Design and Analysis of Information-Theoretically Secure Authentication Codes with Non-Uniformly Random Keys

Junji Shikata

Graduate School of Environment and Information Sciences,
Yokohama National University, Japan.
shikata@ynu.ac.jp

Abstract

The authentication code (A-code) is the one of the most fundamental cryptographic protocols in information-theoretic cryptography, and it provides information-theoretic integrity or authenticity, i.e., preventing information from being altered or substituted by the adversary having unbounded computational powers. In addition, it has a wide range of applications such as multiparty computations and quantum key distribution protocols. The traditional A-code theory states that a good A-code is characterized as an A-code which satisfies equality of a lower bound on size of secret-keys, i.e., an A-code satisfying $|\mathcal{K}| = \epsilon^{-2}$, where $|\mathcal{K}|$ is cardinality of the set of secret-keys and ϵ is the success probability of attacks of the adversary. However, good A-codes imply that secret-keys must be uniformly distributed. Therefore, if a non-uniformly random key is given, we cannot realize a good A-code by using it as a secret-key. Then, a natural question about this is: what is a good A-code having non-uniformly random keys? And, how can we design such a good A-code having non-uniformly random keys? To answer the questions, in this paper, we perform analysis of A-codes having non-uniformly random keys, and show the principle that guides the design for such good A-codes.

Specifically, the contribution of this paper is as follows. We first derive a new lower bound on entropy of secret-keys, and it is described in terms of Rényi entropy. Next, we define that a good A-code having non-uniformly random keys is the one satisfying equality of the bound, and it is characterized by the min-entropy (a special case of Rényi entropy). Furthermore, we introduce the classification methodology for A-codes which are realizable from a biased key-source. This classification is performed by using a mathematical tool, i.e., a group action on the set of authentication matrices. By this analysis, we can understand what kind of A-codes is actually constructable. Finally, we design how to construct good A-codes having 1-bit messages from von Neumann sources. We also show that our construction methodology is superior to the one by applying von Neumann extractors and the traditional optimal A-code constructions. Although the case of 1-bit messages may be restricted, however, this case is simple and we believe that a general case will develop from this simple case.

Keywords: authentication code, non-uniformly random key, information-theoretic security, unconditional security, lower bound, von Neumann source

1 Introduction

Informally, information-theoretic security (a.k.a. unconditional security) means the security which is guaranteed against the adversary having unlimited (i.e., infinite) computational resources, while computational security is the one against the computationally bounded adversary (i.e. polynomial-time Turing machine). Therefore, information-theoretic cryptography is attractive in terms of security. On

the other hand, information-theoretic cryptography has drawbacks, compared to the computational one, in realizable mechanisms and achievable efficiency in cryptographic protocols, in particular, it usually requires long uniformly random secret-keys. Among cryptographic protocols in information-theoretic cryptography, the most important and fundamental protocols include the encryption (cryptosystem) and the authentication code (A-code for short): the former provides confidentiality (or privacy), i.e., keeping information secret from the adversary; and the latter achieves integrity (or authenticity), i.e., preventing information from being altered or substituted by the adversary. Actually, these protocols were studied in the first stage of research of cryptology in history. The encryption was first studied by Shannon [23] in 1949, by which the study of information-theoretic cryptography started. On the other hand, the A-code was invented by Gilbert, MacWilliams, and Sloane in 1974 [7], and the theory of A-codes was intensively developed by Simmons in the 1980's [25]. The purpose of this paper is to further develop the study on the A-code in information-theoretic cryptography, more specifically, the A-code having non-uniformly random secret-keys.

1.1 Background: the study on the A-code

Let us consider a model of the A-code where there are three entities, a sender (or transmitter), a receiver and an adversary (or opponent). An A-code π consists of $([P_K], \mathit{Auth}, \mathit{Vrfy})$, where $[P_K]$ is a key generation algorithm (or a key-source) which outputs a secret-key k according to a probability distribution P_K over a finite set $\mathcal{K}$, Auth is an authentication algorithm, and Vrfy is a verification algorithm. Suppose that the sender and the receiver share a secret key $k \in \mathcal{K}$. For a message $m \in \mathcal{M}$, the sender creates an authenticator (or a tag) $a = \mathit{Auth}(k, m)$, and transmits the authenticated message (m, a) to the receiver via an insecure channel to which the adversary can have perfect read-and-write access[1]. On receiving the authenticated message (m, a), the receiver checks its validity. If $\mathit{Vrfy}(k, (m, a)) = 1$, the receiver accepts m and regards it being sent from the sender. Otherwise, i.e., $\mathit{Vrfy}(k, \sigma) = 0$, the receiver rejects it. In this model, the adversary having unlimited computational power can insert an authenticated message (m, a) into the channel, and/or can substitute an observed authenticated message (m, a) with another one $(m', a') \neq (m, a)$. These two attacks are traditionally called the *impersonation attack* and *substitution attack*, respectively, and the success probabilities of these two attacks are formally defined as follows.

$$P_{I,\pi} := \max_{(m,a)} \Pr\{\, \mathit{Vrfy}(K, (m, a)) = 1\},$$
$$P_{S,\pi}^{\mathsf{kma}} := \sum_{(m,a)} P_{MA}(m, a) \max_{(m',a') \neq (m,a)} \Pr\{\, \mathit{Vrfy}(K, (m', a')) = 1 | (m, a)\},$$

where the probabilities $\Pr\{...\}$ above in RHSs are considered with respect to K.

By performing these two kinds of attacks, the goal of the adversary is that the authenticated message inserted and/or substituted by him/her is accepted by the receiver. The A-code is considered to be *secure*, if the success probabilities of two attacks are at most a small quantity $\epsilon \in (0, 1]$ (note that $\epsilon = 0$ is impossible), which we call ϵ-*security* in this paper. Then, the following lower bounds on the size of secret-keys are well known:

Proposition 1 (Lower bound, [25]) *Suppose that an A-code π satisfies $P_{I,\pi} \leq \epsilon$ and $P_{S,\pi}^{\mathsf{kma}} \leq \epsilon$. Then, it holds that $|\mathcal{K}| \geq \epsilon^{-2}$. More generally, it holds that $H(K) \geq -\log P_{I,\pi} P_{S,\pi}^{\mathsf{kma}}$, where $H(\cdot)$ is the Shannon entropy.*

[1] In the classical notation in A-codes, the *message* and *authenticated message* are called the *source state* and *message*, respectively.

In order to satisfy $P_{S,\pi}^{\mathsf{kma}} \leq \epsilon$ for every distribution of messages P_M, it is sufficient to satisfy that

$$P_{S,\pi}^{\mathsf{max}} := \max_{(m,a)} \max_{(m',a') \neq (m,a)} \Pr\{ \mathit{Vrfy}(K, (m', a')) = 1 | (m, a) \}$$

is not larger than ϵ, since $P_{S,\pi}^{\mathsf{kma}} \leq P_{S,\pi}^{\mathsf{max}}$ by definition. This observation and Proposition 1 immediately show that:

Proposition 2 (Lower bound) $\log |\mathcal{K}| \geq H(K) \geq -\log P_{I,\pi} P_{S,\pi}^{\mathsf{max}}$.

There are several *optimal* constructions of A-codes in the sense that those constructions meet the lower bounds with equalities in Propositions 1 and 2. Specifically, those constructions are proposed by using mathematical structures such as algebra (polynomials over finite fields), geometry (projective spaces in finite geometry), and combinatorics (orthogonal arrays). For the above results on the lower bounds and optimal constructions of A-codes, see [6, 13, 14, 15, 16, 20, 22, 25, 26, 29, 31].

1.2 Motivation and Our Contribution

As explained in the previous section, the traditional theory of A-codes brings us the following results: For ϵ-secure A-codes (i.e., $\max\{P_{I,\pi}, P_{S,\pi}^{\mathsf{kma}}, P_{S,\pi}^{\mathsf{max}}\} \leq \epsilon$), we obtain

(i) *Lower bound on keys* is given by $\log |\mathcal{K}| \geq H(K) \geq -2 \log \epsilon$;

(ii) *Optimal A-code* means an A-code π such that $|\mathcal{K}| = \epsilon^{-2}$.

Based on this, the designing principle for *good* A-codes is made clear (i.e., a good A-code means an optimal A-code). In addition, several optimal constructions of A-codes are already known. However, the above optimality implies that P_K must be the uniform distribution, since $\log |\mathcal{K}| = H(K)$. Therefore, if a non-uniformly random key K is given, we cannot realize an optimal A-code by using it as a secret-key. Then, a natural question about this is: what is a *good* A-code having non-uniformly random keys? And, how can we design such a good A-code having non-uniformly random keys? For example, can we construct a good A-code from a biased key-source by applying extractors and optimal construction above? To answer the questions, in this paper, we perform the detailed analysis of A-codes having non-uniformly random keys, and show the principle that guides the design for good A-codes having non-uniformly random keys. Specifically, the contribution of this paper is as follows.

Analysis of A-codes having non-uniformly random keys. In order to define a *good* A-code having non-uniformly random keys, we derive a new lower bound on keys in Section 5:

(i) **Lower bound on keys.** For any A-code π, it holds $R_\alpha(K) \geq -\log P_{I,\pi} P_{S,\pi}^{\mathsf{max}}$ for any $\alpha \in [0, \infty]$, where $R_\alpha(\cdot)$ is the Rényi entropy of order α (See Appendix A for the Rényi entropy).

Based on this bound, in Section 6, we define the *optimality* of A-codes having non-uniformly random keys (i.e., a definition of good A-codes with biased keys) by the equality of the bound when $\alpha = \infty$:

(ii) **∞-optimality.** An A-code π having a key-source $[P_K]$ is ∞-optimal, if it satisfies

$$R_\infty(K) = -\log P_{I,\pi} P_{S,\pi}^{\mathsf{max}},$$

where $R_\infty(\cdot)$ is the min-entropy (i.e., a special case of the Rényi entropy).

The reasonability of the definition of optimality is also explained in Section 6. Therefore, we consider that a *good* A-code having non-uniformly random keys is the one satisfying the condition of ∞-optimality in this paper. Note that optimality of A-codes having uniform random keys was characterized by the Hartley entropy (i.e., logarithm of the cardinality of a finite set), while optimality of A-codes having non-uniformly random keys is characterized by the min-entropy.

Furthermore, in Section 7, we introduce a classification methodology for A-codes which are realizable from a biased key-source. This classification is performed by using a mathematical tool, a group action on the set of authentication matrices. By this analysis, we can understand what kind of A-codes is actually constructable or not. In addition, we analyze a very simple case – A-codes with 1-bit messages and 1-bit authenticators – as a first illustration of this methodology, since it is generally complicated to clarify all constractable A-codes from an arbitrarily given biased key source.

Design of A-codes with non-uniformly random keys (1-bit message A-codes). In this paper, we design *good* A-codes having 1-bit messages by using a biased key-source. For doing it, in Section 7, we completely classify A-codes with 1-bit messages and 1-bit authenticators, and show that three kinds of A-codes are realizable. Based on this results, we explicitly show how to construct good A-codes from von Neumann sources. The reason why we focus on the von Neumann source includes: it is simple in the sense that it outputs a (biased) binary string based on i.i.d. according to a binary distribution $[p, 1-p]$ with some $p \in (0, 1)$; and it is universal in the sense that we do not have to know such p explicitly. We also show that our construction methodology is superior to the one by applying von Neumann extractor and the traditional optimal A-code construction. Although the case of 1-bit messages may be restricted, however, this case is simple and we believe that a general case will develop from this simple case.

1.3 Related Works

Dodis and Spencer first investigated the A-codes having non-uniformly random keys in [3]. The purpose of the paper [3] is to investigate the strength of *cryptographic sources*, i.e., imperfect sources enough for cryptographic usage of the encryption or the A-code, compared to other sources such as simulatable sources (enough for simulating BPP algorithms) and extractable sources (enough for extracting uniformly random bits). The main result of [3] is that cryptographic sources lie in between simulatable and extractable sources. In the process of showing this result, they focused on the min-entropy of an imperfect source and success probability of substitution attack of an A-code. They only discussed a particular source and an A-code to show the existence of a source and an A-code satisfying the above main result, and our purpose of this paper is different from their aim. However, our results are influenced by their idea and approach, since we also give the definition of optimality of A-codes by the min-entropy of the key-source. Therefore, our results can be regarded as further investigation of A-codes having a non-uniform key-source.

To the best of author's knowledge, all works about A-codes except for [3] assume that uniformly random sources (random keys) are more or less available: the works for traditional A-codes using uniformly random key-sources [6, 13, 14, 15, 16, 20, 22, 25, 26, 29, 31], or (interactive) A-codes using uniformly random sources and biased ones [4]. Therefore, this paper faces a challenge of establishing theory of (non-interactive) A-codes based on non-uniformly random key-sources, like the traditional theory developed by Simmons and others.

2 Authentication Codes (A-codes)

We consider a scenario where there are three entities, a sender (or a transmitter), a receiver and an adversary (or an opponent). Then, the traditional model of the authentication codes without secrecy

is formally defined as follows.

Definition 1 (A-code) An *authentication code without secrecy*[2] π consists of algorithms ($[P_K]$, *Auth*, *Vrfy*) with finite sets $\mathcal{M}, \mathcal{A}, \mathcal{K}$ defined as follows.

- *Finite sets and random variables.* $\mathcal{K}$ is a finite set of *keys* shared by the sender and the receiver, and P_K (resp., K) denotes a probability distribution over $\mathcal{K}$ (resp., a random variable taking values in $\mathcal{K}$); $\mathcal{M}$ is a finite set of *messages*[3], and P_M (resp., M) denotes a probability distribution over $\mathcal{M}$ (resp., a random variable taking values in $\mathcal{M}$). In this paper, we assume that P_K is statistically independent of P_M; $\mathcal{A}$ is a finite set of *authenticators* (or tags), and P_A (resp., A) denotes a probability distribution over $\mathcal{A}$ (resp., a random variable taking values in $\mathcal{A}$).

- *Random key source and sampling algorithm.* $[P_K]$ is a key generation algorithm (or a key-source), and it outputs a key $k \in \mathcal{K}$ according to P_K.

