GA^2)}(S(i_1, \ldots, i_k), S_i) := \max_{e_{S(i_1,\ldots,i_k)}} \max_{(m',\sigma')} \max_{(m,\sigma) \neq (m',\sigma')}$$

$$\Pr(R \textit{ and } A \textit{ accept } (m', \sigma') \ \wedge \textit{someone in } \mathcal{S} \setminus S(i_1, \ldots, i_k)$$
$$\textit{is detected as the sender of } (m', \sigma') \mid e_{S(i_1,\ldots,i_k)}, (m, \sigma)).$$

Then, $P_{S_S}^{(GA^2)}$ *is defined as*

$$P_{S_S}^{(GA^2)} := \max_{S(i_1,\ldots,i_k) \in \mathcal{W}} \max_{S_i \in \mathcal{S} \setminus S(i_1,\ldots,i_k)} P_{S_S}^{(GA^2)}(S(i_1, \ldots, i_k), S_i).$$

(2) After sending an authenticated message to the receiver R*, the malicious senders* $S(i_1, \ldots, i_k)$ *tries to deny having sent it. Let* $P_D^{(GA^2)} := \max(P_{I_D}^{(GA^2)}, P_{S_D}^{(GA^2)})$*, where* $P_{I_D}^{(GA^2)}$ *and* $P_{S_D}^{(GA^2)}$ *are given as follows.*

Denial attack without legal authenticated messages: $S(i_1, \ldots, i_k)$ *tries to generate* (m, σ) *such that* R *accepts it and* A *rejects it (i.e.,* $S(i_1, \ldots, i_k)$ *wins in the arbitration). The success probability of this attack denoted by* $P_{I_D}^{(GA^2)}(S(i_1, \ldots, i_k))$ *is defined as*

$$P_{I_D}^{(GA^2)}(S(i_1, \ldots, i_k)) :=$$

$$\max_{e_{S(i_1,\ldots,i_k)}} \max_{(m,\sigma)} \Pr(R \textit{ accepts } (m,\sigma) \wedge A \textit{ rejects } (m,\sigma) \mid e_{S(i_1,\ldots,i_k)}).$$

Then, we define $P_{I_D}^{(GA^2)} := \max_{S(i_1,\ldots,i_k)\in\mathcal{W}} P_{I_D}^{(GA^2)}(S(i_1,\ldots,i_k))$.

Denial attack with legal authenticated messages: $S(i_1,\ldots,i_k)$ *can observe a transmitted authenticated message* (m,σ) *which is generated by* $S_i \in \mathcal{S} \setminus S(i_1,\ldots,i_k)$*, and then tries to generate* (m',σ') *such that* R *accepts it and* A *rejects it (i.e.,* $S(i_1,\ldots,i_k)$ *wins in the arbitration). The success probability of this attack denoted by* $P_{S_D}^{(GA^2)}(S(i_1,\ldots,i_k),S_i)$ *is defined as*

$$P_{S_D}^{(GA^2)}(S(i_1,\ldots,i_k),S_i) := \max_{e_{S(i_1,\ldots,i_k)}} \max_{(m',\sigma')} \max_{(m,\sigma)\neq(m',\sigma')} \Pr(R \textit{ accepts } (m',\sigma') \wedge A \textit{ rejects } (m',\sigma') \mid e_{S(i_1,\ldots,i_k)}, (m,\sigma)).$$

Then, $P_{S_D}^{(GA^2)}$ *is defined as*

$$P_{S_D}^{(GA^2)} := \max_{S(i_1,\ldots,i_k)\in\mathcal{W}} \max_{S_i\in\mathcal{S}\setminus S(i_1,\ldots,i_k)} P_{S_D}^{(GA^2)}(S(i_1,\ldots,i_k),S_i).$$

(3) After knowing that R *has rejected an authenticated message,* $S(i_1,\ldots,i_k)$ *tries to claim that it is valid. Let* $P_C^{(GA^2)} := \max(P_{I_C}^{(GA^2)}, P_{S_C}^{(GA^2)})$*, where* $P_{I_C}^{(GA^2)}$ *and* $P_{S_C}^{(GA^2)}$ *are given as follows.*

Claim attack without legal authenticated messages: $S(i_1,\ldots,i_k)$ *tries to generate* (m,σ) *such that* R *rejects it and* A *accepts it (i.e.,* $S(i_1,\ldots,i_k)$ *wins in the arbitration). The success probability of this attack denoted by* $P_{I_C}^{(GA^2)}(S(i_1,\ldots,i_k))$ *is defined as*

$$P_{I_C}^{(GA^2)}(S(i_1,\ldots,i_k)) := \max_{e_{S(i_1,\ldots,i_k)}} \max_{(m,\sigma)} \Pr(R \textit{ rejects } (m,\sigma) \wedge A \textit{ accepts } (m,\sigma) \mid e_{S(i_1,\ldots,i_k)}).$$

Then, we define $P_{I_C}^{(GA^2)} := \max_{S(i_1,\ldots,i_k)\in\mathcal{W}} P_{I_C}^{(GA^2)}(S(i_1,\ldots,i_k))$.

