PAPER *Special Section on Discrete Mathematics and Its Applications*

Unconditionally Secure Authenticated Encryption

Junji SHIKATA[†a)], ***Member***, **Goichiro HANAOKA**[††b)], ***Nonmember***, **Yuliang ZHENG**[†††c)],
Tsutomu MATSUMOTO[†d)], ***Members, and*** **Hideki IMAI**[††e)], ***Fellow***

SUMMARY In this paper, we formally define and analyze the security notions of authenticated encryption in unconditional security setting. For confidentiality, we define the notions, *APS (almost perfect secrecy)* and *NM (non-malleability)*, in terms of an information-theoretic viewpoint along with our model where multiple senders and receivers exist. For authenticity, we define the notions, *IntC (integrity of ciphertexts)* and *IntP (integrity of plaintexts)*, from a view point of information theory. And then we combine the above notions to define the security notions of unconditionally secure authenticated encryption. Then, we analyze relations among the security notions. In particular, it is shown that the strongest security notion is the combined notion of APS and IntC. Finally, we formally define and analyze the following generic composition methods in the unconditional security setting along with our model: *Encrypt-and-Sign*, *Sign-then-Encrypt* and *Encrypt-then-Sign*. Consequently, it is shown that: the Encrypt-and-Sign composition method is not always secure; the Sign-then-Encrypt composition method is not always secure; and the Encrypt-then-Sign composition method is always secure, if a given encryption meets APS and a given signature is secure.

key words: *unconditional security, encryption, authenticated encryption, signcryption*

1. Introduction

Confidentiality (secrecy) and authenticity are currently fundamental cryptographic functions, and encryption and signature are usually used for providing confidentiality and authenticity, respectively. Although encryption and signature have been mainly studied in the separate context, there are many applications where both are needed. A cryptographic technique which provides both confidentiality and authenticity is often called *authenticated encryption*, and we also use this term in this paper. In order to study the authenticated encryption, it is important to have a formal notion of what a secure authenticated encryption scheme is, and to construct an authenticated encryption which can be proven to be secure in the formal notion. In this paper, we formally define and analyze the security notions of authenticated encryption in unconditional security setting.

1.1 Related Works

Computational Security: Joint signature and encryption is studied in the public-key setting in [20] with the aim of achieving greater efficiency than simply carrying out signature and encryption separately. We remark that in [20] the term *signcryption* is introduced to represent the notion of joint signature and encryption instead of authenticated encryption. Recently, the proofs for the security of signcryption are provided in [2].

Very recently, in [1] the notions of joint encryption and signature are formally studied in the public-key setting. The paper [1] formally defines confidentiality and authenticity for authenticated encryption (signcryption) and analyzes the security of authenticated encryption (signcryption) designed by three types of *generic compositions* based on the use of a public-key encryption and a digital signature: *Encrypt-then-Sign*, *Sign-then-Encrypt*, and *Commit-then-Encrypt-then-Sign*.

On the other hand, in [4] and [15], joint notions of confidentiality and authenticity for symmetric encryption schemes are considered. In particular, in [4] formal definitions of secrecy and authenticity for symmetric encryption schemes are presented, and relations among the notions are revealed. In addition, the paper [4] analyzes the security of authenticated encryption schemes designed by three types of *generic compositions* based on the use of a symmetric encryption scheme and a MAC: *Encrypt-and-MAC*, *MAC-then-Encrypt*, and *Encrypt-then-MAC*.

Unconditional Security: In unconditional security setting, cryptographic schemes which provide both authenticity and confidentiality have been studied (for example, see [6], [7], [16], [19]). The security notions for authenticity are mainly *impersonation* and *substitution (spoofing)*. However, as shown in [12], [18], there exist stronger security notions and it is not enough to only consider impersonation and substitution (spoofing) if we require strong security for authenticity. On the other hand, the security notion for confidentiality under consideration in existing authenticated encryption schemes is mainly the perfect secrecy introduced by Shannon [17]. However, in addition to the notion, we should also consider the notion of *non-malleability* from an

Manuscript received August 26, 2003.
Manuscript revised December 9, 2003.
Final manuscript received January 6, 2004.

[†] The authors are with the Graduate School of Environment and Information Sciences, Yokohama National University, Yokohama-shi, 240-8501 Japan.

[††] The authors are with the Institute of Industrial Science, the University of Tokyo, Tokyo, 153-8505 Japan.