- *Authentication and verification algorithms.* *Auth* is an authentication algorithm which takes a key $k \in \mathcal{K}$ and a message $m \in \mathcal{M}$ as input and outputs an authenticator $a \leftarrow \mathit{Auth}(k, m)$; *Vrfy* is a verification algorithm which takes a key $k \in \mathcal{K}$ and a pair of messages and authenticators (m, a), which we call an *authenticated message*[4], and outputs a bit $b \leftarrow \mathit{Vrfy}(k, m, a)$: if $b = 1$, it means that (m, a) is valid; otherwise (i.e., $b = 0$), it means that (m, a) is invalid.

The protocol execution of the above authentication code is described in Table 1.

Table 1: Protocol execution of $\pi = ([P_K], \mathit{Auth}, \mathit{Vrfy})$.

– Inner input of Sender: $k \in \mathcal{K}$
– Outer input of Sender: $m \in \mathcal{M}$
– Inner input of Receiver: $k \in \mathcal{K}$
– Outer output of Receiver: a bit $b \in \{0, 1\}$
1. *Auth* computes $a \leftarrow \mathit{Auth}(k, m)$ and sends (m, a) to the receiver by an insecure channel.
2. *Vrfy* computes $b \leftarrow \mathit{Vrfy}(k, m, a)$ and outputs b.

In this paper, for simplicity, we use the terminology of an *authentication code* (or more simply, an *A-code*) instead of an authentication code without secrecy mentioned above. In Definition 1, we require the correctness property of the A-code: For any possible $k \in \mathcal{K}$, $m \in \mathcal{M}$, it holds that $\mathit{Vrfy}(k, m, a) = 1$ for $a \leftarrow \mathit{Auth}(k, m)$.

Also, an A-code $\pi = ([P_K], \mathit{Auth}, \mathit{Vrfy})$ is called an *A-code without splitting*, if *Auth* is a deterministic algorithm, and called an *A-code with splitting* otherwise (i.e., *Auth* is randomized). If $\pi = ([P_K], \mathit{Auth}, \mathit{Vrfy})$ is an A-code without splitting, we can simply suppose that *Vrfy* is trivially constructed by *Auth*: $\mathit{Vrfy}(k, m, a) = 1$ if and only if $\mathit{Auth}(k, m) = a$. In this paper, for simplicity, we only deal with an A-code without splitting, and we call it an A-code for short, again.

[2]It is often called a *Cartesian authentication code*.

[3]In the model of authentication codes, the term *source state* is traditionally used. However, in this paper we use the term *message* as usually used in the context of cryptographic schemes for providing computational authenticity or integrity such as MAC and digital signatures.

[4]Also, in the model of authentication codes, the term *message* is traditionally used. However, in this paper we use the term *authenticated message* not to be confused with elements in $\mathcal{M}$.

The traditional security notion of authentication codes was given in [25]. In the attacking model it is assumed that the adversary can insert an authenticated message into the channel, and/or also can substitute an observed authenticated message with another one. These two attacks are traditionally called the *impersonation attack* and the *substitution attack*, respectively. By performing these attacks, the goal of the adversary is that the authenticated message inserted and/or substituted by him could be accepted as authentic by the receiver. However, there are several possible ways how to formally define the security of A-codes, essentially formalization of substitution attacks, as follows.

Definition 2 (Attacking model) *Let $\pi = ([P_K], Auth, Vrfy)$ be an A-code. The success probabilities of impersonation and substitution attacks are defined as follows, where the probabilities* $\Pr\{...\}$ *below in RHSs are considered with respect to K.*

1. *Success probability of the impersonation attack:* $P_{I,\pi} = \max_{(m,a)} \Pr\{\, Vrfy(K,(m,a)) = 1\}$.

2. *Success probability of the substitution attack:*

$$P_{S,\pi}^{\mathsf{kma}} = \sum_{(m,a)} P_{MA}(m,a) \max_{(m',a')\neq(m,a)} \Pr\{\, Vrfy(K,(m',a')) = 1 \mid (m,a)\},$$
$$P_{S,\pi}^{\mathsf{cma}} = \max_{m} \sum_{a} P_{A|M}(a|m) \max_{(m',a')\neq(m,a)} \Pr\{\, Vrfy(K,(m',a')) = 1 \mid (m,a)\},$$
$$P_{S,\pi}^{\mathsf{max}} = \max_{(m,a)} \max_{(m',a')\neq(m,a)} \Pr\{\, Vrfy(K,(m',a')) = 1 \mid (m,a)\}.$$

Intuitively, the success probabilities of the above three kinds of substitution attacks have the following operational meaning:

- $P_{S,\pi}^{\mathsf{kma}}$: Suppose that the sender selects a message m according to P_M and he has a secret-key k chosen according to P_K. And, an authenticated message (m,a) which occurs with P_{MA} is sent by the sender and observed by the adversary. Then, the adversary will replace it with an illegal $(m',a') \neq (m,a)$ by taking his best strategy, and $P_{S,\pi}^{\mathsf{kma}}$ means the success probability of this attack. In cryptography, this attack can be considered to be the *known message attack*. For example, this kind of the substitution attack is considered in [7, 15, 16, 20, 25, 31] for (multiple) A-codes, and in [10] for variants of A-codes.

- $P_{S,\pi}^{\mathsf{cma}}$: Suppose that the adversary selects a message m of his arbitrary choice, and queries it to the sender by regarding him as an *authentication oracle*, and then he obtains an authenticated message (m,a), where a is generated by a random secret-key with distribution P_K. Then, the adversary will create an illegal $(m',a') \neq (m,a)$ by taking his best strategy hoping that (m',a') will be accepted by the receiver. $P_{S,\pi}^{\mathsf{cma}}$ means the success probability of this kind of the attack, and in cryptography, this attack can be considered to be the *chosen message attack*. This kind of the substitution attack is considered in [3, 4] for (interactive) A-codes using biased key-sources.

- $P_{S,\pi}^{\mathsf{max}}$: The last kind of the attack describes the possibility of the substitution attack in principle. Namely, it is supposed that the adversary can obtain an authenticated message (m,a) of his arbitrary choice so that substitution by $(m',a') \neq (m,a)$ will be most effective. This is also considered to be the *chosen message attack*, however, in the formalization the success probability of this attack, denoted by $P_{S,\pi}^{\mathsf{max}}$, is evaluated as the maximum over all possible (m,a) and (m',a'). This kind of the substitution attack is most powerful among the three kinds of formalizations of the attacks above. And, for example, it is considered in [18, 28] for (multiple) A-codes, and in [11, 21, 24] for variants of A-codes.

By definition, it is easy to observe the following relation among substitution attacks holds: $P_{S,\pi}^{\mathsf{max}} \geq P_{S,\pi}^{\mathsf{cma}} \geq P_{S,\pi}^{\mathsf{kma}}$.

Definition 3 (Security) Let π be an A-code. Then, security of π is defined as follows[5].

(i) π is said to be ϵ-*KMA-secure*, if $\max\{P_{I,\pi}, P_{S,\pi}^{\mathsf{kma}}\} \leq \epsilon$.

(ii) π is said to be ϵ-*CMA-secure*, if $\max\{P_{I,\pi}, P_{S,\pi}^{\mathsf{cma}}\} \leq \epsilon$.

(iii) π is said to be ϵ-*strongly-CMA-secure*, if $\max\{P_{I,\pi}, P_{S,\pi}^{\mathsf{max}}\} \leq \epsilon$.

3 Representing A-codes by Matrices (Arrays)

Let π be an A-code with a message-set $\mathcal{M}$ and an authenticator-set $\mathcal{A}$ which has a key-source $[P_K]$ over $\mathcal{K}$. In general, an A-code can be represented by a $|\mathcal{M}| \times |\mathcal{K}|$ matrix, and it is called *authentication matrix*[6].

Definition 4 (Authentication Matrix, e.g., [2]) For an A-code $\pi = ([P_K], Auth, Vrfy)$, an *authentication matrix* of π, denoted by A_π, is a $|\mathcal{M}| \times |\mathcal{K}|$ matrix in which the rows are indexed by the set $\mathcal{M}$, the columns are indexed by the set $\mathcal{K}$, and the (m,k)-entry for $m \in \mathcal{M}$ and $k \in \mathcal{K}$ is given by $a = Auth(k,m) \in \mathcal{A}$.

So far, we have not paid much attention to *orders* of indexed sets of rows and columns of authentication matrices, since we have focused on the uniformly random secret-keys over $\mathcal{K}$. In order to deal with A-codes having non-uniformly random secret keys over $\mathcal{K}$, we need to pay attention to the orders of the indexed sets. Specifically, we consider orders of indexed sets of rows and columns of authentication matrices as follows.

- Suppose that $(\mathcal{K}, \leq_K)$ is a totally ordered set having a probability distribution P_K[7], and the columns of A_π are indexed by the elements in $\mathcal{K}$ as follows. For $\mathcal{K} := \{k_1, k_2, \ldots, k_{|\mathcal{K}|}\}$, an ordered sequence of all elements in $\mathcal{K}$ is given, i.e., $k_1 \leq_K k_2 \leq \ldots \leq_K k_{|\mathcal{K}|}$, with respect to the order $\leq_K$, and this fixed sequence is used for indexing the columns. In the following, we consider the order $\leq_K$ defined by $k_i \leq_K k_j \iff P_K(k_i) \geq P_K(k_j)$ and an ordered sequence with respect to $\leq_K$ is given, if we do not explain anything about it.

- Similarly, $(\mathcal{M}, \leq_M)$ is a totally ordered set having a probability distribution P_M, and the rows of A_π are indexed by the elements in $\mathcal{M}$. In the following, we also consider the order $\leq_M$ defined by $m_i \leq_M m_j \iff P_M(m_i) \geq P_M(m_j)$, and suppose that an ordered sequence with respect to $\leq_M$ is given and fixed, if we do not explain anything about it.

Remark 1 *Conversely, if a distribution P_K over a totally ordered finite set $(\mathcal{K}, \leq_K)$, P_M over $(\mathcal{M}, \leq_M)$, and an $s \times u$ matrix A with $|\mathcal{K}| = u$ and $|\mathcal{M}| = s$ in which each entry is an element of a t-symbol set are given, an A-code π having a message-set $(\mathcal{M}, \leq_M)$, an authenticator-set $\mathcal{A}$, and a key-set $(\mathcal{K}, \leq_K)$ such that $|\mathcal{A}| = t$ and $A = A_\pi$ is determined. For simplicity, we write π_A for an A-code determined from the matrix A in this way, if it is clear from the context.*

[5] See also Remark 2 in Section 5

[6] In several literatures (e.g., [2]), the authentication matrix is defined as the $|\mathcal{K}| \times |\mathcal{M}|$ matrix, and the relation between its transpose and an orthogonal array will be considered. However, for simplicity, we define the authentication matrix as above so that we do not have to consider its transpose.

[7] Note that the order $\leq_K$ can depend on the distribution P_K over $\mathcal{K}$.

Definition 5 (Reduced Authentication Matrix) An authentication matrix A_π is said to be *reduced*, if every two columns of A_π are different.

Let $[P_K]$ be a key-source and let π be an A-code having a message-set $(\mathcal{M}, \leq_M)$, an authenticator-set $\mathcal{A}$, and a key-set $(\mathcal{K}, \leq_K)$. If there are i_1, i_2 such that $(a_{1,i_1}, a_{2,i_1}, \ldots, a_{|\mathcal{M}|,i_1}) = (a_{1,i_2}, a_{2,i_2}, \ldots, a_{|\mathcal{M}|,i_2})$ (i.e., there are the same columns) in A_π, where $a_{j,i} := \mathrm{Auth}(k_i, m_j)$, we can integrate the two keys k_{i_1} and k_{i_2} into one key k_{i_1,i_2} with probability $P_{K'}(k_{i_1,i_2}) := P_K(k_{i_1}) + P_K(k_{i_2})$, and the index of secret-keys is rearranged by a new distribution $P_{K'}$ over a set $\mathcal{K}' := (\mathcal{K} \setminus \{k_{i_1}, k_{i_2}\}) \bigcup \{k_{i_1,i_2}\}$ with the total order $\leq_{K'}$. Suppose that A_π is transformed in this way several times until all columns are different, and then, the resulting probability distribution and authentication matrix are denoted by $P_{K^{(R)}}$ and $A_\pi^{(R)}$, respectively. Then, we give the following definition.

Definition 6 (Reduced Form) Suppose that an A-code π having a key-source distribution P_K over $(\mathcal{K}, \leq_K)$ is given, and let A_π be its authentication matrix. An authentication matrix B is said to be a *reduced form* of A_π, if B is reduced and B can be obtained from A_π by repeating the above procedure.

Considering the procedure mentioned above to obtain a reduced form is reasonable and natural, since the procedure does not change security of π (i.e., all of $P_{I,\pi}$, $P_{S,\pi}^{\mathsf{kma}}$, $P_{S,\pi}^{\mathsf{cma}}$, and $P_{S,\pi}^{\mathsf{max}}$) and it simplifies the authentication matrix of π. The description of success probabilities of attacks by reduced forms is given in the next section.