Claim attack with legal authenticated messages: $S(i_1,\ldots,i_k)$ *can observe a transmitted authenticated message* (m,σ) *which is generated by* $S_i \in \mathcal{S}\setminus S(i_1,\ldots,i_k)$*, and then tries to generate* (m',σ') *such that* R *rejects it and* A *accepts it (i.e.,* $S(i_1,\ldots,i_k)$ *wins in the arbitration). The success probability of this attack denoted by*

$P_{S_C}^{(GA^2)}(S(i_1,\ldots,i_k),S_i)$ *is defined as*

$$P_{S_C}^{(GA^2)}(S(i_1,\ldots,i_k),S_i) := \max_{e_{S(i_1,\ldots,i_k)}} \max_{(m',\sigma')} \max_{(m,\sigma)\neq(m',\sigma')} \Pr(R \textit{ rejects } (m',\sigma') \wedge A \textit{ accepts } (m',\sigma') \mid e_{S(i_1,\ldots,i_k)}, (m,\sigma)).$$

Then, $P_{S_C}^{(GA^2)}$ *is defined as*

$$P_{S_C}^{(GA^2)} := \max_{S(i_1,\ldots,i_k)\in\mathcal{W}} \max_{S_i\in\mathcal{S}\setminus S(i_1,\ldots,i_k)} P_{S_C}^{(GA^2)}(S(i_1,\ldots,i_k),S_i).$$

(iii) ***Attacks by*** R*: The malicious receiver* R *tries to trump up an authenticated message from some honest sender. Let* $P_R^{(GA^2)} := \max(P_{I_R}^{(GA^2)}, P_{S_R}^{(GA^2)})$*, where* $P_{I_R}^{(GA^2)}$ *and* $P_{S_R}^{(GA^2)}$ *are given as follows.*

Impersonation attack: R *tries to generate a fraudulent authenticated message* (m,σ) *such that* A *accepts it and someone of senders is detected as the sender of* (m,σ)*. The success probability of this attack denoted by* $P_{I_R}^{(GA^2)}$ *is defined as*

$$P_{I_R}^{(GA^2)} := \max_{e_R} \max_{(m,\sigma)} \Pr(A \textit{ accepts } (m,\sigma) \wedge \textit{ someone in } \mathcal{S} \textit{ is detected as the sender of } (m,\sigma) \mid e_R).$$

Substitution attack*:* R *can observe a transmitted authenticated message* (m,σ) *which is generated by* S_i*, and then tries to generate a fraudulent one* $(m',\sigma') \neq (m,\sigma)$ *such that* A *accepts it and someone of senders is detected as the sender of* (m',σ')*. The success probability of this attack denoted by* $P_{S_R}^{(GA^2)}(S_i)$ *is defined as*

$$P_{S_R}^{(GA^2)}(S_i) := \max_{e_R} \max_{(m,\sigma)} \max_{(m',\sigma')\neq(m,\sigma)} \Pr(A \textit{ accepts } (m',\sigma') \wedge \textit{ someone in } \mathcal{S} \textit{ is detected as the sender of } (m',\sigma') \mid e_R, (m,\sigma)).$$

Then, $P_{S_R}^{(GA^2)}$ *is defined as* $P_{S_R}^{(GA^2)} := \max_{S_i\in\mathcal{S}} P_{S_R}^{(GA^2)}(S_i)$

(iv) ***Collusion-attacks by*** $S(i_1,\ldots,i_k)$ ***and*** R*: The malicious senders* $S(i_1,\ldots,i_k)$ *and the receiver* R *collude together and try to trump up an authenticated message from some honest sender. Let* $P_{SR}^{(GA^2)} := \max(P_{I_{SR}}^{(GA^2)}, P_{S_{SR}}^{(GA^2)})$*, where* $P_{I_{SR}}^{(GA^2)}$ *and* $P_{S_{SR}}^{(GA^2)}$ *are given as follows.*

Impersonation attack*:* $S(i_1,\ldots,i_k)$ *and* R *try to generate a fraudulent authenticated message* (m,σ) *such that* A *accepts it and someone in* $\mathcal{S}\setminus S(i_1,\ldots,i_k)$ *is detected as the sender of it. The success probability* *of this attack denoted by* $P_{I_{SR}}^{(GA^2)}(S(i_1,\ldots,i_k))$ *is defined as*

$$P_{I_{SR}}^{(GA^2)}(S(i_1,\ldots,i_k)) := \max_{e_{S(i_1,\ldots,i_k)}} \max_{e_R} \max_{(m,\sigma)} \Pr(A \textit{ accepts } (m,\sigma) \ \wedge \textit{someone in } \mathcal{S} \setminus S(i_1,\ldots,i_k) \textit{ is detected as the sender of } (m,\sigma) \mid e_{S(i_1,\ldots,i_k)}, e_R).$$

Then, $P_{I_{SR}}^{(GA^2)}$ *is defined as* $P_{I_{SR}}^{(GA^2)} := \max_{S(i_1,\ldots,i_k)\in\mathcal{W}} P_{I_{SR}}^{(GA^2)}(S(i_1,\ldots,i_k))$.