[†††] The author is with the Department of Software and Information Systems, University of North Carolina at Charlotte, 9201, University City Blvd, Charlotte, NC 28223, USA.

a) E-mail: shikata@ynu.ac.jp
b) E-mail: hanaoka@imailab.iis.u-tokyo.ac.jp
c) E-mail: yzheng@uncc.edu
d) E-mail: tsutomu@mlab.jks.ynu.ac.jp
e) E-mail: imai@iis.u-tokyo.ac.jp

information-theoretic viewpoint if we require strong security for confidentiality as in computational security.

1.2 Our Results

In this paper, as mentioned before, we formally define and analyze the security notions of authenticated encryption in unconditional security setting.

For confidentiality, we introduce the notions, *APS (almost perfect secrecy)* and *NM (non-malleability)*, in terms of an information-theoretic viewpoint along with our model where multiple senders and receivers exist. The notion of APS is a straightforward relaxed notion of prefect secrecy by Shannon [17]. The notion NM is newly defined in the context of unconditional security based on the idea of NM in computational security [3], [4], [8], [9]. On the other hand, for authenticity, we define the notions, *IntC (integrity of ciphertexts)* and *IntP (integrity of plaintexts)*, from a view point of information theory along with our model. The notions, IntC and IntP, are newly defined in the context of unconditional security based on the idea of that of computational security setting [4].

Next, we combine the above notions of confidentiality and authenticity to define the security notions of unconditionally secure authenticated encryption. And, we analyze relations among the security notions under consideration. As a result, in particular, it is shown that the strongest security notion is the combined notion of APS and IntC.

Finally, we formally define and analyze the following generic composition methods in the unconditional security setting along with our model: *Encrypt-and-Sign*, *Sign-then-Encrypt* and *Encrypt-then-Sign*. Consequently, it is shown that: the Encrypt-and-Sign composition method is not always secure; the Sign-then-Encrypt composition method is not always secure; and the Encrypt-then-Sign composition method is always secure, if a given encryption meets APS and a given signature is secure.

The rest of this paper is organized as follows: in Sect. 2, we formally define cryptographic models and formalize security notions from information-theoretic viewpoints. In particular, we define the model of authenticated encryption with unconditional security, and formalize the security notions, APS, NM, IntC and IntP, for authenticated encryption in unconditional security setting; in Sect. 3, we analyze relations among the security notions for authenticated encryption, and show that the strongest security notion is the combined notion of APS and IntC; and finally, in Sect. 4, we formally define and analyze the generic composition methods, Encrypt-and-Sign, Sign-then-Encrypt and Encrypt-then-Sign. In particular, we show that Encrypt-and-Sign and Sign-then-Encrypt methods are not always secure while Encrypt-then-Sign method is always secure, if a given encryption meets APS and a given signature is secure.

2. The Model

In this section, we consider cryptographic models and formalize security notions in terms of information theory.

In this paper, we use the following notations: For a finite set $\mathcal{X}$, let X be a random variable which takes on the set $\mathcal{X}$ with probability distribution $\Pr_X$. Here, the probability that X takes a value $x \in \mathcal{X}$ is denoted by $\Pr_X(x)$ and briefly $\Pr(x)$ if X and $\mathcal{X}$ are clear in the context. Also, let X_1 (resp. X_2) be a random variable which takes on the finite set $\mathcal{X}_1$ (resp. $\mathcal{X}_2$) with probability distribution $\Pr_{X_1}$ (resp. $\Pr_{X_1}$). Then, the conditional probability that $X_1 = x_1$ $(\in \mathcal{X}_1)$ given $X_2 = x_2$ $(\in \mathcal{X}_2)$ is denoted by $\Pr_{X_1|X_2}(x_1|x_2)$ and briefly $\Pr(x_1|x_2)$ if X_1, X_2, $\mathcal{X}_1$ and $\mathcal{X}_2$ are clear in the context.

2.1 A Model of Encryption and Authenticated Encryption Schemes with Unconditional Security

In this subsection, we describe a model of encryption and authenticated encryption with unconditional security, and introduce formal definitions of security.

First, we start with the following model of unconditionally secure encryption where multiple senders and receivers exist.