4 Representing Success Probabilities of Attacks by Reduced Forms

Let $\pi = ([P_K], \mathit{Auth}, \mathit{Vrfy})$ be an A-code having a message-set $(\mathcal{M}, \leq_M)$, an authenticator-set $\mathcal{A}$, and a key-set $(\mathcal{K}, \leq_K)$. For any $(m, a) \in \mathcal{M} \times \mathcal{A}$, we define

$$\mathcal{K}(m, a) := \{k \in \mathcal{K} \mid \mathit{Auth}(k, m) = a\}. \tag{1}$$

Note that, for arbitrary $m \in \mathcal{M}$ and $a, a' \in \mathcal{A}$ with $a \neq a'$, we have $\mathcal{K}(m, a) \cap \mathcal{K}(m, a') = \emptyset$, and hence, for arbitrary $m \in \mathcal{M}$, we have

$$\mathcal{K} = \coprod_{a \in \mathcal{A}} \mathcal{K}(m, a). \tag{2}$$

Furthermore, for arbitrary $m_0, m_1 \in \mathcal{M}$ with $m_0 \neq m_1$, let $\pi|_{\{m_0,m_1\}}$ to be the A-code obtained from π by restricting its message-set $\{m_0, m_1\}$, i.e., π having the message-set consisting of two elements m_0, m_1. In addition, let $A_{\pi|_{\{m_0,m_1\}}}$ be the authentication matrix of $\pi|_{\{m_0,m_1\}}$, and suppose that $A^{(R)}_{\pi|_{\{m_0,m_1\}}}$ is a reduced form of $A_{\pi|_{\{m_0,m_1\}}}$. Then, we denote an induced key-set and an induced distribution over it by $K^{(R)}_{m_0,m_1}$ and $P_{K^{(R)}_{m_0,m_1}}$, respectively. Now, we define the following set in a similar way as (1): For $m \in \{m_0, m_1\}$,

$$\mathcal{K}^{(R)}_{m_0,m_1}(m, a) := \{k \in \mathcal{K}^{(R)}_{m_0,m_1} \mid \mathit{Auth}(k, m) = a\}. \tag{3}$$

Then, we define

$$\begin{aligned}
P_{I,\pi}(m_0) &:= \max_a \sum_{k\in\mathcal{K}(m_0,a)} P_K(k),\\
P^{\mathsf{max}}_{S,\pi}(m_0,m_1) &:= \max_{m\in\{m_0,m_1\}} \max_a \frac{\max\limits_{k\in\mathcal{K}^{(R)}_{m_0,m_1}(m,a)} P_{K^{(R)}_{m_0,m_1}}(k)}{\sum\limits_{k\in\mathcal{K}^{(R)}_{m_0,m_1}(m,a)} P_{K^{(R)}_{m_0,m_1}}(k)},\\
P^{\mathsf{cma}}_{S,\pi}(m_0,m_1) &:= \max_{m\in\{m_0,m_1\}} \sum_a \max_{k\in\mathcal{K}^{(R)}_{m_0,m_1}(m,a)} P_{K^{(R)}_{m_0,m_1}}(k).
\end{aligned}$$

Then, by definition, it can be shown that

$$\begin{aligned}
P_{I,\pi} &= \max_m P_{I,\pi}(m),\\
P^{\mathsf{max}}_{S,\pi} &= \max_{(m,m'),\ m\neq m'} P^{\mathsf{max}}_{S,\pi}(m,m'),\\
P^{\mathsf{cma}}_{S,\pi} &= \max_{(m,m'),\ m\neq m'} P^{\mathsf{cma}}_{S,\pi}(m,m').
\end{aligned}$$

5 New Bounds for A-codes

By definition, it is straightforward to see that $P^{\mathsf{kma}}_{S,\pi} \le P^{\mathsf{cma}}_{S,\pi} \le P^{\mathsf{max}}_{S,\pi}$ for any A-code π. First, we show that $P_{I,\pi} \le P^{\mathsf{cma}}_{S,\pi}$ for any A-code π.

Theorem 1 *For any A-code π, we have $P_{I,\pi} \le P^{\mathsf{cma}}_{S,\pi}$.*

Proof. First, we show the following lemmas.

Lemma 1 *For any A-code π with 1-bit messages, we have $P_{I,\pi} \le P^{\mathsf{cma}}_{S,\pi}$.*

Proof. Let $\mathcal{M} = \{m_0, m_1\}$. Suppose that an arbitrary A-code $\pi = ([P_K], \mathit{Auth}, \mathit{Vrfy})$ having $\mathcal{M}$ is given. Without loss of generality, we assume that an authentication matrix of π, denoted by A_π, is an element of the orthogonal array of degree 2 and order s, $\mathrm{OA}(2,s)$ (see Remark 5), by considering its reduced form.

For $m_0, m_1 \in \mathcal{M}$ with $m_0 \neq m_1$, we recall the definitions:

$$\begin{aligned}
P_{I,\pi}(m_i) &= \max_{a\in\mathcal{A}} \sum_{k\in\mathcal{K}(m_i,a)} P_K(k) \quad \text{for } i = 0, 1, \text{ and}\\
P^{\mathsf{cma}}_{S,\pi} &= \max_{m\in\{m_0,m_1\}} \sum_a \max_{k\in\mathcal{K}(m,a)} P_K(k).
\end{aligned}$$

Without loss of generality, we suppose $P_{I,\pi}(m_0) \ge P_{I,\pi}(m_1)$ and (m_0, a_0) satisfies

$$a_0 = \arg P_{I,\pi}(m_0).$$

Let $\mathcal{K}(m_0,a_0) = \{k_{i_1}, k_{i_2}, \ldots, k_{i_j}\}$ $(1 \le j \le s)$, and $a_{i_h} := \mathit{Auth}(k_{i_h}, m_1)$ for $1 \le h \le j$. Then, we see that $a_{i_1}, a_{i_2}, \ldots, a_{i_j}$ are all different, since all columns of $A_\pi \in \mathrm{OA}(2,s)$ are different. Therefore, for distinct $a_{i_1}, a_{i_2}, \ldots, a_{i_j}$, we have $k_{i_h} \in \mathcal{K}(m_1, a_{i_h})$ for $1 \le h \le j$, and hence

$$P^{\mathsf{cma}}_{S,\pi} \ge \sum_a \max_{k\in\mathcal{K}(m_1,a)} P_K(k) \ge \sum_{h=1}^{j} P_K(k_{i_h}) = P_{I,\pi}(m_0) = P_{I,\pi}.$$

□

Lemma 2 *For any A-code π, we have*

$$\max\{P_{I,\pi}(m_0), P_{I,\pi}(m_1)\} \leq P^{\mathsf{cma}}_{S,\pi}(m_0, m_1)$$

for all $m_0, m_1 \in \mathcal{M}$ with $m_0 \neq m_1$.

Proof. For any A-code π with a message-space $\mathcal{M}$ and arbitrary $m_0, m_1 \in \mathcal{M}$, we consider the A-code π with a restricted message-space $\bar{\mathcal{M}} := \{m_0, m_1\}$. Then, we apply Lemma 1, and the proof is completed. □

Proof of Theorem 1. Let $m_{max} \in \mathcal{M}$ be a message which gives $P_{I,\pi}$, i.e., $P_{I,\pi} = P_{I,\pi}(m_{max})$. For $m \in \mathcal{M}$ with $m \neq m_{max}$, we have

$$\begin{aligned} P_{I,\pi} &= P_{I,\pi}(m_{max}) \\ &= \max\{P_{I,\pi}(m_{max}), P_{I,\pi}(m)\} \\ &\leq P^{\mathrm{cma}}_{S,\pi}(m_{max}, m) \qquad (4) \\ &\leq \max_{m,m'} P^{\mathrm{cma}}_{S,\pi}(m, m') \\ &= P^{\mathrm{cma}}_{S,\pi}, \end{aligned}$$

where (4) follows from Lemma 2. Therefore, the proof is completed. □

Corollary 1 *For any A-code π, it holds that $P_{I,\pi} \leq P^{\mathsf{max}}_{S,\pi}$.*

Proof. The proof immediately follows from the trivial relation $P^{\mathsf{cma}}_{S,\pi} \leq P^{\mathsf{max}}_{S,\pi}$ and the inequality $P_{I,\pi} \leq P^{\mathsf{cma}}_{S,\pi}$ by Theorem 1. □

Remark 2 *One may think that the above inequalities in Theorem 1 and Corollary 1 are straightforward, since the adversary having a certain information is not less powerful than the adversary having no information. However, it does not hold that $P_{I,\pi} \leq P^{\mathsf{kma}}_{S,\pi}$ in general. To the best of author's knowledge, the above inequalities have not explicitly been mentioned before. Actually, several papers provided two kinds of proofs to show that both success probabilities of impersonation and substitution attacks of proposed A-codes are small. On the other hand, a few papers consider only the substitution attack $P^{\mathsf{cma}}_{S,\pi}$ or $P^{\mathsf{max}}_{S,\pi}$, and do not focus on the impersonation attack, e.g., see [3, Section 4] for $P^{\mathsf{cma}}_{S,\pi}$, and [18, Section II-C] for $P^{\mathsf{max}}_{S,\pi}$. This could be considered to be reasonable from the above inequalities. Furthermore, if we take into account the above inequalities, we can give a simpler security definition rather than Definition 3: π is said to be ϵ-strongly-CMA-secure if $P^{\mathsf{max}}_{S,\pi} \leq \epsilon$; and π is said to be ϵ-CMA-secure if $P^{\mathsf{cma}}_{S,\pi} \leq \epsilon$.*

Now, we show a lower bound on key-size in terms of both $P_{I,\pi}$ and $P^{\mathsf{max}}_{S,\pi}$.

Theorem 2 *Let π be an A-code having a key-source $[P_K]$. Then, for any $\alpha \in [0, \infty]$, we have*

$$R_\alpha(K) \geq -\log P_{I,\pi} P^{\mathsf{max}}_{S,\pi}.$$

Proof. The proof follows from Lemma 3 below and the fact that Rényi entropy $R_\alpha(X)$ is a monotone decreasing function of $\alpha \in [0, \infty]$.

Lemma 3 *Let π be an A-code having a key-source $[P_K]$. Then, we have $R_\infty(K) \geq -\log P_{I,\pi} P^{\mathsf{max}}_{S,\pi}$.*

Proof. For arbitrarily given $m \in \mathcal{M}$, we arrange elements in $\mathcal{A}$ by $a_1(m), a_2(m), \ldots, a_t(m)$, where $t = |\mathcal{A}|$, such that

$$\sum_{k \in \mathcal{K}(m,a_1(m))} P_K(k) \geq \sum_{k \in \mathcal{K}(m,a_2(m))} P_K(k) \geq \cdots \geq \sum_{k \in \mathcal{K}(m,a_t(m))} P_K(k).$$

Then, by considering the impersonation attack using $(m, a_1(m))$, we obtain

$$P_{I,\pi} \geq \sum_{k \in \mathcal{K}(m,a_1(m))} P_K(k). \tag{5}$$

Also, we define, for any $i \in \{1, 2, \ldots, t\}$,

$$q_i(m) := \max_{k \in \mathcal{K}(m,a_i(m))} P_K(k).$$

Then, it follows that, for any $m \in \mathcal{M}$ and any $i \in \{1, 2, \ldots, t\}$,

$$P_{S,\pi}^{\max} \geq \frac{q_i(m)}{\sum_{k \in \mathcal{K}(m,a_i(m))} P_K(k)}. \tag{6}$$

Let $k_{max} := \max_k P_K(k)$ and, for given m, suppose $k_{max} \in \mathcal{K}(m, a_j(m))$ for some $j \in \{1, 2, \ldots, t\}$. Then, we obtain

$$\begin{aligned} P_{I,\pi} P_{S,\pi}^{\max} &\geq \left(\sum_{k \in \mathcal{K}(m,a_j(m))} P_K(k) \right) \left(\frac{q_j(m)}{\sum_{k \in \mathcal{K}(m,a_j(m))} P_K(k)} \right) \qquad (7) \\ &= q_j(m) = k_{max} = \max_k P_K(k), \end{aligned}$$

where (7) follows from (5) and (6). This completes the proof. □

Remark 3 *The lower bound of Proposition 2 is a special case of Theorem 2, since it is obtained by taking $\alpha = 1$ in Theorem 2. Furthermore, by combining Theorem 2 and Corollary 1, we get*

$$R_\alpha(K) \geq -2 \log P_{S,\pi}^{\mathsf{max}}. \tag{8}$$

However, if we discuss optimality in terms of equality of the bound (8), namely, $R_\alpha(K) = -2 \log P_{S,\pi}^{\mathsf{max}}$, it is implicitly assumed that $P_{I,\pi} = P_{S,\pi}^{\mathsf{max}}$ which may be too strong condition. Therefore, we put importance on the lower bound in Theorem 2 which is more general than the bound (8). For this illustration of A-codes with 1-bit messages and 1-bit authenticators, see Proposition 4, Theorem 6, and Theorem 7 in Section 7.

Next, we show a lower bound on key-size in terms of $P_{S,\pi}^{\mathsf{kma}}$ and $P_{S,\pi}^{\mathsf{cma}}$, instead of $P_{S,\pi}^{\mathsf{max}}$.

Theorem 3 *Let π be an A-code having a key-source $[P_K]$. Then, it holds that, for any $\alpha \in [0, 2]$,*

$$R_\alpha(K) \geq -\log P_{I,\pi} P_{S,\pi}^{\mathsf{kma}}, \tag{9}$$

$$R_\alpha(K) \geq -\log P_{I,\pi} P_{S,\pi}^{\mathsf{cma}}. \tag{10}$$

Proof. The second inequality follows from the first inequality and the relation $P_{S,\pi}^{\mathsf{kma}} \leq P_{S,\pi}^{\mathsf{cma}}$. Furthermore, since $R_\alpha(X)$ is a monotone decreasing function of α (see also Proposition 6 in Appendix), we obtain the first inequality by Lemma 4 below.

Lemma 4 *For any A-code π having a key-source $[P_K]$, we have $R_2(K) \geq -\log P_{I,\pi} P_{S,\pi}^{\mathrm{kma}}$.*

Proof. By (2) in Section 4, for arbitrary $m \in \mathcal{M}$, we have

$$\mathcal{K} = \coprod_{a \in \mathcal{A}} \mathcal{K}(m,a). \tag{11}$$

For arbitrarily fixed $m \in \mathcal{M}$, we arrange elements in $\mathcal{A}$ by $a_1, a_2, \ldots, a_t$, where $t = |\mathcal{A}|$, such that

$$\sum_{k \in \mathcal{K}(m,a_1)} P_K(k) \geq \sum_{k \in \mathcal{K}(m,a_2)} P_K(k) \geq \cdots \geq \sum_{k \in \mathcal{K}(m,a_t)} P_K(k). \tag{12}$$

Then, by considering the impersonation attack using (m, a_1), we obtain

$$P_{I,\pi} \geq \sum_{k \in \mathcal{K}(m,a_1)} P_K(k).$$

We next define, for any $m \in \mathcal{M}$ and for any $i \in \{1, 2, \ldots, t\}$,

$$q_i(m) := \max_{k \in \mathcal{K}(m,a_i)} P_K(k), \tag{13}$$

$$f(m) := \sum_a P_{A|M}(a|m) \max_{(m',a') \neq (m,a)} \Pr\{\, \mathit{Vrfy}(K, (m', a')) = 1 \mid (m, a)\}. \tag{14}$$

Then, for each $i \in \{1, 2, \ldots, t\}$, we have

$$\begin{aligned} &P_{A|M}(a_i|m) \max_{(m',a') \neq (m,a)} \Pr\{\, \mathit{Vrfy}(K, (m', a')) = 1 \mid (m, a)\} \\ &\geq P_{A|M}(a_i|m) \cdot \frac{q_i(m)}{P_{A|M}(a_i|m)} = q_i(m), \end{aligned}$$

and hence, it follows that $f(m) \geq \sum_{i=1}^{t} q_i(m)$.