Substitution attack*:* $S(i_1,\ldots,i_k)$ *and* R *can observe a transmitted authenticated message* (m,σ) *which is generated by* S_i*, and then try to generate a fraudulent one* $(m',\sigma') \neq (m,\sigma)$ *such that* A *accepts it and someone in* $\mathcal{S} \setminus S(i_1,\ldots,i_k)$ *is detected as the sender of it. The success probability of this attack denoted by* $P_{S_{SR}}^{(GA^2)}$ *is defined as*

$$P_{S_{SR}}^{(GA^2)}(S(i_1,\ldots,i_k),S_i) := \max_{e_{S(i_1,\ldots,i_k)}} \max_{e_R} \max_{(m,\sigma)} \max_{(m',\sigma')\neq(m\sigma)} \Pr(A \textit{ accepts } (m',\sigma') \ \wedge \textit{someone in } \mathcal{S} \setminus S(i_1,\ldots,i_k) \textit{ is detected as the sender of } (m',\sigma') \mid e_{S(i_1,\ldots,i_k)}, e_R, (m,\sigma)).$$

Then, $P_{S_{SR}}^{(GA^2)}$ *is defined as*

$$P_{S_{SR}}^{(GA^2)} := \max_{S(i_1,\ldots,i_k)\in\mathcal{W}} \max_{S_i\in\mathcal{S}\setminus S(i_1,\ldots,i_k)} P_{S_{SR}}^{(GA^2)}(S(i_1,\ldots,i_k),S_i).$$

4. GA^2-codes: Construction

In this section, we propose a construction of the one-time secure GA^2-code based on polynomials over finite fields. We show our construction method by combining the A^2-code and bijective mappings. This idea is similar to that of GA-codes in [**5**]. In the following, the finite field with q elements is denoted by $GF(q)$, where q is a prime power and $q \geq n$. In addition to this, the degree of x_i in a multivariable polynomial $f(x_1,\ldots,x_n)$ is denoted by $\deg_{x_i} f$, and in particular, the degree of a polynomial $f(x)$ with one variable x is simply denoted by $\deg f$.

1. **Key Generation and Distribution by** TI: Let $\mathcal{M} = GF(q) \setminus \{0\}$. TI chooses uniformly at random four polynomials $f_d(x)$ and $g_d(x)$ $(d = 0,1)$ over $GF(q)$ with one variable x, in which the degree of x is at most $k+1$. TI also chooses $v_R, v_A \in GF(q)$ uniformly at random. Also, TI chooses distinct numbers β_i $(i = 1,2,\ldots,n)$ from $GF(q)$ uniformly at random such that $f_0(\beta_i) + f_1(\beta_i)v_R \neq f_0(\beta_j) + f_1(\beta_j)v_R$ and $f_0(\beta_i) + f_1(\beta_i)v_A \neq f_0(\beta_j) + f_1(\beta_j)v_A$ for any i,j with $1 \leq i < j \leq n$. TI randomly generates two bijective mappings $\pi_1 : GF(q) \to \mathcal{S}$ and $\pi_2 : GF(q) \to \mathcal{S}$ such that

$\pi_1(f_0(\beta_i) + f_1(\beta_i)v_R) = S_i$ and $\pi_2(f_0(\beta_i) + f_1(\beta_i)v_A) = S_i$ for any i. TI constructs a polynomial $F(x, y, z) := \sum_{i=0}^{1}(f_i(x) + zg_i(x))y^i$. Next, TI gives $e_{S_i} := (\beta_i, F(\beta_i, y, z))$, $e_R := (v_R, F(x, v_R, z))$, $e_A := (v_A, F(x, v_A, z))$, and $e_G := (\pi_1, \pi_2)$ to S_i, R, A, and G, respectively, via secure channels. After distributing those keys, TI deletes his memory.

2. **Authenticator Generation**: For $m \in \mathcal{M}$, S_i generates an authenticator σ by $\sigma = (\beta_i, h(y))$, where $h(y) := F(\beta_i, y, z)|_{z=m}$.
3. **Verification**: R accepts (m, σ) as valid if and only if $h(y)|_{y=v_R} = F(x, v_R, z)|_{x=\beta_i, z=m}$.
4. **Tracing**: When R wants to reveal the identity of the sender of (m, σ), R first sends a request to G. If R's request is approved by G, R transmits $F(\beta_i, v_R, 0)$ via a secure channel. Then, G reveals the sender's identity by $S_i = \pi_1(F(\beta_i, v_R, 0))$ and transmits this result back to R.
5. **Arbitration**.