Definition 1: (Encryption) An *encryption scheme* Π consists of
($\mathcal{U}$, TA, $\mathcal{M}$, $\mathcal{C}$, $\mathcal{E}$, $\mathcal{D}$, *GEN*, *ENC*, *DEC*):

1. **Notation:**
   - $\mathcal{U} := \{S_1, S_2, \ldots, S_{n_1}, R_1, R_2, \ldots, R_{n_2}\}$ is a finite set of users, where $S_i (1 \le i \le n_1)$ are senders and $R_i (1 \le i \le n_2)$ are receivers. Let $\mathcal{U}_S := \{S_1, S_2, \ldots, S_{n_1}\}$ and $\mathcal{U}_R := \{R_1, R_2, \ldots, R_{n_2}\}$. We also use S_i (resp. R_j) as S_i's (resp. R_j's) identity.
   - TA is a trusted authority.
   - $\mathcal{M} = \{\mathcal{M}_k\}_{k \in \boldsymbol{N}}$ is a sequence of finite sets of possible plaintexts. Here, k is a security parameter and $\mathcal{M}_k \subset \{0, 1\}^{l_M(k)}$, where $l_M(k)$ is a polynomial of k.
   - $\mathcal{C} = \{\mathcal{C}_k\}_{k \in \boldsymbol{N}}$ is a sequence of finite sets of possible ciphertexts. Here, $\mathcal{C}_k \subset \{0, 1\}^{l_C(k)}$, where $l_C(k)$ is a polynomial of k.
   - $\mathcal{E} = \{\mathcal{E}_k\}_{k \in \boldsymbol{N}}$ is a sequence of finite sets of possible encryption-keys. Here, $\mathcal{E}_k \subset \{0, 1\}^{l_E(k)}$, where $l_E(k)$ is a polynomial of k.
   - $\mathcal{D} = \{\mathcal{D}_k\}_{k \in \boldsymbol{N}}$ is a sequence of finite sets of possible decryption-keys. Here, $\mathcal{D}_k \subset \{0, 1\}^{l_D(k)}$, where $l_D(k)$ is a polynomial of k.
   - *GEN* is a key generation algorithm which outputs encryption-keys and decryption-keys.
   - $ENC : \mathcal{E} \times \mathcal{M} \times \mathcal{U}_R \longrightarrow \mathcal{C}$ is an encryption algorithm,
   - $DEC : \mathcal{D} \times \mathcal{C} \times \mathcal{U}_S \longrightarrow \mathcal{M} \cup \{\perp\}$ is a decryption algorithm.
2. **Key Generation and Distribution by TA:** The TA generates an *encryption-key* $e_i \in \mathcal{E}$ for each sender S_i, and a *decryption-key* $d_j \in \mathcal{D}$ for each receiver R_j using the key generation algorithm *GEN*. Here *GEN* is a probabilistic algorithm which produces,

on input 1^k, where k is a security parameter, keys $(e_1, e_2, \ldots, e_{n_1}, d_1, d_2, \ldots, d_{n_2})$ of matching encryption and decryption keys, where $e_i \in \mathcal{E}_k$ for $1 \le i \le n_1$ and $d_j \in \mathcal{D}_k$ for $1 \le j \le n_2$. Then, TA transmits the encryption-key e_i to the sender S_i and the decryption-key d_j to the receiver R_j via a secure channel. After delivering these keys, the TA may erase the keys from his memory. Each sender keeps secret his encryption-key, and each receiver keeps secret his decryption-key.

3. **Encryption:** For a plaintext $m \in \mathcal{M}_k$, the sender S_i generates a ciphertext $c = ENC(e_i, m, R_j) \in C_k$ which will be sent to the receiver R_j by using his encryption-key e_i in conjunction with the encryption algorithm ENC.
4. **Decryption:** On receiving a ciphertext c from a sender S_i, the receiver R_j recovers a plaintext using his decryption-key d_j and the decryption algorithm DEC. More precisely, if $DEC(d_j, c, S_i) = \perp$, R_j regards the received ciphertext c as invalid. Otherwise, R_j recovers the plaintext $m = DEC(d_j, c, S_i)$ as valid ciphertext from S_i. Here, we require that $DEC(d_j, ENC(e_i, m, R_j), S_i) = m$ for all $m \in \mathcal{M}_k$.