Therefore, for arbitrary $m \in \mathcal{M}$, we have

$$\begin{aligned} P_{I,\pi} f(m) &\geq \left(\sum_{k \in \mathcal{K}(m,a_1)} P_K(k) \right) \left(\sum_{i=1}^{t} q_i(m) \right) \\ &\geq \sum_{i=1}^{t} \left(q_i(m) \sum_{k \in \mathcal{K}(m,a_i)} P_K(k) \right) && (15) \\ &\geq \sum_{i=1}^{t} \sum_{k \in \mathcal{K}(m,a_i)} P_K(k)^2 && (16) \\ &= \sum_{k \in \mathcal{K}} P_K(k)^2, && (17) \end{aligned}$$

where (15), (16), and (17) follow from (12), (13), and (11), respectively. Hence, we obtain

$$\begin{aligned} P_{I,\pi} P_{S,\pi}^{\mathsf{kma}} &= P_{I,\pi} \left(\sum_m P_M(m) f(m) \right) \\ &= \sum_m P_M(m) \left(P_{I,\pi} f(m) \right) \\ &\geq \sum_{k \in \mathcal{K}} P_K(k)^2, && (18) \end{aligned}$$

where the last inequality (18) follows from (17). Therefore, the proof is completed. □

Remark 4 *The lower bounds in Proposition 1 are special cases of Theorem 3, since they are obtained by taking $\alpha = 0, 1$ in the lower bound (9) of Theorem 3. And the proof of Theorem 3 is essentially completed by showing the lower bound on Rényi entropy of order two of secret-keys (see Lemma 4). Our proof technique is mathematically simple and elementary compared to previous proofs of*

$$H(K) \geq -\log P_{I,\pi} P_{S,\pi}^{\mathsf{kma}}. \tag{19}$$

In fact, the traditional proof technique for the inequality (19) first shows the lower bounds on $P_{I,\pi}$ and $P_{S,\pi}^{\mathsf{kma}}$,

$$\log P_{I,\pi} \geq -I(K; MA), \quad \log P_{S,\pi}^{\mathsf{kma}} \geq -H(K \mid M, A),$$

by using the log-sum inequality and the Jensen's inequality, and next derives the bound (19) by combining these two inequalities. For this technique, for example, see [25] for A-codes and [10] for a variant of A-codes. Another proof technique for the inequality (19) is to use hypothesis testing theory, and see [15] for this technique. Our proof technique is mathematically different from these two previous techniques.

A natural question is whether the inequalities (9) and (10) hold for $\alpha \in (2, \infty]$. The following proposition shows that neither (9) nor (10) holds for $\alpha \in [5, \infty]$ in general, while we do not have the answer for the case $\alpha \in (2, 5)$.

Proposition 3 *There exists an A-code π having a key-source $[P_K]$ such that*

$$\begin{aligned} R_5(K) &< -\log P_{I,\pi} P_{S,\pi}^{\mathsf{kma}}, \\ R_5(K) &< -\log P_{I,\pi} P_{S,\pi}^{\mathsf{cma}}. \end{aligned}$$

Proof. Consider the Type-I construction π of A-codes in Section 7 having a 4-symbol-key-source whose probability distribution is given by $p_1 = 7/10$, $p_2 = p_3 = p_4 = 1/10$. Then, $P_{I,\pi} = P_{S,\pi}^{\mathsf{kma}} = P_{S,\pi}^{\mathsf{cma}} = p_1 + p_2 = 4/5$. Since $\sum_i p_i^5 > (P_{I,\pi} P_{S,\pi}^{\mathsf{cma}})^4 = (P_{I,\pi} P_{S,\pi}^{\mathsf{kma}})^4$, the two inequalities of the proposition are satisfied in this construction. □

6 Optimality of A-codes

From a theoretical viewpoint, it is important to find a construction π of A-codes having a key-source $[P_K]$ such that, given small ϵ_0 and ϵ_1 which mean security level, π satisfies $P_{I,\pi} \leq \epsilon_0$ and $P_{S,\pi}^{\mathsf{max}} \leq \epsilon_1$ requiring as short secret-keys as possible, and such a construction is often called an *optimal construction*. Thus, we are interested in (optimal) constructions π which meet our generic lower bound in Theorem 2 with equality, i.e., $R_\alpha(K) = -\log P_{I,\pi} P_{S,\pi}^{\mathsf{max}}$ for some $\alpha \in [0, \infty]$.

In this section, we try to characterize the level of optimality for various constructions for A-codes, in particular, for A-codes having not necessarily uniform random keys. To do this, by taking into account the bound in Theorem 2, we first give the following definition for the level of optimal constructions.

Definition 7 *Let π be a construction of A-codes having a key-source $[P_K]$. Then, for $\alpha \in \mathbb{N} \cup \{0, \infty\}$, π is said to be optimal of level α (α-optimal for short)[8], if π satisfies*

$$R_\beta(K) > R_\alpha(K) = -\log P_{I,\pi} P_{S,\pi}^{\mathsf{max}}$$

for all $\beta < \alpha$ with $\beta \in \mathbb{N} \cup \{0\}$.

[8] In this paper, for simplicity, we consider non-negative integers and infinity for α's values, though we can consider non-negative real numbers and infinity for α's values in general. Anyway, we will see that it is sufficient to consider only $\alpha = 0, \infty$ by Theorem 4.

The above definition seems to capture a wide range of optimal constructions. However, interestingly, we next show that the only possible α-optimality of constructions are the cases of $\alpha = 0, \infty$.

Theorem 4 *Let $\alpha \in \mathbb{N} \cup \{0, \infty\}$. Then, there exists an α-optimal construction of A-codes if and only if $\alpha = 0, \infty$.*

Proof. First, if there exists an α-optimal construction π of A-codes for some $\alpha \in \mathbb{N} \cup \{0, \infty\}$, we show $\alpha = 0, \infty$. For this, we prove that there is no α-optimal construction if $\alpha \in \mathbb{N}$. Suppose on the contrary that there exists an α-optimal construction π for some $\alpha \in \mathbb{N}$. Then, by Theorem 2 and Definition 7, we have

$$R_{\alpha-1}(K) > R_\alpha(K) = R_{\alpha+1}(K) = R_{\alpha+2}(K) = \cdots = -\log P_{I,\pi} P_{S,\pi}^{\mathsf{max}}.$$

We note that $R_\beta(K)$ is a monotone decreasing function of non-negative real numbers β, and in particular, for $\alpha, \gamma \in \mathbb{N}$ with $\alpha < \gamma$ (say, $\gamma = \alpha + 1$), it holds that $R_\alpha(K) = R_\gamma(K)$ if and only if P_K is uniform over the set $\mathrm{Supp}(P_K) := \{k \mid P_K(K) > 0\}$ (See Proposition 7 in the appendix). Without loss of generality, we suppose $\mathrm{Supp}(P_K) = \mathcal{K}$. If P_K is uniform over $\mathcal{K}$, $R_\beta(K) = \log|\mathcal{K}|$ for all $\beta \in \mathbb{N} \cup \{0, \infty\}$. Thus, in this case, π is 0-optimal, which contradicts the assumption of $\alpha \in \mathbb{N}$. Therefore, there is no α-optimal construction such that $\alpha \in \mathbb{N}$, which implies $\alpha = 0, \infty$.

Next, we show the converse part. For $\alpha = 0$, it is trivial that there exists a 0-optimal construction of A-codes, since there is already known construction π which meets $|\mathcal{K}| = (P_{I,\pi} P_{S,\pi}^{\mathsf{max}})^{-1}$. For $\alpha = \infty$, we will actually propose an ∞-optimal construction of A-codes in Sections 7 and 8. □

Note that the 0-optimal construction implies that P_K is uniform over $\mathrm{Supp}(P_K)(= \mathcal{K})$. In other words, the construction which meets $|\mathcal{K}| \geq \{P_{I,\pi} P_{S,\pi}^{\mathsf{max}}\}^{-1}$ with equality is 0-optimal, and in such a construction, uniform random keys are always required, since it holds that $\log|\mathcal{K}| = H(K)(= -\log P_{I,\pi} P_{S,\pi}^{\mathsf{max}})$. Up to date, to the best of author's knowledge, all constructions for A-codes focused on in terms of short key-size are this kind of constructions (i.e., the ones with uniform random keys). The purpose of this section is to characterize optimality of constructions of A-codes with non-uniformly random keys, and hence, it is reasonable to do it by using the other notion of optimality, namely, ∞-optimality. In this paper, we adopt the notion of ∞-optimality for optimal constructions of A-codes having non-uniformly random keys.

As explained in Section 1.3, Dodis and Spencer investigated A-codes having non-uniformly random key-sources for analyzing cryptographic sources in [3]. And, in it they focused on the min-entropy of an imperfect source and success probability of the substitution attack of an A-code. Therefore, even from this line of research, it would be reasonable to adopt our ∞-optimality for optimal constructions of A-codes having non-uniformly random keys.

7 Classification of Authentication Matrices by Group Actions

In Section 3, we have seen that any A-code with a message-set $\mathcal{M}$, an authenticator-set $\mathcal{A}$, and a key-set $\mathcal{K}$ is represented by a $|\mathcal{M}| \times |\mathcal{K}|$ matrix (i.e., authentication matrix) whose entries are chosen from $|\mathcal{A}|$-symbols. Since the cardinality of the sets are essentially important for discussing authentication matrices, we set $s = |\mathcal{M}|$ and $t = |\mathcal{A}|$. Then, for arbitrarily given distribution P_K over $\mathcal{K}$, all A-codes having $\mathcal{M}$ and $\mathcal{A}$, respectively, are represented by $s \times t^s$ matrices by considering reduced forms of authentication matrices: Since the number of all $s \times 1$ column vectors with t symbols is t^s, without loss of generality, we assume that any distribution P_K over $\mathcal{K}$ connected to A-codes having s messages and t authenticators can be given such that $|\mathcal{K}| \leq t^s$. In addition, if $|\mathcal{K}| < t^s$, we can add elements $k_{|\mathcal{K}|+1}, k_{|\mathcal{K}|+2}, \ldots, k_{t^2}$ with probabilities $P_K(k_{|\mathcal{K}|+1}) = P_K(k_{|\mathcal{K}|+2}) = \cdots = P_K(k_{t^2}) = 0$ into $\mathcal{K}$. Therefore, without loss of generality, we assume that $|\mathcal{K}| = t^s$.

Let $\mathrm{M}(s,t)$ be the set of all $s \times t^s$ arrays with entries from a set of t symbols (say, $\{0,1,2,\ldots,t-1\}$) such that every $s \times 1$ column vector with t symbols appears one time. In this section, without loss of generality, we assume that $\mathcal{M} = \{0,1,2,\ldots,s-1\}$ and $\mathcal{A} = \{0,1,2,\ldots,t-1\}$, and we deal with A-codes whose authentication matrices are reduced and given as elements of $\mathrm{M}(s,t)$. In the following, for a positive integer n, $\mathscr{S}_n$ denotes the set of all permutations over the n-symbol set $\{0,1,2,\ldots,n-1\}$.

Now, we consider the following transformations over $\mathrm{M}(s,t)$.

- For arbitrary positive integers ℓ_1, ℓ_2 with $1 \le \ell_1 \le \ell_2 \le s$, the transformation T_{ℓ_1,ℓ_2} over $\mathrm{M}(s,t)$ is defined as follows: For $A \in \mathrm{M}(s,t)$, $T_{\ell_1,\ell_2}(A)$ is the element of $\mathrm{M}(s,t)$ obtained by exchanging the ℓ_1-th row and the ℓ_2-th one of A.
- For an arbitrary positive integer ℓ with $1 \le \ell \le s$ and for arbitrary $\sigma \in \mathscr{S}_t$, the transformation $T_{\ell,\sigma}$ over $\mathrm{M}(s,t)$ is defined as follows: For $A \in \mathrm{M}(s,t)$, $T_{\ell,\sigma}(A)$ is the element of $\mathrm{M}(s,t)$ in which the ℓ-th row vector $(a_{\ell,1}, a_{\ell,2}, \ldots, a_{\ell,t^s})$ of A is replaced with the vector $(\sigma(a_{\ell,1}), \sigma(a_{\ell,2}), \ldots, \sigma(a_{\ell,t^s}))$.

Then, it is straightforward to see that the transformations above satisfy the following relation: For all integers $\ell_1, \ell_2, \ell_3 \in [1,s]$, and for all permutations $\sigma, \tau \in \mathscr{S}_t$, it holds that

$$\begin{aligned} &T_{\ell_1,\ell_1} = 1, \quad T_{\ell_2,\ell_3} = T_{\ell_1,\ell_2} T_{\ell_2,\ell_3} T_{\ell_1,\ell_3}, \\ &T_{\ell_1,id} = 1, \quad T_{\ell_1,\tau} T_{\ell_1,\sigma} = T_{\ell_1,\tau\sigma}, \\ &T_{\ell_2,\sigma} T_{\ell_1,\ell_2} = T_{\ell_1,\ell_2} T_{\ell_1,\sigma}, \end{aligned}$$

where id is the identity element of $\mathscr{S}_t$, and 1 is the identity transformation over $\mathrm{M}(s,t)$, i.e., for every $A \in \mathrm{M}(s,t)$, $1(A) = A$.