   (1) Cooperating with G, R ascribes an authenticated message (m, σ) to S_i, but S_i denies it. Then, S_i or R asks for arbitration.

   - R wins if $h(y)|_{y=v_A} = F(x, v_A, z)|_{x=\beta_i, z=m}$ and $S_i = \pi_2(F(\beta_i, v_A, 0))$.
   - R loses otherwise.

   (2) S_i produces (m, σ) such that R will accept it. After having sent it to R, S_i attempts to deny having created (m, σ). Then, S_i or R asks for arbitration.

   - S_i wins if $h(y)|_{y=v_A} \neq F(x, v_A, z)|_{x=\beta_i, z=m}$.
   - S_i loses otherwise.

   (3) After knowing that R has rejected (m, σ), S_i claims that (m, σ) is valid. Then, S_i or R asks for arbitration.

   - S_i wins if $h(y)|_{y=v_A} = F(x, v_A, z)|_{x=\beta_i, z=m}$.
   - S_i loses otherwise.

The following theorem shows that the above construction meets our security definition of GA^2-codes.

THEOREM 1. *The above construction results in $(1/q, k, n)$-one-time secure GA^2-code requiring the following memory sizes:*

$$|\Sigma| = nq^2, \quad |\mathcal{E}_{S_i}| = nq^4 \text{ for } i = 1, 2, \ldots, n,$$
$$|\mathcal{E}_R| = |\mathcal{E}_A| = q^{2k+5}, \quad |\mathcal{E}_G| = (n!)^2.$$

Proof. To complete the proof of Theorem 1, we show the following lemmas.

Lemma 1. *For any $f(y), g(y) \in GF(q)[y]$ such that $\deg f \leq 1$, $\deg g \leq 1$ and $g(y) \neq f(y)$, the probability that $g(v) = f(v)$ for randomly chosen $v \in GF(q)$ is at most $1/q$.*

Proof. The probability that $g(v) = f(v)$ for randomly chosen $v \in GF(q)$ is

$$\begin{aligned}&\frac{|\{v \in GF(q) \mid g(y) \neq f(y) \wedge g(v) = f(v)\}|}{|\{v \in GF(q)\}|}\\ =&\frac{|\{v \in GF(q) \mid G(y) \neq 0 \wedge G(v) = 0 \wedge \deg G \leq 1\}|}{|\{v \in GF(q)\}|}\\ \leq&\frac{1}{q},\end{aligned}$$

where $G(y) := g(y) - f(y)$. This completes the proof. □

Lemma 2. *In the above construction, it holds that*

$$\max(P_{I_O}^{(GA^2)}, P_{I_S}^{(GA^2)}, P_{I_R}^{(GA^2)}, P_{I_{SR}}^{(GA^2)}) \leq \frac{1}{q}, \text{ and}$$
$$\max(P_{S_O}^{(GA^2)}, P_{S_S}^{(GA^2)}, P_{S_R}^{(GA^2)}, P_{S_{SR}}^{(GA^2)}) \leq \frac{1}{q}.$$

Proof. We show $P_{S_{SR}}^{(GA^2)} \leq 1/q$. To succeed in substitution attacks, the colluders consisting of $S(i_1, \ldots, i_k)$ and R try to create a fraudulent authenticated message $(m', \sigma') = (m', \beta_i, \tilde{h}(y))$ which A will accept, after observing a valid one $(m, \sigma) = (m, \beta_{i_0}, h(y))$ with $(m', \sigma') \neq (m, \sigma)$, where $\beta_i, \beta_{i_0} \notin \{\beta_{i_1}, \ldots, \beta_{i_k}\}$ and σ is generated by $S_{i_0} \notin S(i_1, \ldots, i_k)$. We consider probability of guessing $F(\beta_i, v_A, m')$ from information that the colluders have. Then, we consider two cases: (i) $\beta_i = \beta_{i_0}$ and $m' \neq m$; (ii) $\beta_i \neq \beta_{i_0}$. First, we consider the case (i). $F(\beta_i, y, m') = (g_0(\beta_i) + g_1(\beta_i)y)(m' - m) + h(y)$ and the colluders try to guess the polynomial $g_0(\beta_i) + g_1(\beta_i)y$ from their information $F(\beta_{i_1}, y, z), \ldots, F(\beta_{i_k}, y, z)$. However, $\deg_x F(x, y, z) \leq k + 1$ and the number of information on $F(x, y, z)$ which the colluders have is at most k. Therefore, they cannot guess $g_0(\beta_i) + g_1(\beta_i)y$ with probability more than $1/q$, and hence cannot guess such $F(\beta_i, v_A, m')$ with probability more than $1/q$. Next, we consider the case (ii). Then, the colluders try to guess the polynomial $F(\beta_i, y, m')$ from their k information $F(\beta_{i_1}, y, m'), \ldots, F(\beta_{i_k}, y, m')$ and observed information $h(y) = F(\beta_{i_0}, y, m)$. However, $\deg_x F(x, y, z) \leq k+1$ and the number of information on $F(x, y, z)$ which the colluders have is at most $k + 1$. Therefore, they cannot guess $F(\beta_i, y, m')$ and hence $F(\beta_i, v_A, m')$ with probability more than $1/q$. From the above discussion, it follows that the success probability of substitution attacks is at most $1/q$.