The model of authenticated encryption is syntactically identical to that of encryption as defined above. The difference between encryption and authenticated encryption lies in their security goals: the goal of encryption is to achieve only confidentiality while the goal of authenticated encryption is to achieve both confidentiality and authenticity. In this paper, we use the model in Definition 1 even for authenticated encryption as well. In addition, we use *encryption* (resp. *authenticated encryption*) to emphasize cases that we are targeting confidentiality goals (resp. both confidentiality and authenticity goals).

Let t_1 and t_2 be the number up to which each sender is allowed to encrypt plaintexts and the number up to which each receiver is allowed to decrypt ciphertexts, respectively, and let ω be the number of possible colluders among users. Let $\mathcal{W} := \{W \subset \mathcal{U} | \#W \le \omega\}$. Each element of $\mathcal{W}$ represents a group of possibly collusive users. For a set $\mathcal{T}$ and a non-negative integer t, let $\mathcal{P}(\mathcal{T}, t) := \{T \subset \mathcal{T} \mid \#T \le t\}$ be the family of all subsets of $\mathcal{T}$ whose cardinality are less than or equal to t.

Definition 2: (Exponentially Negligible Function) Let $\epsilon(k)$ be a function defined over the positive integers $k \in \boldsymbol{N}$ that takes non-negative real numbers. Then, $\epsilon(k)$ is called *exponentially negligible* if there exists an integer k_0 and some constant $a (1 < a)$ such that $\epsilon(k) \le \frac{1}{a^k}$ for all $k \ge k_0$.

We now consider security notions and formulate them along with our model in Definition 1 from information-theoretic viewpoints. In this paper, we consider the following security goals: for confidentiality, *APS (Almost Perfect Secrecy)* and *NM (Non-Malleability)*; and for authenticity, *IntC (Integrity of Ciphertexts)* and *IntP (Integrity of Plaintexts)*. The first notion of APS is a straightforward relaxed notion of *perfect secrecy* by Shannon [17]. The second one, NM, will be formally defined in the context of unconditional security based on the idea of the notion of computational security [3], [4], [8], [9]. The third and fourth ones, IntC and IntP, will be formally defined in the context of unconditional security setting based on the idea of that of computational security setting [4].

In addition, we consider the above four security goals under the most powerful attacking model, that is, *chosen plaintext attacks and chosen ciphertext attacks (CPA and CCA)* in unconditional security setting. Here, CPA and CCA means the attacks where the adversary can obtain the encryption of any plaintext of his choice and the decryption of any ciphertext of his choice except the target ciphertext. Namely, the adversary is given oracle access to an encryption function and a decryption function, but is not allowed to ask for the decryption of the target ciphertext itself.

First, we introduce the notion of almost perfect secrecy against chosen plaintext attacks and chosen ciphertext attacks (APS against CPA and CCA). Intuitively, the notion of APS means that the partial information on the plaintext from a target ciphertext which the adversary can derive is upper-bounded by a small quantity ϵ. We note that this notion can capture the notion of perfect secrecy (PS) by considering the case that $\epsilon = 0$. We formalize APS from an information-theoretic viewpoint as follows.

Definition 3 ((A)PS against CPA and CCA (cf. [17])): Let Π be an encryption or authenticated encryption scheme. Let k be a security parameter. For $W \in \mathcal{W}$ such that $S_i, R_j \notin W$, we define

$$P_{\Pi}^{PS}(S_i, R_j, W) := \max_{e_W} \max_{M_{S_i}} \max_{C_{R_j}}$$

$$\max_{M_{S_1},\ldots,M_{S_l},\ldots,M_{S_{n_1}} (l \ne i)} \max_{C_{R_1},\ldots,C_{R_s},\ldots,C_{R_{n_2}} (s \ne j)}$$

$$\max_{c} \left\{ \sum_{m \in \mathcal{M}_k} \Big| \Pr(m | c, e_W, \right.$$

$$\left. \{M_{S_l} | 1 \le l \le n_1\}, \{C_{R_s} | 1 \le s \le n_2\}) - \Pr(m) \Big| \right\},$$