Let G be a group generated by all transformations above, i.e., $T_{\ell_1,\ell_2}(A)$ $(1 \le^{\forall} \ell_1 \le^{\forall} \ell_2 \le s)$, and $T_{\ell,\sigma}$ $(1 \le^{\forall} \ell \le s$ and $^{\forall}\sigma \in \mathscr{S}_t)$. Then, G acts on the set $\mathrm{M}(s,t)$. The reason why we consider the group G is explained by the following theorem.

Theorem 5 *For any $A \in M(s,t)$ and any $T \in G$, it holds that*

$$P_{I,\pi_A} = P_{I,\pi_{T(A)}}, \quad P^{\mathrm{cma}}_{S,\pi_A} = P^{\mathrm{cma}}_{S,\pi_{T(A)}}, \quad P^{\max}_{S,\pi_A} = P^{\max}_{S,\pi_{T(A)}},$$

namely, $P_{I,\pi_A}, P^{\mathrm{cma}}_{S,\pi_A}, P^{\max}_{S,\pi_A}$ are G-invariant.

Proof. It is not difficult to see that, by definition, each of T_{ℓ_1,ℓ_2} $(1 \le \ell_1 \le \ell_2 \le s)$ and $T_{\ell,\sigma}$ $(1 \le \ell \le s$ and $\sigma \in \mathscr{S}_t)$ does not change success probabilities of the attacks, and hence any $T \in G$ does not change them. □

Next, for arbitrarily given P_K over $(\mathcal{K}, \le_K)$, we investigate how many kinds of A-codes having the key-source $[P_K]$ can be constructed. To see this, we define an equivalence relation $\sim$ on the set $\mathrm{M}(s,t)$ by the G-action as follows: For $A, B \in \mathrm{M}(s,t)$, we define

$$A \sim B \iff B = T(A) \text{ for some } T \in G. \tag{20}$$

When we focus on $P_{I,\pi}, P^{\mathrm{cma}}_{S,\pi}, P^{\max}_{S,\pi}$ for any possible construction π for A-codes[9], it is mathematically reasonable to consider $\mathrm{M}(s,t)/\sim$ from Theorem 5. Then, we can see that there are $|\mathrm{M}(s,t)/\sim|$ kinds of constructions for A-codes.

[9] In particular, we are interested in $P_{I,\pi}$ and $P^{\max}_{S,\pi}$ in terms of ∞-optimality in this paper.

Remark 5 *Let $OA(s,t)$ be the set of all orthogonal arrays of degree s (or constraints s) and order t (or level t), namely, the set of all $s \times t^2$ arrays with entries from a set of t symbols such that, for every $2 \times t^2$ submatrix, every 2×1 column vector appears one time. It is known that an A-code which meets the lower bound with equality is well characterized by $OA(s,t)$, where $s = |\mathcal{M}|$ and $t = |\mathcal{A}|$, since a $\frac{1}{t}$-secure A-code meets $|\mathcal{K}| = t^2$ (i.e., equality of the lower bound) iff its authentication matrix becomes an element of $OA(s,t)$ and P_K is uniformly random (for example, see [2, Section 3.2] for the survey). We note that the group G considered above also acts on the set $OA(s,t)$, i.e., for ${}^{\forall}T \in G$, ${}^{\forall}A \in OA(s,t)$, $T(A) \in OA(s,t)$. Therefore, the same discussion for classifying all elements of $OA(s,t)$ is possible.*

In the following, as a simple illustration, we analyze A-codes having 1-bit messages and 1-bit authenticators (i.e., $\mathcal{M} = \mathcal{A} = \{0,1\}$) based on the discussion above. Therefore, we apply $s = t = 2$ in the above discussion. By setting $s = t = 2$ above, we note that $\mathrm{M}(2,2)$=$\mathrm{OA}(2,2)$ is the set of all 2×4 arrays with entries from the set $\{0,1\}$ such that every 2×1 column vector appears one time. For this simple case, suppose that an arbitrary key-source $[P_K]$ over a 4-symbol set $\mathcal{K} = \{k_1, k_2, k_3, k_4\}$ (say, $\mathcal{K} = \{0,1\}^2$) is given. In addition, without loss of generality, we assume that $p_i := P_K(k_i)$ for $1 \le i \le 4$ and $p_1 \ge p_2 \ge p_3 \ge p_4$.

We define two kinds of transformations over $\mathrm{M}(2,2)$ as follows.

- For $A \in \mathrm{M}(2,2)$, $T_{1,2}$ exchanges the first row and the second one of A, i.e., for $A = \begin{bmatrix} a & b & c & d \\ e & f & g & h \end{bmatrix}$, $T_{1,2}(A) := \begin{bmatrix} e & f & g & h \\ a & b & c & d \end{bmatrix}$.
- Let σ be the permutation over $\{0,1\}$ defined by $\sigma(x) = \bar{x}$ for $x \in \{0,1\}$. For $A = \begin{bmatrix} a & b & c & d \\ e & f & g & h \end{bmatrix}$, $T_{1,\sigma}(A) := \begin{bmatrix} \bar{a} & \bar{b} & \bar{c} & \bar{d} \\ e & f & g & h \end{bmatrix}$ and $T_{2,\sigma}(A) := \begin{bmatrix} a & b & c & d \\ \bar{e} & \bar{f} & \bar{g} & \bar{h} \end{bmatrix}$.

Then, we can observe that the following relations hold:

$$T_{1,2}^2 = 1, \quad T_{1,\sigma}^2 = 1, \quad T_{2,\sigma}^2 = 1,$$
$$T_{1,\sigma}T_{2,\sigma} = T_{2,\sigma}T_{1,\sigma}, \quad T_{1,\sigma}T_{1,2} = T_{1,2}T_{2,\sigma},$$

where 1 means the identity transformation, i.e., for every $A \in \mathrm{M}(2,2)$, $1(A) = A$.

Let G be the group generated by $T_{1,2}$, $T_{1,\sigma}$ and $T_{2,\sigma}$, i.e., $G := \langle T_{1,2}, T_{1,\sigma}, T_{2,\sigma} \rangle$. Then, G acts on the set $\mathrm{M}(2,2)$, and we define the equivalence relation $\sim$ on $\mathrm{M}(2,2)$ by the G-action: For $A, B \in \mathrm{M}(2,2)$, we define $A \sim B$ if and only if $B = T(A)$ for some $T \in G$. Then, we note that $|\mathrm{M}(2,2)| = 4! = 24$ and $|G| = 8$, and we obtain

$$\mathrm{M}(2,2)/\sim \; = \; \{\bar{A}_{\mathrm{I}}, \bar{A}_{\mathrm{II}}, \bar{A}_{\mathrm{III}}\},$$

where the equivalence classes $\bar{A}_{\mathrm{I}}, \bar{A}_{\mathrm{II}}, \bar{A}_{\mathrm{III}}$ are represented by

$$A_{\mathrm{I}} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}, \quad A_{\mathrm{II}} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}, \quad A_{\mathrm{III}} = \begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}.$$

From this, it follows that $\mathrm{M}(2,2)$ is divided into the following subsets by the G-action:

$$\begin{aligned} \mathrm{M}(2,2) &= G(A_{\mathrm{I}}) \amalg G(A_{\mathrm{II}}) \amalg G(A_{\mathrm{III}}), \\ G(A_i) &= \{A_i, T_{1,2}(A_i), T_{1,\sigma}(A_i), T_{2,\sigma}(A_i), (T_{1,2}T_{1,\sigma})(A_i), \\ &\qquad (T_{1,2}T_{2,\sigma})(A_i), (T_{1,\sigma}T_{2,\sigma})(A_i), (T_{1,2}T_{1,\sigma}T_{2,\sigma})(A_i)\}, \end{aligned}$$

for $i \in \{\text{I, II, III}\}$.

We say that π_A, a construction of A-codes by $A \in \mathrm{M}(2,2)$, is Type-I construction if $A \in G(A_{\mathrm{I}})$. Similarly, we call π_A Type-II (resp., Type-III) construction if $A \in G(A_{\mathrm{II}})$ (resp., $A \in G(A_{\mathrm{III}})$). In Table 2, we give success probabilities of the attacks, $P_{I,\pi}$, $P_{S,\pi}^{\max}$, and $P_{S,\pi}^{\mathrm{cma}}$, for Type-I, Type-II, and Type-III constructions.

Table 2: Success probabilities of the attacks for Type-I, Type-II, and Type-III constructions: $P_K = (p_1, p_2, p_3, p_4)$ with $p_1 \geq p_2 \geq p_3 \geq p_4$.

		Type-I	Type-II	Type-III
Substitution	$P_{S,\pi}^{\max}$	$\max(\frac{p_1}{p_1+p_3}, \frac{p_2}{p_2+p_4})$	$\frac{p_1}{p_1+p_4}$	$\frac{p_1}{p_1+p_4}$
	$P_{S,\pi}^{\mathrm{cma}}$	p_1+p_2	p_1+p_2	p_1+p_2
Impersonation	$P_{I,\pi}$	p_1+p_2	p_1+p_3	p_1+p_2

The following proposition analyzes necessary and sufficient conditions for ∞-optimality of Type-I, Type-II, and Type-III constructions, respectively.

Proposition 4 *Necessary and sufficient conditions for ∞-optimality of Type-I, Type-II, and Type-III constructions are given as follows.*

(i) A Type-I construction π_A ($A \in G(A_{\mathrm{I}})$) is ∞-optimal if and only if $p_1 \geq p_2 = p_3 \geq p_4$ and $p_1 p_4 \geq p_2^2$.

(ii) A Type-II construction π_A ($A \in G(A_{\mathrm{II}})$) is ∞-optimal if and only if $p_1 \geq p_2 \geq p_3 = p_4$.

(iii) A Type-III construction π_A ($A \in G(A_{\mathrm{III}})$) is ∞-optimal if and only if $p_1 \geq p_2 = p_3 = p_4$.

Proof. Note that the ∞-optimal condition $R_\infty(K) = -\log P_{I,\pi} P_{S,\pi}^{\mathsf{max}}$ is equivalent to

$$\max_k P_K(k) = P_{I,\pi} P_{S,\pi}^{\mathsf{max}}. \tag{21}$$

(i) From the assumption $p_1 \geq p_2 \geq p_3 \geq p_4$ and our results in Table 2, it follows that (21) holds iff $p_1 = (p_1+p_2) \cdot \max(\frac{p_1}{p_1+p_3}, \frac{p_2}{p_2+p_4})$, which is equivalent to $p_2 = p_3$ and $p_1 p_4 \geq p_2^2$.

(ii) Similarly, by our results in Table 2, (21) holds iff $p_1 = (p_1+p_3) \cdot \frac{p_1}{p_1+p_4}$, which is equivalent to $p_3 = p_4$.

(iii) Similarly again, by our results in Table 2, (21) holds iff $p_1 = (p_1+p_2) \cdot \frac{p_1}{p_1+p_4}$, which is equivalent to $p_2 = p_4$. □

Based on the above proposition, the following theorem explicitly shows which kind of construction is ∞-optimal for a given key-source over a 4-symbol set.

Theorem 6 *It holds that:*

(i) If $p_2 = p_3 = p_4$, all of Type-I, Type-II, and Type-III constructions are ∞-optimal;

(ii) If $p_2 = p_3 > p_4$, only Type-I construction is ∞-optimal;

(iii) If $p_2 > p_3 = p_4$, only Type-II construction is ∞-optimal;

(iv) Otherwise (i.e., $p_2 > p_3 > p_4$), none of Type-I, Type-II and Type-III constructions is ∞-optimal.

Proof. The proof immediately follows from Proposition 4. □

For an ϵ-strongly CMA-secure A-code π, it holds that $R_\infty(K) \geq -2\log\epsilon$ by Theorem 2 or Lemma 3. Then, we consider the following natural question: Which kind of construction satisfies the above lower bound with equality (i.e., $R_\infty(K) = -2\log\epsilon$)? For analyzing a condition for the equality, we need to consider the case $P_{I,\pi} = P_{S,\pi}^{\mathsf{max}} = \epsilon$. Therefore, we prove the following theorem to explicitly show the condition.

Theorem 7 *A necessary and sufficient condition that an A-code π satisfies ∞-optimality and $P_{I,\pi} = P_{S,\pi}^{\mathsf{max}}$ is given as follows:*

(i) If π is a Type-II or Type-III construction, P_K is uniform over $\mathcal{K}$ or deterministic.

(ii) If π is a Type-I construction, P_K is given by $p_4 = \epsilon$, $p_3 = p_2 = \sqrt{\epsilon} - \epsilon$, and $p_1 = (1-\sqrt{\epsilon})^2$ for a real number $\epsilon \in [0, 1/4]$.

Proof. First, we show the case where π is a Type-III construction. By Proposition 4, we have $p_2 = p_3 = p_4$, if π satisfies ∞-optimality. Let $p_2 = p_3 = p_4 = \epsilon \in [0,1]$ and $p_1 = 1 - 3\epsilon$. Then, by the assumption of $P_{I,\pi} = P_{S,\pi}^{\mathsf{max}}$, we have $p_1 + p_2 = \frac{p_1}{p_1+p_2}$, which is equivalent to $\epsilon - 4\epsilon^2 = 0$. From this, it follows that $\epsilon = 0$ or $\epsilon = 1/4$. Therefore, P_K is deterministic if $\epsilon = 0$, and P_K is uniform if $\epsilon = 1/4$. Conversely, if P_K is uniform over $\mathcal{K}$ or deterministic, π satisfies ∞-optimality and $P_{I,\pi} = P_{S,\pi}^{\mathsf{max}}$.