In a manner similar to the above one, we can also prove that $P_{S_O}^{(GA^2)}$, $P_{S_S}^{(GA^2)}$, and $P_{S_R}^{(GA^2)}$ are at most $1/q$. In addition, it is shown that all kinds of impersonation attacks are at most $1/q$ in a similar way. □

Lemma 3. *In the above construction, $P_D^{(GA^2)} \leq 1/q$.*

Proof. First, we show $P_{S_D}^{(GA^2)} \leq 1/q$. To succeed in the denial attacks, any set of colluders $S(i_1, \ldots, i_k)$ tries to produce a fraudulent authenticated message $(m', \sigma') = (m', \beta_i, \tilde{h}(y))$ which R will accept, but A will not, after observing a valid one $(m, \sigma) = (m, \beta_{i_0}, h(y))$, where $\beta_{i_0} \notin \{\beta_{i_1}, \ldots, \beta_{i_k}\}$. Namely, the colluders try to find a polynomial $\tilde{h}(y)$ that satisfies the following conditions:

$$\tilde{h}(y)|_{y=v_R} = F(\beta_i, y, m')|_{y=v_R} \tag{1}$$

$$\tilde{h}(y)|_{y=v_A} \neq F(\beta_i, y, m')|_{y=v_A} \tag{2}$$

In particular, the second condition (2) implies that the colluders have to find $\tilde{h}(y)$ such that $\tilde{h}(y) \neq F(\beta_i, y, m')$. Here, we note that the colluders can know $F(\beta_i, y, m')$ since $\beta_i \in \{\beta_{i_1}, \ldots, \beta_{i_k}\}$. However, since the colluders do not know R's secret information v_R, they cannot create $\tilde{h}(y)$ such that $\tilde{h}(y) \neq F(\beta_i, y, m')$ and $\tilde{h}(v_R) = F(\beta_i, v_R, m')$ (i.e., condition (1)) with the probability more than $1/q$, even if they have the information $h(y) = F(\beta_{i_0}, y, m)$. This follows from Lemma 1 by applying $f(y) := F(\beta_i, y, m')$, $g(y) := \tilde{h}(y)$ and $v := v_R$. Therefore, the success probability of the denial attack, $P_{S_D}^{(GA^2)}$, is at most $1/q$. Similarly, we can also prove $P_{I_D}^{(GA^2)} \leq 1/q$. Hence, $P_D^{(GA^2)} \leq 1/q$. □

Lemma 4. *In the above construction, $P_C^{(GA^2)} \leq 1/q$.*

Proof. Since v_R and v_A are constructed in a similar way, it is easy to show that the statement is true by Lemma 3. □

Lemma 5. *In the above construction, each of $S(i_1, \ldots, i_k)$, R, A and G obtains no information on the identity of the sender of (m, σ) from (m, σ) itself and own secret information. Furthermore, even if malicious senders $S(i_1, \ldots, i_k)$ collude with the malicious receiver R, they cannot get any information on that. If (m, σ) is valid, R and A can reveal the identity of the sender of (m, σ) by cooperating with G with probability* 1*, respectively.*

Proof. First of all, we prove that each of R, A and G cannot obtain any information on the identity of the sender of (m, σ) alone. Namely, we prove the following:

(a) $\max_{(m,\sigma)} \max_{e_R} |\Pr(S_i \mid e_R, (m, \sigma)) - \Pr(S_i \mid e_R)| = 0;$

(b) $\max_{(m,\sigma)} \max_{e_A} |\Pr(S_i \mid e_A, (m,\sigma)) - \Pr(S_i \mid e_A)| = 0;$ *and*

(c) $\max_{(m,\sigma)} \max_{e_G} |\Pr(S_i \mid e_G, (m,\sigma)) - \Pr(S_i \mid e_G)| = 0.$

First, we prove (a). Since the receiver R having e_R does not know the mapping π_1, R cannot guess the sender of (m,σ) effectively more than $\Pr(S_i \mid e_R)$. Hence, the equality (a) holds. In a similar manner, it is easy to see that the equality (b) holds, since the arbiter A having e_A does not know the mapping π_2. On the other hand, since G having $e_G = (\pi_1, \pi_2)$ knows neither $f_0(\beta_i) + f_1(\beta_i)v_R$ nor $f_0(\beta_i) + f_1(\beta_i)v_A$, G cannot guess the sender of (m,σ) with probability effectively more than $\Pr(S_i \mid e_G)$. Hence, the equality (c) holds.