where e_W is taken over all possible combination of keys of W; M_{S_i} is taken over $\mathcal{P}(\mathcal{M}_k \times C_k, t_1 - 1)$ such that any element (m_{S_i}, c_{S_i}) of M_{S_i} is a pair of a plaintext m_{S_i} and a corresponding ciphertext c_{S_i} encrypted by S_i; $M_{S_l} (l \ne i)$ is taken over $\mathcal{P}(\mathcal{M}_k \times C_k, t_1)$ such that any element (m_{S_l}, c_{S_l}) of M_{S_l} is a pair of a plaintext m_{S_l} and a corresponding ciphertext c_{S_l} encrypted by S_l; C_{R_j} is taken over $\mathcal{P}(C_k \times (\mathcal{M}_k \cup \{\perp\}), t_2)$ such that any element of C_{R_j} is a pair of a ciphertext c_{R_j} and a decryption result of c_{R_j} by R_j; $C_{R_s} (s \ne j)$ is taken over $\mathcal{P}(C_k \times (\mathcal{M}_k \cup \{\perp\}), t_2)$ such that any element of C_{R_s} is a pair of a ciphertext c_{R_s} and a decryption result of c_{R_s} by R_s; and c is taken over valid ciphertexts from S_i to R_j such that c does not appear in C_{R_j}.

We define

$$P_{\Pi}^{PS} := \max_{S_i, R_j, W} P_{\Pi}^{PS}(S_i, R_j, W).$$

Then, the scheme Π is said to be (ω, t_1, t_2)-APS (*Almost Per-*

fectly Secure) if $P_{\Pi}^{PS} \leq \epsilon$ for some exponentially negligible function ϵ. In particular, if $P_{\Pi}^{PS} = 0$, the scheme Π is said to be (ω, t_1, t_2)-PS (*Perfectly Secure*).

Remark 1: The above notion of APS is defined only in terms of probability distribution since we are discussing information-theoretic security. On the other hand, we note that in the public-key setting the notion of semantic security [10] is known as a computational analogue of Shannon's definition of perfect secrecy [17]. And, in order to define semantic security or equivalently indistinguishability [10], the computational complexity-theoretic approach by using computational models whose computational complexity is polynomially bounded is taken rather than the information-theoretic one by the use of probability distribution.

Remark 2: In Definition 3, we have considered the attacking model of CPA and CCA. In the public-key setting, for each of CPA and CCA *adaptive* and *non-adaptive* cases are currently known. However, there is no difference between them in Definition 3. This is because all possible information which the adversary with unlimited computational power can obtain by having access to both encryption and decryption oracles is taken into account. The same can also be applied to other security definitions in this paper. Thus, in the sequel we do not consider adaptive and non-adaptive cases separately in formalizing CPA and CCA, since there is no difference between them in formalization.

We next formally define the notion of non-malleability in unconditional security setting based on the idea of that of non-malleability in computational setting [3], [8], [9]. Intuitively, the notion of non-malleability means that from a ciphertext c it is difficult for the adversary to create a ciphertext $c'(\neq c)$ such that underlying plaintexts of them are meaningfully related. While the notion of non-malleability in [3], [8], [9] is considered from a computational complexity-theoretic point of view, we formulate this notion by the use of probability distribution in the following since we are discussing information-theoretic security.

Definition 4 (NM against CPA and CCA): Let Π be an encryption or authenticated encryption scheme. Let k be a security parameter and $\epsilon(k)$ an exponentially negligible function. For simplicity, we denote the exponentially negligible function $\epsilon(k)$ by ϵ. For a relation $\mathfrak{R}$ on $\mathcal{M}_k$, we write $\mathfrak{R}(x_1, x_2) = 1$ if the relation $\mathfrak{R}$ holds for $x_1, x_2 \in \mathcal{M}_k$, and we write $\mathfrak{R}(x_1, x_2) = 0$ otherwise. For any relation $\mathfrak{R}$ on $\mathcal{M}_k$, we extend $\mathfrak{R}$ to the relation $\hat{\mathfrak{R}}$ on $\mathcal{M}_k \cup \{\perp\}$ as follows:

$$\hat{\mathfrak{R}}(x_1, x_2) := \begin{cases} \mathfrak{R}(x_1, x_2) & \text{if } x_1, x_2 \in \mathcal{M}_k \\ 0 & \text{if } x_1 = \perp \text{ or } x_2 = \perp \end{cases}$$