Second, we show the case where π is a Type-II construction. By Proposition 4, we have $p_3 = p_4$, if π satisfies ∞-optimality. Let $p_3 = p_4 = \epsilon \in [0,1]$, $p_2 = \delta \in [0,1]$, and $p_1 = 1 - 2\epsilon - \delta$ with the condition

$$0 \leq \epsilon \leq \delta \leq 1 - 2\epsilon - \delta \leq 1. \tag{22}$$

Then, by the assumption of $P_{I,\pi} = P_{S,\pi}^{\mathsf{max}}$, we have $p_1 + p_3 = \frac{p_1}{p_1+p_3}$, which is equivalent to $1 - 2\epsilon - \delta = (1 - \epsilon - \delta)^2$. From this, we obtain

$$\epsilon = \sqrt{\delta} - \delta. \tag{23}$$

From the condition (23) and $\epsilon \leq \delta$ by (22), it follows that $\sqrt{\delta} - \delta \leq \delta$, which is equivalent to

$$\delta = 0 \quad \text{or} \quad \delta \geq 1/4. \tag{24}$$

On the other hand, from the condition (23) and $\delta \leq 1 - 2\epsilon - \delta$ by (22), it follows that $\delta \leq 1/4$. Combining this condition with (24), we have $\delta = 0$ or $\delta = 1/4$. Therefore, P_K is deterministic if $\delta = 0$, and P_K is uniform over $\mathcal{K}$ if $\delta = 1/4$. Conversely, if P_K is uniform over $\mathcal{K}$ or deterministic, π satisfies ∞-optimality and $P_{I,\pi} = P_{S,\pi}^{\mathsf{max}}$.

Third, we show the case where π is a Type-I construction. By Proposition 4, we have $p_2 = p_3$ and $p_1 p_4 \geq p_2^2$, if π satisfies ∞-optimality. Let $p_4 = \epsilon \in [0,1]$, $p_2 = p_3 = \delta \in [0,1]$, and $p_1 = 1 - \epsilon - 2\delta$. Then, the conditions of $p_4 \leq p_3$, $p_2 \leq p_1$, and $p_1 p_4 \geq p_2^2$ are equivalent to

$$\epsilon \leq \delta, \tag{25}$$

$$\epsilon \leq 1 - 3\delta, \tag{26}$$

$$\epsilon \geq (\epsilon + \delta)^2, \tag{27}$$

respectively. In addition, by the assumption of $P_{I,\pi} = P_{S,\pi}^{\mathsf{max}}$, we have $p_1 + p_2 = \frac{p_1}{p_1+p_2}$, which is equivalent to $1-\epsilon-2\delta = (1-\epsilon-\delta)^2$. By this, we obtain

$$\delta = \sqrt{\epsilon} - \epsilon. \tag{28}$$

In addition, from (25)–(27), it follows that $0 \leq \epsilon \leq 1/4$.

Conversely, for arbitrary $\epsilon \in [0, 1/4]$, we set $\delta := \sqrt{\epsilon} - \epsilon$. Then, such ϵ and δ satisfy (25)–(27).

From the above discussion, the proof is completed. □

For considering A-codes having non-uniformly random keys, Theorem 7 explains that an interesting construction is only the Type-I construction, since other constructions require uniformly random keys or deterministic keys.

Remark 6 *It is well known that the following construction of A-codes is traditionally optimal (i.e., 0-optimal): Let $\mathbb{F}_q$ be a finite field of q elements. For a message $m \in \mathbb{F}_q$ and a secret-key $k := (b_1, b_2) \in \mathbb{F}_q^2$, a corresponding authenticator $a \in \mathbb{F}_q$ is computed by $a = Auth(k, m) := b_1 m + b_2$. For 1-bit messages and 1-bit authenticators, we set $q = 2$ in the construction above. And, we suppose that each of b_1 and b_2 is randomly generated according to the probability distribution $\Pr(b_1 = 0) = \Pr(b_2 = 0) = p$ and $\Pr(b_1 = 1) = \Pr(b_2 = 1) = 1 - p$ with some $p \in (0, 1)$. Then, this construction is traditionally optimal (i.e., 0-optimal) if $p = 1/2$ (i.e., it is uniform). However, this construction is a Type-II construction, and hence, it is not interesting from the above reason if $p \neq 1/2$.*

Furthermore, let $p := 1 - \sqrt{\epsilon}$ in (ii) of Theorem 7. Then, we have $p \in [1/2, 1]$ and

$$p_1 = p^2, \quad p_2 = p_3 = p(1-p), \quad p_4 = (1-p)^2.$$

This probability distribution is naturally captured by the von Neumann source over $\mathcal{K} = \{0,1\}^2$. In the next section, we will present construction methodology for 1-bit message A-codes from von Neumann sources in general.

8 Design of A-codes from von Neumann Sources

In this section, we explicitly show how to construct good A-codes (i.e., ∞-optimal A-codes) having 1-bit messages from von Neumann sources.

A distribution P_K over $\{0,1\}^n$ is a von Neumann source, if for $K = (K_1, K_2, \ldots, K_n)$, $P_{K_i}(0) = p \in (0,1)$ for every $1 \leq i \leq n$, i.e., K is the i.i.d. according to a binary distribution $[p, 1-p]$. For simplicity, we assume $1/2 \leq p < 1$.

In the following, for a non-negative integer z, we denote its binary string by $[z]_2$. On the other hand, for a binary string x, $[x]_{10}$ denotes the non-negative integer whose binary string is x. In this section, for a von-Neumann source $[P_K]$ over $(\{0,1\}^n, \leq_K)$, if there is no explanation about the order $\leq_K$, we assume that it is given as follows: for $x, y \in \{0,1\}^n$, we define $x \leq_K y$ if $[x]_{10} \leq [y]_{10}$.

8.1 Compositional Construction

For an $s \times u$ matrix $X = (x_{i,j})$ and an $s \times v$ matrix $Y = (y_{i,j})$, we define an $s \times uv$ matrix $Z := X \odot Y$ by

$$Z = (z_{i,j}), \quad z_{i,(j_1-1)v+j_2} := (x_{i,j_1} \parallel y_{i,j_2}) \ \text{ for } \ 1 \leq i \leq s,\ 1 \leq j_1 \leq u,\ 1 \leq j_2 \leq v,$$

where $(x \parallel y)$ means the concatenation of x and y.

Compositional Construction. Let P_{K_i} be a distribution over $(\mathcal{K}_i, \leq_{K_i})$ for $i = 1, 2$. Let $\pi_1 = ([P_{K_1}], \mathit{Auth}_1, \mathit{Vrfy}_1)$ and $\pi_2 = ([P_{K_2}], \mathit{Auth}_2, \mathit{Vrfy}_2)$ be A-codes with the same message-set $(\mathcal{M}, \leq_M)$, and suppose that A_{π_1} and A_{π_2} are the authentication matrices of π_1 and π_2, respectively. Then, we construct an A-code $\pi = ([P_K], \mathit{Auth}, \mathit{Vrfy})$ with the message-set $(\mathcal{M}, \leq_M)$ whose authentication matrix is given by $A_\pi := A_{\pi_1} \odot A_{\pi_2}$, where $(\mathcal{K}, \leq_K)$ is given as follows:

$$\begin{aligned}
&\mathcal{K} := \{k = (k_1 \parallel k_2) \mid \ k_1 \in \mathcal{K}_1 \text{ and } k_2 \in \mathcal{K}_2\},\\
&(k_1 \parallel k_2) \leq_K (k_1^* \parallel k_2^*) \text{ iff } k_1 \neq k_1^* \text{ and } k_1 \leq_{K_1} k_1^*,\\
&\qquad\qquad\qquad\qquad \text{or } k_1 = k_1^* \text{ and } k_2 \leq_{K_2} k_2^*.
\end{aligned}$$

For simplicity, we denote the A-code π obtained by the above construction by $\pi = \pi_1 \odot \pi_2$.

Remark 7 *Note that, if both A_{π_1} and A_{π_2} are reduced, $A_\pi = A_{\pi_1} \odot A_{\pi_2}$ is reduced.*

We show that π meets the following security.

Theorem 8 *The A-code $\pi = \pi_1 \odot \pi_2$ satisfies*

$$P_{I,\pi} \leq P_{I,\pi_1} \times P_{I,\pi_2}, \tag{29}$$
$$P_{S,\pi}^{\mathsf{cma}} \leq P_{S,\pi_1}^{\mathsf{cma}} \times P_{S,\pi_2}^{\mathsf{cma}}, \quad \textit{and} \tag{30}$$
$$P_{S,\pi}^{\mathsf{max}} \leq P_{S,\pi_1}^{\mathsf{max}} \times P_{S,\pi_2}^{\mathsf{max}}. \tag{31}$$

Furthermore, equality of (29) holds if there exists $m_0 \in \mathcal{M}$ such that $P_{I,\pi_i} = P_{I,\pi_i}(m_0)$ for $i = 1, 2$; equality of (30) holds if there are $m_0, m_1 \in \mathcal{M}$ such that

$$P_{S,\pi_i}^{\mathsf{cma}} = \sum_a \max_{k \in (\mathcal{K}_i)^{(R)}_{m_0,m_1}(m_0,a)} P_{(K_i)^{(R)}_{m_0,m_1}}(k)$$

for $i = 1, 2$; and equality of (31) holds if there are $m_0, m_1 \in \mathcal{M}$ such that

$$P_{S,\pi_i}^{\mathsf{max}} = \max_a \frac{\max_{k \in (\mathcal{K}_i)^{(R)}_{m_0,m_1}(m_0,a)} P_{(K_i)^{(R)}_{m_0,m_1}}(k)}{\sum_{k \in (\mathcal{K}_i)^{(R)}_{m_0,m_1}(m_0,a)} P_{(K_i)^{(R)}_{m_0,m_1}}(k)}$$

for $i = 1, 2$.

Proof. Without loss of generality, we assume that both A_{π_1} and A_{π_2} are reduced, and hence, $A_\pi = A_{\pi_1} \odot A_{\pi_2}$ is reduced (see Remark 7).

First, we show (29). For arbitrarily given $m \in \mathcal{M}$, let $(a_1 \parallel a_2) = \arg P_{I,\pi}(m)$. Then, we have

$$\begin{aligned}
P_{I,\pi}(m) &= \sum_{a_1 = \mathit{Auth}_1(k_1,m),\ a_2 = \mathit{Auth}_2(k_2,m)} P_{K_1 \| K_2}(k_1 \parallel k_2)\\
&= \sum_{a_1 = \mathit{Auth}_1(k_1,m),\ a_2 = \mathit{Auth}_2(k_2,m)} P_{K_1}(k_1) \cdot P_{K_2}(k_2)\\
&= \left(\sum_{a_1 = \mathit{Auth}_1(k_1,m)} P_{K_1}(k_1)\right)\left(\sum_{a_2 = \mathit{Auth}_2(k_2,m)} P_{K_2}(k_2)\right)\\
&= P_{I,\pi_1}(m) \times P_{I,\pi_2}(m).
\end{aligned} \tag{32}$$

Let $m_0 = \arg\max_m P_{I,\pi}(m)$. Then, it holds that

$$\begin{aligned} P_{I,\pi} &= P_{I,\pi}(m_0) \\ &= P_{I,\pi_1}(m_0) \times P_{I,\pi_2}(m_0) \\ &\leq P_{I,\pi_1} \times P_{I,\pi_2}, \end{aligned}$$

where the second equality follows from (32).

Second, we show (30). For arbitrary $m_0, m_1 \in \mathcal{M}$, we have

$$\begin{aligned} P^{\mathsf{cma}}_{S,\pi}(m_0,m_1) &= \max_{m\in\{m_0,m_1\}} \sum_{(a_1\|a_2)} \max_{(k_1\|k_2)\in\mathcal{K}^{(R)}_{m_0m_1}(m,(a_1\|a_2))} P_{(K_1\|K_2)^{(R)}_{m_0,m_1}}(k_1 \parallel k_2) \\ &= \max_{m\in\{m_0,m_1\}} \sum_{a_1}\sum_{a_2} \left(\max_{k_1\in(\mathcal{K}_1)^{(R)}_{m_0m_1}(m,a_1)} P_{(K_1)^{(R)}_{m_0m_1}}(k_1) \right) \left(\max_{k_2\in(\mathcal{K}_2)^{(R)}_{m_0m_1}(m,a_2)} P_{(K_2)^{(R)}_{m_0m_1}}(k_2) \right) \\ &= \max_{m\in\{m_0,m_1\}} \left(\sum_{a_1} \max_{k_1\in(\mathcal{K}_1)^{(R)}_{m_0m_1}(m,a_1)} P_{(K_1)^{(R)}_{m_0m_1}}(k_1) \right) \left(\sum_{a_2} \max_{k_2\in(\mathcal{K}_2)^{(R)}_{m_0m_1}(m,a_2)} P_{(K_2)^{(R)}_{m_0m_1}}(k_2) \right) \\ &\leq P^{\mathsf{cma}}_{S,\pi_1}(m_0,m_1) \times P^{\mathsf{cma}}_{S,\pi_2}(m_0,m_1). \end{aligned} \tag{33}$$

Let $(m_0, m_1) = \arg\max_{(m_0,m_1)} P^{\mathsf{cma}}_{S,\pi}(m_0,m_1)$. Then, it holds that

$$\begin{aligned} P^{\mathsf{cma}}_{S,\pi} &= P^{\mathsf{cma}}_{S,\pi}(m_0,m_1) \\ &\leq P^{\mathsf{cma}}_{S,\pi_1}(m_0,m_1) \times P^{\mathsf{cma}}_{S,\pi_2}(m_0,m_1) \\ &\leq P^{\mathsf{cma}}_{S,\pi_1} \times P^{\mathsf{cma}}_{S,\pi_2}, \end{aligned}$$

where the first inequality follows from (33).