Then, we prove that no information on the identity of the sender of (m,σ) is leaked from (m,σ) against the following adversaries:

(d) any set of colluders $S(i_1,\ldots,i_k)$, namely,

$$\max_{(m,\sigma)} \max_{e_{S(i_1,\ldots,i_k)}} \left|\Pr(S_i \mid e_{S(i_1,\ldots,i_k)}, (m,\sigma)) - \Pr(S_i \mid e_{S(i_1,\ldots,i_k)})\right| = 0; \text{ and}$$

(e) any collusion between $S(i_1,\ldots,i_k)$ and R, namely,

$$\max_{(m,\sigma)} \max_{e_{S(i_1,\ldots,i_k)}} \max_{e_R} \left|\Pr(S_i \mid e_{S(i_1,\ldots,i_k)}, e_R, (m,\sigma)) - \Pr(S_i \mid e_{S(i_1,\ldots,i_k)}, e_R)\right| = 0.$$

We next prove (d). Since $S(i_1,\ldots,i_k)$ knows neither π_1 nor π_2, they cannot guess the sender of (m,σ) effectively more than $\Pr(S_i \mid e_{S(i_1,\ldots,i_k)})$, which implies that (d) holds. Similarly, it is easy to see that (e) holds.

Finally, it is obvious from the construction that each of R and A can respectively identify the sender of (m,σ) by cooperating with G with probability 1, if (m,σ) is valid. □

Proof of Theorem 1. From Lemmas 2-5, it follows that our construction is a $(\frac{1}{q}, k, n)$-one-time secure GA^2-code. Furthermore, it is straightforward to evaluate memory sizes required in the construction. □

5. Extension of GA^2-codes: GA^3-codes

In the GA^2-code, it is assumed that the arbiter is always trusted. Here, we remove this assumption and call this GA^3-code, since this model can be regarded as extension of GA^2-codes and has properties similar to those of A^3-codes.

Our model of GA^3-codes is the same as that of GA^2-codes (see Definition 5). The difference between GA^2-codes and GA^3-codes lies in security definitions and the security definition of GA^3-codes is slightly stronger than that of GA^2-codes. In the model of GA^3-codes, we assume that the arbiter honestly gives a judgment on the case of a dispute based on the arbitration rule by using his secret key, however, that the arbiter may perform impersonation or substitution attacks in cooperation with some malicious entities. We define the security definition of GA^3-codes based on the idea in [**7**]. However, in our model, we do not consider the case that the arbiter A colludes with the receiver R. The reason is that A and R can always find an authenticated message which will be accepted by their keys e_A and e_R, since they have unbounded computational powers, which means that any colluding group including A and R will always win in the arbitration. Therefore, in this sense we consider that it is meaningless to consider the case (for example, see [**4**] for the similar discussion).

We formally provide the security definition of GA^3-codes as follows.

Definition 7 (Security of GA^3-code). *Let Π be a (p,k,n)-one-time secure GA^2-code. The scheme Π is said to be a (p,k,n)-one-time secure GA^3-code if the following conditions are satisfied.*

1) *No information on the identity of the sender of (m,σ) is leaked from (m,σ) against collusion between arbitrary malicious senders $S(i_1,\ldots,i_k)$ and the malicious arbiter A. Namely, for any $S(i_1,\ldots,i_k) \in \mathcal{W}$ and $S_i \in \mathcal{S} \setminus S(i_1,\ldots,i_k)$, we have*

$$\max_{(m,\sigma)} \max_{e_{S(i_1,\ldots,i_k)}} \max_{e_A} \left|\Pr(S_i \mid e_{S(i_1,\ldots,i_k)}, e_A, (m,\sigma)) - \Pr(S_i \mid e_{S(i_1,\ldots,i_k)}, e_A)\right| = 0.$$

The above equation means that, after distributing secret-keys $e_{S(i_1,\ldots,i_k)}$ and e_A, $S(i_1,\ldots,i_k)$ and A obtain no information on the identity of the sender from arbitrary (m,σ), where σ is taken such that $\sigma = GSign(e_{S_i}, m)$ for e_{S_i} and m.