For $W \in \mathcal{W}$ such that $S_i, R_j \notin W$ and a relation $\mathfrak{R}$ on $\mathcal{M}_k$, we define

$$P_{\Pi}^{NM}(\mathfrak{R}; S_i, R_j, W) := \max_{e_W} \max_{M_{S_i}} \max_{C_{R_j}} \max_{M_{S_1},\ldots,M_{S_l},\ldots,M_{S_{n_1}} (l \neq i)} \max_{C_{R_1},\ldots,C_{R_s},\ldots,C_{R_{n_2}} (s \neq j)} \max_{c} \max_{c'} \sum_{d \in \mathcal{D}_k} \Pr(d) \cdot \Big| \chi_{NM}(\hat{\mathfrak{R}}; S_i, R_j; DEC(d, c, S_i), DEC(d, c', S_i) \; | c, e_W, \{M_{S_l} | 1 \leq l \leq n_1\}, \{C_{R_s} | 1 \leq s \leq n_2\}) - \sum_{m \in \mathcal{M}_k} \Pr(m) \chi_{NM}(\hat{\mathfrak{R}}; S_i, R_j; m, DEC(d, c', S_i)) \Big|,$$

where e_W is taken over all possible combination of keys of W; M_{S_i} is taken over $\mathcal{P}(\mathcal{M}_k \times \mathcal{C}_k, t_1 - 1)$ such that any element (m_{S_i}, c_{S_i}) of M_{S_i} is a pair of a plaintext m_{S_i} and a corresponding ciphertext c_{S_i} encrypted by S_i; $M_{S_l} (l \neq i)$ is taken over $\mathcal{P}(\mathcal{M}_k \times \mathcal{C}_k, t_1)$ such that any element (m_{S_l}, c_{S_l}) of M_{S_l} is a pair of a plaintext m_{S_l} and a corresponding ciphertext c_{S_l} encrypted by S_l; C_{R_j} is taken over $\mathcal{P}(\mathcal{C}_k \times (\mathcal{M}_k \cup \{\perp\}), t_2 - 1)$ such that any element of C_{R_j} is a pair of a ciphertext c_{R_j} and a decryption result of c_{R_j} by R_j; $C_{R_s} (s \neq j)$ is taken over $\mathcal{P}(\mathcal{C}_k \times (\mathcal{M}_k \cup \{\perp\}), t_2)$ such that any element of C_{R_s} is a pair of a ciphertext c_{R_s} and a decryption result of c_{R_s} by R_s; c is taken over valid ciphertexts from S_i to R_j; c' is taken over ciphertexts from S_i to R_j such that $c' \neq c$; and the function $\chi_{NM}(\hat{\mathfrak{R}}; S_i, R_j; m, DEC(d, c', S_i))$ is defined as follows. For $m \in \mathcal{M}_k, c' \in \mathcal{C}_k$ and R_j's decryption key $d \in \mathcal{D}_k$,

$$\chi_{NM}(\hat{\mathfrak{R}}; S_i, R_j; m, DEC(d, c', S_i)) := \begin{cases} 1 & \text{if } \hat{\mathfrak{R}}(m, DEC(d, c', S_i)) = 1 \\ & \quad \text{for } R_j\text{'s decryption key } d \\ 0 & \text{otherwise} \end{cases}$$

Similarly, the function $\chi_{NM}(\hat{\mathfrak{R}}; S_i, R_j; DEC(d, c, S_i), DEC(d, c', S_i)) \mid c, e_W, \{M_{S_l} | 1 \leq l \leq n_1\}, \{C_{R_s} | 1 \leq s \leq n_2\})$ is defined as follows. For the given $(c, e_W, \{M_{S_l} | 1 \leq l \leq n_1\}, \{C_{R_s} | 1 \leq s \leq n_2\})$, and $d \in \mathcal{D}_k, c' \in \mathcal{C}_k$ with $c' \neq c$,

$$\chi_{NM}(\hat{\mathfrak{R}}; S_i, R_j; DEC(d, c, S_i), DEC(d, c', S_i) \; | c, e_W, \{M_{S_l} | 1 \leq l \leq n_1\}, \{C_{R_s} | 1 \leq s \leq n_2\}) := \begin{cases} 1 & \text{if the given} \\ & (c, e_W, \{M_{S_l} | 1 \leq l \leq n_1\}, \{C_{R_s} | 1 \leq s \leq n_2\}) \\ & \quad \text{can occur with positive probability and} \\ & \quad \hat{\mathfrak{R}}(DEC(d, c, S_i), DEC(d, c', S_i)) = 1 \\ & \quad \text{for } R_j\text{'s decryption key } d \\ 0 & \text{otherwise} \end{cases}$$

We define

$$P_{\Pi}^{NM}(\mathfrak{R}) := \max_{S_i, R_j, W} P_{\Pi}^{NM}(\mathfrak{R}; S_i, R_j, W).$$

Then, the scheme Π is said to be (ω, t_1, t_2)-NM (*Non-Malleable*) if $P_{\Pi}^{NM}(\mathfrak{R}) \leq \epsilon$ for any relation $\mathfrak{R}$.