Finally, we prove (31). For arbitrary $m_0, m_1 \in \mathcal{M}$, we have

$$\begin{aligned} P^{\mathsf{max}}_{S,\pi}(m_0,m_1) &= \max_{m\in\{m_0,m_1\}} \max_{(a_1\|a_2)} \frac{\max_{(k_1\|k_2)\in\mathcal{K}^{(R)}_{m_0m_1}(m,(a_1\|a_2))} P_{(K_1\|K_2)^{(R)}_{m_0m_1}}(k_1 \parallel k_2)}{\sum_{(k_1\|k_2)\in\mathcal{K}^{(R)}_{m_0m_1}(m,(a_1\|a_2))} P_{(K_1\|K_2)^{(R)}_{m_0m_1}}(k_1 \parallel k_2)} \\ &= \max_{m\in\{m_0,m_1\}} \max_{(a_1\|a_2)} \frac{\max_{k_1\in(\mathcal{K}_1)^{(R)}_{m_0m_1}(m,a_1),\ k_2\in(\mathcal{K}_2)^{(R)}_{m_0m_1}(m,a_2)} P_{(K_1)^{(R)}_{m_0m_1}}(k_1)\cdot P_{(K_2)^{(R)}_{m_0m_1}}(k_2)}{\sum_{k_1\in(\mathcal{K}_1)^{(R)}_{m_0m_1}(m,a_1),\ k_2\in(\mathcal{K}_2)^{(R)}_{m_0m_1}(m,a_2)} P_{(K_1)^{(R)}_{m_0m_1}}(k_1)\cdot P_{(K_2)^{(R)}_{m_0m_1}}(k_2)} \\ &= \max_{m\in\{m_0,m_1\}} \max_{(a_1\|a_2)} \left(\frac{\max_{k_1\in(\mathcal{K}_1)^{(R)}_{m_0m_1}(m,a_1)} P_{(K_1)^{(R)}_{m_0m_1}}(k_1)}{\sum_{k_1\in(\mathcal{K}_1)^{(R)}_{m_0m_1}(m,a_1)} P_{(K_1)^{(R)}_{m_0m_1}}(k_1)} \right) \left(\frac{\max_{k_2\in(\mathcal{K}_2)^{(R)}_{m_0m_1}(m,a_2)} P_{(K_2)^{(R)}_{m_0m_1}}(k_2)}{\sum_{k_2\in(\mathcal{K}_2)^{(R)}_{m_0m_1}(m,a_2)} P_{(K_2)^{(R)}_{m_0m_1}}(k_2)} \right) \\ &\leq P^{\mathsf{max}}_{S,\pi_1}(m_0,m_1) \times P^{\mathsf{max}}_{S,\pi_2}(m_0,m_1). \end{aligned} \tag{34}$$

Let $(m_0, m_1) = \arg\max_{(m_0,m_1)} P^{\mathsf{max}}_{S,\pi}(m_0,m_1)$. Then, it holds that

$$\begin{aligned} P^{\mathsf{max}}_{S,\pi} &= P^{\mathsf{max}}_{S,\pi}(m_0,m_1) \\ &\leq P^{\mathsf{max}}_{S,\pi_1}(m_0,m_1) \times P^{\mathsf{max}}_{S,\pi_2}(m_0,m_1) \\ &\leq P^{\mathsf{max}}_{S,\pi_1} \times P^{\mathsf{max}}_{S,\pi_2}, \end{aligned}$$

where the first inequality follows from (34). □

8.2 Primary Construction

Primary Construction I (by 1-bit von Neumann key-source). The first primary construction is trivial, and it is a construction for an A-code π having $\mathcal{M} = \mathcal{A} = \mathcal{K} = \{0,1\}$. Although this construction itself is not secure since $P^{\mathsf{max}}_{S,\pi} = 1$ as seen below, the construction will be effectively used in combination with other constructions.

We construct an A-code having 1-bit messages and 1-bit authenticators, $\mathcal{M} = \mathcal{A} = \{0,1\}$, and it is connected to a von-Neumann key-source $[P_K]$ over $\{0,1\}$ according to a binary distribution $[p, 1-p]$. Consider an A-code whose authentication matrix is given by

$$A = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}.$$

Then, it is easy to show the security of π_A above.

Proposition 5 *The A-code π_A constructed above satisfies $P_{I,\pi_A} = p$ and $P^{\mathsf{cma}}_{S,\pi_A} = P^{\mathsf{max}}_{S,\pi_A} = 1$, and hence it is ∞-optimal.*

Although the above A-code π_A is insecure since $P^{\mathsf{cma}}_{S,\pi_A} = P^{\mathsf{max}}_{S,\pi_A} = 1$, this construction is the *best* one of A-codes under the situation where a von-Neumann key-source $[P_K]$ over $\{0,1\}$ can be used only once. This can be observed as follows: We denote all 2×2 matrices consisting of binary elements by $\tilde{\mathrm{M}}(2,2)$, and consider the group G which acts on the set $\tilde{\mathrm{M}}(2,2)$ as in Section 7. Then, we can see that $|\tilde{\mathrm{M}}(2,2)/\sim| = 3$, and these three elements are represented by the following matrices M_1, M_2, M_3:

$$M_1 = A = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}, \quad M_2 = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \quad M_3 = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$

Then, it is seen that $P_{I,\pi_{M_i}} = P^{\mathsf{cma}}_{S,\pi_{M_i}} = P^{\mathsf{max}}_{S,\pi_{M_i}} = 1$ in the A-codes π_{M_i} for $i = 2, 3$. Hence, π_A is the best A-code from 1-bit von-Neumann key-source.

Primary Construction II (by 2-bit von Neumann key-source). We propose the second primary construction based on the results in Section 7. Here, we propose three kinds of constructions of A-codes with 1-bit messages and 1-bit authenticators, $\mathcal{M} = \mathcal{A} = \{0,1\}$, by using 2-bit von Neumann key-source $[P_K]$ over $\{0,1\}^2$, where P_K consists of probabilities $p_1 \geq p_2 \geq p_3 \geq p_4$ given by

$$p_1 := P_K(00) = p^2,\ p_2 := P_K(01) = p(1-p),\ p_3 := P_K(10) = p(1-p),\ p_4 := P_K(11) = (1-p)^2.$$

In Section 7, it is shown that there exist three kinds of constructions of A-codes, and they are called, Type-I, Type-II, and Type-III constructions. In Table 3, we summarize success probabilities of the attacks for those constructions. Note that only the Type-I construction among the three is ∞-optimal.

Table 3: Success probabilities of the attacks for Type-I, Type-II, and Type-III constructions from von-Neumann sources over $\{0,1\}^2$: $p_1 = p^2$, $p_2 = p_3 = p(1-p)$, and $p_4 = (1-p)^2$.

		Type-I	Type-II	Type-III
Substitution	$P^{\max}_{S,\pi}$	p	$\frac{p^2}{p^2+(1-p)^2}$	$\frac{p^2}{p^2+(1-p)^2}$
	$P^{\mathrm{cma}}_{S,\pi}$	p	p	p
Impersonation	$P_{I,\pi}$	p	p	p

8.3 ∞-optimal Constructions

In this section, we show explicitly ∞-optimal constructions of A-codes by using von Neumann key-sources $[P_K]$ over $\{0,1\}^n$ according to a binary distribution $[p, 1-p]$.

We consider the simple case of A-codes, namely, A-codes having 1-bit messages (i.e., $\mathcal{M} = \{0,1\}$). For any positive integer n and arbitrary non-negative integers i, j such that $0 \leq j \leq \lfloor n/2 \rfloor$ and $i + j = n$, we can construct an A-code π such that $(P_{I,\pi}, P^{\max}_{S,\pi}) = (p^i, p^j)$ as follows. Let π_I be the Type-I construction by using the 2-bit von-Neumann key-source over $\{0,1\}^2$. Then, for arbitrary j with $0 \leq j \leq \lfloor n/2 \rfloor$, we construct the A-code $\pi_I^{(j)}$ by applying the compositional construction j times, i.e.,

$$\pi_I^{(j)} := \underbrace{\pi_I \odot \cdots \odot \pi_I}_{j \text{ times}}.$$

Then, since $(P_{I,\pi_I}, P^{\max}_{S,\pi_I}) = (p, p)$ (see Table 3), we have $(P_{I,\pi_I^{(j)}}, P^{\max}_{S,\pi_I^{(j)}}) = (p^j, p^j)$ by Theorem 8. Next, let π_0 be the A-code construction explained in primary construction I by using the 1-bit von-Neumann key-source over $\{0,1\}$. Then, we define the A-code

$$\pi := \underbrace{\pi_0 \odot \cdots \odot \pi_0}_{i-j \text{ times}} \odot \pi_I^{(j)}.$$

For the A-code π, we have $(P_{I,\pi}, P^{\max}_{S,\pi}) = (p^i, p^j)$ by Theorem 8 and Proposition 5. We note that the above A-code π satisfying $(P_{I,\pi}, P^{\max}_{S,\pi}) = (p^i, p^j)$ $(i + j = n)$ is ∞-optimal, since it meets $R_\infty(K) = -\log P_{I,\pi} P^{\max}_{S,\pi}$, i.e., the equality of the lower bound. In Table 4, we summarize all possible $(P_{I,\pi}, P^{\max}_{S,\pi})$ achieved by this construction method. In particular, by the method above, we have an ∞-optimal A-code π having security $P^{\max}_{S,\pi} = p^{\lfloor n/2 \rfloor}$ and $P_{I,\pi} = p^{\lceil n/2 \rceil}$, in which $P^{\max}_{S,\pi}$ is minimized.

Table 4: Realizable ∞-optimal A-codes with 1-bit messages from von Neumann sources over $\{0,1\}^n$.

	P_K over $\{0,1\}^n$								
	$n=1$	$n=2$	$n=3$	$n=4$	$n=5$	$n=6$	$\cdots$	n	$\cdots$
$(P_{I,\pi}, P^{\max}_{S,\pi})$	$(p,1)$	(p,p)	(p^2,p)	(p^3,p) (p^2,p^2)	(p^4,p) (p^3,p^2)	(p^5,p) (p^4,p^2) (p^3,p^3)	$\cdots$ $\cdots$ $\cdots$	(p^i,p^j) $0 \leq j \leq \lfloor n/2 \rfloor$ $i+j=n$	$\cdots$ $\cdots$ $\cdots$

8.4 Constructions by von Neumann Extractors and 0-optimal A-codes

Suppose that a von Neumann source $[P_K]$ over $\{0,1\}^n$ according to a binary distribution $[p, 1-p]$ is given. Then, in order to construct an A-code, one may think the following procedures: First, by using a randomness extractor, we extract a uniform random bits from $[P_K]$; and next, we apply an existing optimal construction of A-codes requiring uniform random keys (i.e., a construction called *0-optimal* in this paper). In this section, we analyze performance of the procedure. Since our purpose is to construct A-codes from a given non-uniformly random key-source, we only consider deterministic extractors. The most famous and important deterministic extractors for von Neumann sources include the von Neumann extractor [30] and its improved ones [5, 17]. We investigate A-codes constructed from those extractors, and compare the performance of such a construction of A-codes with ∞-optimal constructions in the previous section in the scenario of 1-bit message A-codes, for simplicity.

For an input sequence $(x_1, x_2, \ldots, x_n)$ from $[P_K]$, the *von Neumann extractor* [30] outputs a uniform random sequence by the following procedure: First, divide the n input bits into pairs $(x_{2i-1}x_{2i})$ for $i = 1, 2, \ldots$; and then, for $i = 1, 2, \ldots$, it outputs $\perp$ if $(x_{2i-1}x_{2i}) = (00)$ or (11), outputs 0 if $(x_{2i-1}x_{2i}) = (01)$, and outputs 1 if $(x_{2i-1}x_{2i}) = (10)$, where $\perp$ means no output. Once a 1-bit $b \in \{0, 1\}$ is output, it satisfies $\Pr\{b = 0\} = \Pr\{b = 1\} = p(1-p)$ and be uniformly random. From the n biased bits, the von Neumann extractor asymptotically (i.e., for sufficiently large n) extracts $u = np(1-p)$ uniformly random bits.

Then, we select a 0-optimal A-code π_1 (e.g., by using polynomials, projective spaces, or orthogonal arrays [2, 1, 12]) having u uniformly random keys, and its security is evaluated by

$$P^{\mathsf{max}}_{S,\pi_1} = \frac{1}{2^{u/2}} = \left(\frac{1}{2^{p(1-p)}}\right)^{n/2}.$$

On the other hand, as explained in Section 8.3 (see also Table 4), we can construct an ∞-optimal A-code π_2 such that $P^{\mathsf{max}}_{S,\pi_2} = p^{n/2}$. Since $p < (\frac{1}{2^{p(1-p)}})$ for any $p \in (1/2, 1)$, we obtain $P^{\mathsf{max}}_{S,\pi_2} < P^{\mathsf{max}}_{S,\pi_1}$ for arbitrary p, which concludes that the ∞-optimal construction π_2 is superior to π_1 constructed by combining the von Neumann extractor and 0-optimal construction.

We next consider applying the *iterated von Neumann extractor* [17], instead of the von Neumann extractor, which achieves the information-theoretic bound (the entropy bound). We do not describe the procedure of the iterated von Neumann extractor, since it is more complicated than that of the von Neumann extractor (see [17] for details). Roughly speaking, the iterated procedures in it are defined recursively on $\nu \geq 1$, where ν is the number of iteration, and it coincides with the von Neumann extractor when $\nu = 1$. Let $r_\nu(p)$ be the *rate* of the ν-iterated extractor, and in particular, $r_1(p) = p(1-p)$ (i.e., the rate of the von Neumann extractor). Then, it is shown in [17] that $r_\nu(p)$ is a monotone increasing function of ν and $r_\infty(p) := \lim_{\nu\to\infty} r_\nu(p) = h(p)$ (the entropy bound), where $h(\cdot)$ is the binary entropy function. Suppose that we first apply the ν-iterated von Neumann extractor to obtain asymptotically $u = nr_\nu(p)$ uniformly random bits, and next apply a 0-optimal A-code having u-bit uniformly random keys, Then, the security of the resulting A-code π_3 is evaluated by

$$P^{\mathsf{max}}_{S,\pi_3} = \left(\frac{1}{2^{r_\nu(p)}}\right)^{n/2}.$$

Here, for arbitrary $p \in (1/2, 1)$, it holds that

$$\left(\frac{1}{2^{h(p)}}\right)^{n/2} < \left(\frac{1}{2^{r_\nu(p)}}\right)^{n/2} < \left(\frac{1}{2^{p(1-p)}}\right)^{n/2} \text{ and } \left(\frac{1}{2^{h(p)}}\right)^{n/2} < p^{n/2} < \left(\frac{1}{2^{p(1-p)}}\right)^{n/2}.$$

Hence, if ν is large enough, the ∞-optimal construction π_2 is inferior to π_3 above in security. To see this more explicitly, we define an *authentication rate* of an A-code π by

$$a_\pi(p) := \frac{-2\log P^{\mathsf{max}}_{S,\pi}}{n}.$$

Then, we obviously have $a_{\pi_1}(p) = \nu_1(p) = p(1-p)$, $a_{\pi_2}(p) = -\log p$, and $a_{\pi_3}(p) = r_\nu(p)$ for $p \in [1/2, 1)$. The graphs of these authentication rates are given in Figure 1[10].