2) *All of the success probabilities of attacks, $P_A^{(GA^3)}$ and $P_{SA}^{(GA^3)}$, are at most p, where $P_A^{(GA^3)}$ and $P_{SA}^{(GA^3)}$ are defined as follows.*

   (i) ***Attacks by** A: The malicious arbiter A tries to trump up an authenticated message from some honest sender. Let $P_A^{(GA^3)} := \max(P_{I_A}^{(GA^3)}, P_{S_A}^{(GA^3)})$, where $P_{I_A}^{(GA^3)}$ and $P_{S_A}^{(GA^3)}$ are given as follows.*

   ***Impersonation attack:** A tries to generate a fraudulent authenticated message (m,σ) such that R accepts it and someone of senders is detected as the sender of (m,σ). The success probability of this attack denoted by $P_{I_A}^{(GA^3)}$ is defined as*

$$P_{I_A}^{(GA^3)} := \max_{e_A} \max_{(m,\sigma)} \Pr(R \textit{ accepts } (m,\sigma) \wedge \textit{someone in } \mathcal{S} \textit{ is detected as the sender of } (m,\sigma) \mid e_A).$$

   ***Substitution attack:** A can observe a transmitted authenticated message (m,σ) which is generated by S_i, and then tries to generate a fraudu-*

lent one $(m',\sigma') \neq (m,\sigma)$ such that R accepts it and someone of senders is detected as the sender of (m',σ'). The success probability of this attack denoted by $P_{S_A}^{(GA^3)}(S_i)$ is defined as

$$P_{S_A}^{(GA^3)}(S_i) := \max_{e_A} \max_{(m,\sigma)} \max_{(m',\sigma')\neq(m,\sigma)} \Pr(R \textit{ accepts } (m',\sigma') \wedge \textit{someone in } \mathcal{S} \textit{ is detected as the sender of } (m',\sigma') \mid e_A, (m,\sigma)).$$

Then, $P_{S_A}^{(GA^3)}$ is defined as $P_{S_A}^{(GA^3)} := \max_{S_i \in \mathcal{S}} P_{S_A}^{(GA^3)}(S_i)$.

(ii) ***Collusion-attack by** $S(i_1,\ldots,i_k)$ **and** A: The malicious senders $S(i_1,\ldots,i_k)$ and the arbiter A collude together and try to trump up an authenticated message from some honest sender. Let $P_{SA}^{(GA^3)} := \max(P_{I_{SA}}^{(GA^3)}, P_{S_{SA}}^{(GA^3)})$, where $P_{I_{SA}}^{(GA^3)}$ and $P_{S_{SA}}^{(GA^3)}$ are given as follows.*

***Impersonation attack**: $S(i_1,\ldots,i_k)$ and A try to generate a fraudulent authenticated message (m,σ) such that R accepts it and someone in $\mathcal{S} \setminus S(i_1,\ldots,i_k)$ is detected as the sender of it. The success probability of this attack denoted by $P_{I_{SA}}^{(GA^3)}(S(i_1,\ldots,i_k))$ is defined as*

$$P_{I_{SA}}^{(GA^3)}(S(i_1,\ldots,i_k)) := \max_{e_{S(i_1,\ldots,i_k)}} \max_{e_A} \max_{(m,\sigma)} \Pr(R \textit{ accepts } (m,\sigma) \wedge \textit{someone in } \mathcal{S} \setminus S(i_1,\ldots,i_k) \textit{ is detected as the sender of } (m,\sigma) \mid e_{S(i_1,\ldots,i_k)}, e_A).$$

Then, $P_{I_{SA}}^{(GA^3)}$ is defined as $P_{I_{SA}}^{(GA^3)} := \max_{S(i_1,\ldots,i_k)\in\mathcal{W}} P_{I_{SA}}^{(GA^3)}(S(i_1,\ldots,i_k))$.

***Substitution attack**: $S(i_1,\ldots,i_k)$ and A can observe a transmitted authenticated message (m,σ) which is generated by S_i, and then try to generate a fraudulent one $(m',\sigma') \neq (m,\sigma)$ such that R accepts it and someone in $\mathcal{S} \setminus S(i_1,\ldots,i_k)$ is detected as the sender of it. The success probability of this attack denoted by $P_{S_{SA}}^{(GA^3)}$ is defined as*

$$P_{S_{SA}}^{(GA^3)}(S(i_1,\ldots,i_k), S_i) := \max_{e_{S(i_1,\ldots,i_k)}} \max_{e_A} \max_{(m,\sigma)} \max_{(m',\sigma')\neq(m,\sigma)} \Pr(R \textit{ accepts } (m',\sigma') \wedge \textit{someone in } \mathcal{S} \setminus S(i_1,\ldots,i_k) \textit{ is detected as the sender of } (m',\sigma') \mid e_{S(i_1,\ldots,i_k)}, e_A, (m,\sigma)).$$

Then, $P_{S_{SA}}^{(GA^3)}$ is defined as

$$P_{S_{SA}}^{(GA^3)} := \max_{S(i_1,\ldots,i_k)\in\mathcal{W}} \max_{S_i \in \mathcal{S}\setminus S(i_1,\ldots,i_k)} P_{S_{SA}}^{(GA^3)}(S(i_1,\ldots,i_k), S_i).$$

We next consider a construction of the GA^3-code. Interestingly, the construction proposed in the previous section meets the security definition of the GA^3-code.