For confidentiality, we have already introduced the notions of almost perfect secrecy and non-malleability in the unconditional setting. In addition to the notions of confidentiality, we formally define two notions of the integrity, IntC (Integrity of Ciphertexts) and IntP (Integrity of Plaintexts), for authenticated encryption in the unconditional setting. The notion of IntC prevents the adversary from illegitimately producing a ciphertext which the sender has not previously created, while the notion of IntP prevents the adversary from illegitimately producing a ciphertext decrypting to a plaintext which the sender had never encrypted.

We first consider IntC. Intuitively, the notion of IntC means that it is difficult for the adversary to create a ciphertext c that has not been previously created by the sender but will be accepted as valid and authentic by the receiver. This notion is formalized in [4] in the context of symmetric encryption in terms of computational security. We note that the notion of IntC along with the model of symmetric encryption is also formalized in [5] and [14].

In the following, we formulate the notion of IntC along with our model only by the use of probability distribution since we are discussing information-theoretic security along with our model.

Definition 5 (IntC against CPA and CCA): Let Π be an authenticated encryption scheme. Let k be a security parameter and ϵ an exponentially negligible function. For $W \in \mathcal{W}$ such that $S_i, R_j \notin W$, we define

$$P_{\Pi}^{IntC}(S_i, R_j, W) := \max_{e_W} \max_{M_{S_i}} \max_{C_{R_j}} \max_{M_{S_1},\ldots,M_{S_l},\ldots,M_{S_{n_1}} (l \neq i)} \max_{C_{R_1},\ldots,C_{R_s},\ldots,C_{R_{n_2}} (s \neq j)} \max_{c} \Pr(R_j \text{ decrypts } c \text{ from } S_i \text{ as not } \perp | \; e_W, \{M_{S_l} | 1 \leq l \leq n_1\}, \{C_{R_s} | 1 \leq s \leq n_2\}),$$

where e_W is taken over all possible combination of keys of W; M_{S_i} is taken over $\mathcal{P}(\mathcal{M}_k \times C_k, t_1)$ such that any element (m_{S_i}, c_{S_i}) of M_{S_i} is a pair of a plaintext m_{S_i} and a corresponding ciphertext c_{S_i} encrypted by S_i; $M_{S_l} (l \neq i)$ is taken over $\mathcal{P}(\mathcal{M}_k \times C_k, t_1)$ such that any element (m_{S_l}, c_{S_l}) of M_{S_l} is a pair of a plaintext m_{S_l} and a corresponding ciphertext c_{S_l} encrypted by S_l; C_{R_j} is taken over $\mathcal{P}(C_k \times (\mathcal{M}_k \cup \{\perp\}), t_2 - 1)$ such that any element of C_{R_j} is a pair of a ciphertext c_{R_j} and a decryption result of c_{R_j} by R_j; $C_{R_s} (s \neq j)$ is taken over $\mathcal{P}(C_k \times (\mathcal{M}_k \cup \{\perp\}), t_2)$ such that any element of C_{R_s} is a pair of a ciphertext c_{R_s} and a decryption result of c_{R_s} by R_s; c is taken over ciphertexts such that c does not appear in M_{S_i} and also not in C_{R_j} except $(c, \perp)$; and for given $(e_W, \{M_{S_l} | 1 \leq l \leq n_1\}, \{C_{R_s} | 1 \leq s \leq n_2\})$, the probability $\Pr(R_j$ decrypts c from S_i as not $\perp \; | \; e_W, \{M_{S_l} | 1 \leq l \leq n_1\}, \{C_{R_s} | 1 \leq s \leq n_2\})$ is strictly defined as follows. For the given $(e_W, \{M_{S_l} | 1 \leq l \leq n_1\}, \{C_{R_s} | 1 \leq s \leq n_2\})$,