Finally, we summarize the comparison of the ∞-optimal A-code π_2 with the A-codes π_1, π_3 constructed by the (iterated) von Neumann extractor and 0-optimal constructions.

[10]For $a_{\pi_3}(p)$, the cases of $\nu = 2, \infty$ are calculated and drawn.

- The achievable security by using the (iterated) von Neumann extractor is evaluated only in terms of its asymptotical behavior (i.e., for a sufficiently large n), and the security of π_1, π_3 above is not necessarily guaranteed for an actual finite n. On the other hand, the achievable security of π_2 is strict and always be possible, since we have not used asymptotical arguments in its analysis.

- Even in asymptotical analysis, π_2 is superior to π_1 for arbitrary $p \in [1/2, 1)$.

- In asymptotical analysis, π_3 is superior to π_2 for arbitrary $p \in (1/2, 1)$, if the number of iteration ν is sufficiently large (i.e., $\nu \to \infty$). However, this may be unrealistic, since we need to select a finite ν so that its time complexity is reasonable in a real world. Actually, the time complexity of the ν-iterated von Neumann extractor depends on ν, and it is evaluated as $T_\nu(n) = O(\nu T_1(n) + (\nu - 1)n)$ bit-operations, where $T_1(n)$ is time complexity of the von Neumann extractor. Furthermore, the selection of ν such that π_3 is superior to π_2 depends on (not explicitly known) p, and we need to select such ν if the range of $p \in [\frac{1}{2}, 1)$ can be more precisely evaluated[11]. If such selection of ν is not possible, there will be no advantage to use π_3 rather than π_2.

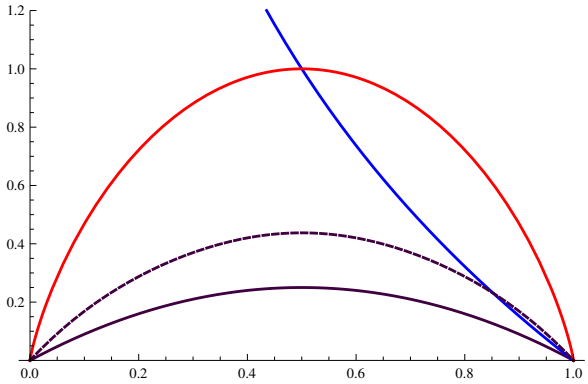

Figure 1: Graphs of authentication rates of A-codes for $p \in [1/2, 1)$: The black curve means $a_{\pi_1}(p) = r_1(p) = p(1-p)$, the black dashed curve means $r_2(p) = pq + \frac{1}{2}(p^2+q^2)(1-p^2-q^2) + \frac{1}{2}p^2q^2(p^2+q^2)^{-1}$, where $q = 1-p$, the red curve means $r_\infty(p) = h(p) = -p\log p - (1-p)\log(1-p)$ (i.e., the binary entropy function), and the blue curve means $a_{\pi_2}(p) = -\log p$ which is realizable by our methodology.

9 Concluding Remarks

In this paper, we have shown:

(i) Tight lower bound on the min-entropy of keys in terms of success probabilities of both impersonation and substitution attacks, and reasonability of basing optimality of A-codes having non-uniformly random keys on it;

(ii) Methodology of classifying realizable A-codes with non-uniformly random keys by equivalence classes, and illustration of this for small parameters (i.e., A-codes with 1-bit messages and 1-bit authenticators);

[11] For example, if p can be evaluated as $p \in [\frac{1}{2} + \delta, 1)$ for some $0 \ll \delta < 1/2$, small ν may be enough to guarantee that π_3 is superior to π_2. However, if $p \approx 1/2$, large ν would be required to guarantee that π_3 is superior to π_2 (see also Figure 1).

(iii) Methodology of optimal constructions for 1-bit-message A-codes from von Neumann sources.

For further development of authentication theory based on non-uniformly random key-sources, it would be interesting to reveal:

- Methodology of optimal constructions for A-codes with long messages; and
- Methodology of optimal constructions for A-codes from a large class of non-uniformly random key-sources.

References

[1] J. L. Carter, and M. N. Wegman, Universal classes of hash functions, Journal of Computer and System Sciences, 18, pp.143–154, 1979.

[2] J. C. Colbourn, and H. J. Dinitz, *The CRC Handbook of Combinatorial Designs*, CRC Press, Inc., 1996.

[3] Y. Dodis, and J. Spencer, On the (non)universality of the one-time pad, The 43rd IEEE Symposium on Foundations of Computer Science (FOCS2002), pp.376–388, 2002.

[4] Y. Dodis, and D. Wichs, Non-malleable extractors and symmetric key cryptography from weak secrets, ACM Symposium on Theory of Computing (STOC09), pp.601–610, 2009.

[5] P. Elias, The efficient construction of an unbiased random sequence, The Annals of Mathematical Statistics, 1972, Vol.43, No.3, pp.865–870.

[6] V. Fåk, Repeated use of codes which detect deception, IEEE Trans. Information Theory, vol.25, no.2, pp.233–234, 1979.

[7] E. N. Gilbert, F. J. MacWilliams, and N. J. A. Sloane, Codes which detect deception, Bell Tech. J. **53**, pp.405–424, 1974.

[8] P. Godlewski, and C. Mitchell, Key-minimal cryptosystems for unconditional secrecy, J. Cryptology, Vol.3, pp.1–25, 1990.

[9] M. Iwamoto, and J. Shikata, Information-theoretic security for encryption based on conditional Rényi entropies, ICITS2013, LNCS 8317, pp.103-121, Springer, 2014. The full version is available at `http://eprint.iacr.org/2013/440`

[10] T. Johansson, Lower bounds on the probability of deception in authentication with arbitration, IEEE Trans. Inform. Theory 40, 5, pp.1573-1585, 1994.

[11] T. Johansson, Further results on asymmetric authentication schemes, Information and Computation, 151, pp.100-133, 1999.

[12] G. Longo, M. Marchi, and A. Sgarro (eds.), Geometries, Codes and Cryptography, International Centre for Mechanical Sciences, Volume 313, Springer, 1990.

[13] J. Massey, Cryptography: a selective survey, Alta Frequenza, LV (1), pp.4–11, 1986.

[14] J. Massey, Contemporary cryptology: an introduction, In Contemporary Cryptology, IEEE Press, New York, pp.1–39, 1991.

[15] U. Maurer, Authentication theory and hypothesis testing, IEEE Trans. Information Theory, vol. 46, no. 4, pp.1350–1356, July 2000.

[16] D. Pei, Information-theoretic bounds for authentication codes and block designs, J. Cryptology 8, pp.177–188, 1995.

[17] Y. Peres, Iterating von Neumann's procedure for extracting random bits, The annals of statistics, 1992, Vol.20, No.1, pp.590–597.

[18] C. Portmann, Key recycling in authentication, IEEE Trans. Information Theory, Vol.60, No.7, pp.4383–4396, July 2014.

[19] A. Rényi, On measures of information and entropy, Proc. of the 4th Berkeley Symposium on Mathematics, Statistics and Probability 1960 (1961), pp.547–561.

[20] U. Rosenbaum, A lower bound on authentication after having observed a sequence of messages, J. Cryptology 6, pp.135-156, 1993.

[21] R. Safavi-Naini, and H. Wang, Multireceiver authentication codes: models, bounds, constructions and extensions, Information and Computation, 151, pp.148-172, 1999.

[22] A. Sgarro, Information-theoretic bounds for authentication frauds, J. Comput. Security 2, pp.53-63, 1993.

[23] C. E. Shannon, Communication theory of secrecy systems, Bell System Technical Journal 28, pp.656–715, 1949.

[24] J. Shikata, G. Hanaoka, Y. Zheng, and H. Imai, Security notions for unconditionally secure signature schemes, Advances in Cryptology - EUROCRYPT 2002, LNCS 2332, pp.434-449, Springer, 2002.

[25] G. J. Simmons, Authentication theory/coding theory, Advances in Cryptology - CRYPTO '84, LNCS 196, pp.411–432, Springer, 1985.

[26] B. Smeets, Bounds on the probability of deception in multiple authentication, IEEE Trans. Information Theory, vol.40, no.5, pp.1586-1591, 1994.

[27] D. Stinson, Some constructions and bounds for authentication codes, J. Cryptology, vol.1, no.1, pp.37-51, 1988.

[28] D. Stinson, Universal hashing and authentication codes, Designs, Codes and Cryptography, 4 (3), pp. 369–380, 1994.

[29] D. Stinson, Some constructions and bounds for authentication codes, J. Cryptology, vol.1, no.1, pp.37-51, 1988.

[30] J. von Neumann, Various technique used in connection with random digits, Monte Carlo Method, Applied Mathematics Series, No.12, U.S. National Bureau of Standards, Washington D.C., pp.36–38, 1951.

[31] M. Walker, Information-theoretic bound for authentication schemes, J. Cryptology, Vol.2, No.3, pp.131–143, 1990.

Appendix: Rényi Entropy

Definition 8 ([19]) *Let X be a random variable taking values in a finite set $\mathcal{X}$. For $\alpha \in [0,\infty]$, the Rényi entropy of order α is defined by*

$$R_\alpha(X) := \frac{1}{1-\alpha}\log \sum_{x\in \mathrm{Supp}(P_X)} P_X(x)^\alpha,$$

where the cases of $\alpha = 1,\infty$ are meant to take the limits at such α, respectively.

It is known that various entropies such as Hartley entropy ($\alpha = 0$), Shannon entropy ($\alpha = 1$), collision entropy ($\alpha = 2$), and min-entropy ($\alpha = \infty$) are special cases of Rényi entropy as follows:

$$\begin{aligned} R_0(X) &= \log|\mathrm{Supp}(P_X)|, \\ R_1(X) &= -\sum_{x\in \mathrm{Supp}(P_X)} P_X(x)\log P_X(x), \\ R_2(X) &= -\log \Pr\{X = X'\}, \\ R_\infty(X) &= \min_{x\in \mathrm{Supp}(P_X)} \{-\log P_X(x)\}, \end{aligned}$$

where X and X' are independently and identically distributed (i.i.d.) random variables.

In addition, the following result on the Rényi entropy is well-known.

Proposition 6 *Let X be a random variable taking values in a finite set $\mathcal{X}$. Then, $R_\alpha(X)$ is a monotone decreasing function of $\alpha \in [0,\infty]$.*

Furthermore, we investigate the condition when the equality $R_\alpha(X) = R_\beta(X)$ ($\alpha \neq \beta$) holds for $\alpha,\beta \in \mathbb{N}\cup\{0\}$ in details, since this condition is used to discuss optimality of A-codes in Section 6. The proof of the following proposition is not difficult, and it follows by carefully investigating equality condition in the well-known proof of Proposition 6.

Proposition 7 *Suppose $\alpha,\beta \in \mathbb{N}\cup\{0\}$ with $\alpha < \beta$. Let X be a random variable taking values in a finite set $\mathcal{X}$. Then, $R_\alpha(X) = R_\beta(X)$ if and only if the distribution P_X is uniform over Supp(P_X).*

Proof. Without loss of generality, we prove the statement by using $\ln(\cdot)$ for the logarithm. In addition, it is sufficient to prove the case $\beta = \alpha + 1$, and we show it in the following.

First, let α be a variable taking real numbers in $(1,\infty)$. Then, we have

$$\begin{aligned} (1-\alpha)^2\frac{d}{d\alpha}R_\alpha(X) &= (1-\alpha)\sum_x \left(\frac{P_X(x)^\alpha}{\sum_x P_X(x)^\alpha}\right)\ln P_X(x) + \ln\sum_x P_X(x)^\alpha \\ &= \sum_x Q_X(x)\left(\ln P_X(x)^{1-\alpha}\right) + \ln\sum_x P_X(x)^\alpha \\ &\le \ln\sum_x Q_X(x)\ln P_X(x)^{1-\alpha} + \ln\sum_x P_X(x)^\alpha \qquad (35) \\ &= -\ln\sum_x P_X(x)^\alpha + \ln\sum_x P_X(x)^\alpha \\ &= 0, \end{aligned}$$

where $Q_X(x) := P_X(x)^\alpha/\sum_x P_X(x)^\alpha$ for $x\in\mathcal{X}$, and (35) follows from Jensen's inequality. Moreover, it should be noted that equality in (35) holds if and only if $P_X(x)$ are equal for all $x \in \mathrm{Supp}(P_X)$.

Therefore, in particular, for $\alpha, \beta \in \mathbb{N}$ with $1 < \alpha < \beta$, it holds that $R_\alpha(X) = R_\beta(X)$ if and only if the distribution P_X is uniform over $\mathrm{Supp}(P_X)$.

Second, we show that $R_0(X) = R_1(X)$ if and only if P_X is uniform over $\mathrm{Supp}(P_X)$. However, this is the well-known fact, since $R_0(X) = R_1(X)$ is equivalent to $H(X) = \ln |\mathrm{Supp}(P_X)|$.

Third, we show that $R_1(X) = R_2(X)$ if and only if P_X is uniform over $\mathrm{Supp}(P_X)$. Let $s \in (0, 1)$ be a real number, and then, we have $R_1(X) \geq R_{1+s}(X) \geq R_2(X)$ by Proposition 6. Suppose $R_1(X) = R_2(X)$, then we get $R_{1+s}(X) = R_2(X)$. Furthermore, by the equality condition in (35), it follows that P_X is uniform over $\mathrm{Supp}(P_X)$. Conversely, it is straightforward that we have $R_1(X) = R_2(X)$ if P_X is uniform over $\mathrm{Supp}(P_X)$.

Therefore, the proof is completed. □