THEOREM 2. *The construction proposed in Section 4 results in a* $(\frac{1}{q}, k, n)$*-one-time secure* GA^3*-code.*

Proof. What remains to be shown is that the construction satisfies that $P_A^{(GA^3)}$ and $P_{SA}^{(GA^3)}$ are at most $1/q$ and the collusion between malicious senders and the malicious arbiter cannot get any information on the identity of the sender of (m, σ) from (m, σ) itself and their own information. We note that the arbiter's key e_A and the receiver's key e_R are generated in a similar way. Therefore, it is easy to see that $P_A^{(GA^3)} = P_R^{(GA^3)}$ and $P_{SA}^{(GA^3)} = P_{SR}^{(GA^3)}$ by Definition 7. In addition to this, by Definition 7, the fact that R cannot obtain any information on the identity of the sender of (m, σ) implies the fact that A cannot also get any information on that. Thus, from Theorem 1, it follows that $P_A^{(GA^3)}$ and $P_{SA}^{(GA^3)}$ are at most $1/q$ and $\max_{(m,\sigma)} \max_{e_{S(i_1,\ldots,i_k)}} \max_{e_A} \left|\Pr(S_i \mid e_{S(i_1,\ldots,i_k)}, e_A, (m, \sigma)) - \Pr(S_i \mid e_{S(i_1,\ldots,i_k)}, e_A)\right| = 0.$

□

References

[1] E. Brickell and D. Stinson. Authentication codes with multiple arbiters. In D. Barstow, W. Brauer, P. Brinch Hansen, D. Gries, D. Luckham, C. Moler, A. Pnueli, G. Seegmüller, J. Stoer, N. Wirth, and C. Günther, editors, *Advances in Cryptology — EUROCRYPT '88*, volume 330, pages 51–55. Springer Berlin Heidelberg, 1988.

[2] D. Chaum and E. Heyst. Group signatures. In D. Davies, editor, *Advances in Cryptology — EUROCRYPT '91*, volume 547, pages 257–265. Springer Berlin Heidelberg, 1991.

[3] E. N. Gilbert, F. J. MacWilliams, and N. J. A. Sloane. Codes which detect deception. *Bell System Technical Journal*, 53(3):405–424, 1974.

[4] G. Hanaoka, J. Shikata, Y. Hanaoka, and H. Imai. The role of arbiters in asymmetric authentication schemes. In C. Boyd and W. Mao, editors, *Information Security*, volume 2851, pages 428–441. Springer Berlin Heidelberg, 2003.

[5] G. Hanaoka, J. Shikata, Y. Hanaoka, and H. Imai. Unconditionally secure anonymous encryption and group authentication. *The Computer Journal*, 49(3):310–321, 2006.

[6] R. L. Rivest. Unconditionally secure commitment and oblivious transfer schemes using private channels and a trusted initializer. 1999.

[7] R. Safavi-Naini and Y. Wang. a^3-codes under collusion attacks. *JCMCC. The Journal of Combinatorial Mathematics and Combinatorial Computing*, 45:163–182, 2003.

[8] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[9] G. Simmons. Authentication theory/coding theory. In G. Blakley and D. Chaum, editors, *Advances in Cryptology*, volume 196 of *Lecture Notes in Computer Science*, pages 411–431. Springer Berlin Heidelberg, 1985.

[10] G. Simmons. Message authentication with arbitration of transmitter/receiver disputes. In D. Chaum and W. Price, editors, *Advances in Cryptology — EUROCRYPT' 87*, volume 304, pages 151–165. Springer Berlin Heidelberg, 1988.

[11] G. Simmons. A cartesian product construction for unconditionally secure authentication codes that permit arbitration. *Journal of Cryptology*, 2(2):77–104, 1990.

Takenobu Seito

Graduate School of Environment and Information Sciences, Yokohama National University
Tokiwadai 79-7, Hodogaya-ku, Yokohama, 240-8501, Japan

Yohei Watanabe

Graduate School of Environment and Information Sciences, Yokohama National University
Tokiwadai 79-7, Hodogaya-ku, Yokohama, 240-8501, Japan
watanabe-yohei-xs@ynu.jp

Kazuyuki Kinose

Graduate School of Environment and Information Sciences, Yokohama National University
Tokiwadai 79-7, Hodogaya-ku, Yokohama, 240-8501, Japan

Junji Shikata

Graduate School of Environment and Information Sciences, Yokohama National University
Tokiwadai 79-7, Hodogaya-ku, Yokohama, 240-8501, Japan
shikata@ynu.ac.jp