$$\begin{aligned} &\Pr(R_j \text{ decrypts } c \text{ from } S_i \text{ as not } \perp \\ &\qquad | \; e_W, \{M_{S_l} | 1 \leq l \leq n_1\}, \{C_{R_s} | 1 \leq s \leq n_2\}) \\ &:= \sum_{d \in \mathcal{D}_k} \Pr(d) \cdot \chi_{IntC}(S_i, R_j; c, d \,|\, e_W, \\ &\qquad \{M_{S_l} | 1 \leq l \leq n_1\}, \{C_{R_s} | 1 \leq s \leq n_2\}), \\ &\chi_{IntC}(S_i, R_j; c, d \,|\, e_W, \{M_{S_l} | 1 \leq l \leq n_1\}, \\ &\qquad \{C_{R_s} | 1 \leq s \leq n_2\}) \\ &:= \begin{cases} 1 & \text{if the given} \\ & (e_W, \{M_{S_l} | 1 \leq l \leq n_1\}, \{C_{R_s} | 1 \leq s \leq n_2\}) \\ & \text{can occur with positive probability and} \\ & DEC(d, c, S_i) \neq \perp \\ & \text{for } R_j\text{'s decryption key } d \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

We define $P_{\Pi}^{IntC} := \max_{S_i, R_j, W} P_{\Pi}^{IntC}(S_i, R_j, W)$. Then, the scheme Π is said to be (ω, t_1, t_2)-IntC if $P_{\Pi}^{IntC} \leq \epsilon$.

We next consider IntP. Intuitively, the notion of IntP means that it is difficult for the adversary to create a ciphertext c that will be accepted as valid and authentic by the receiver and be decrypting to a plaintext which the sender had never encrypted. As well as IntC, the notion of IntP is formalized in [4] in the context of symmetric key encryption in terms of computational security. In the following, as well as IntC, we formulate this notion along with our model only by the use of probability distribution.

Definition 6 (IntP against CPA and CCA): Let Π be an authenticated encryption scheme. Let k be a security parameter and ϵ an exponentially negligible function. For $W \in \mathcal{W}$ such that $S_i, R_j \notin W$, we define

$$P_{\Pi}^{IntP}(S_i, R_j, W) := \max_{e_W} \max_{M_{S_i}} \max_{C_{R_j}} \max_{M_{S_1},\ldots,M_{S_l},\ldots,M_{S_{n_1}} (l \neq i)} \max_{C_{R_1},\ldots,C_{R_s},\ldots,C_{R_{n_2}} (s \neq j)} \max_{c} \Pr(R_j \text{ decrypts } c \text{ from } S_i \text{ as not } \perp \text{ and not in } M_{S_i} | e_W, \{M_{S_l} | 1 \leq l \leq n_1\}, \{C_{R_s} | 1 \leq s \leq n_2\}),$$

where e_W is taken over all possible combination of keys of W; M_{S_i} is taken over $\mathcal{P}(\mathcal{M}_k \times C_k, t_1)$ such that any element (m_{S_i}, c_{S_i}) of M_{S_i} is a pair of a plaintext m_{S_i} and a corresponding ciphertext c_{S_i} encrypted by S_i; $M_{S_l} (l \neq i)$ is taken over $\mathcal{P}(\mathcal{M}_k \times C_k, t_1)$ such that any element (m_{S_l}, c_{S_l}) of M_{S_l} is a pair of a plaintext m_{S_l} and a corresponding ciphertext c_{S_l} encrypted by S_l; C_{R_j} is taken over $\mathcal{P}(C_k \times (\mathcal{M}_k \cup \{\perp\}), t_2 - 1)$ such that any element of C_{R_j} is a pair of a ciphertext c_{R_j} and a decryption result of c_{R_j} by R_j; $C_{R_s} (s \neq j)$ is taken over $\mathcal{P}(C_k \times (\mathcal{M}_k \cup \{\perp\}), t_2)$ such that any element of C_{R_s} is a pair of a ciphertext c_{R_s} and a decryption result of c_{R_s} by R_s; c is taken over ciphertexts such that $DEC(d, c, S_i) \neq \perp$ for R_j's decryption key d and $DEC(d, c, S_i)$ does not appear in M_{S_i}; and for given $(e_W, \{M_{S_l} | 1 \leq l \leq n_1\}, \{C_{R_s} | 1 \leq s \leq n_2\})$, the probability $\Pr(R_j$ decrypts c from S_i as not $\perp$ and not in $M_{S_i} \; | \; e_W, \{M_{S_l} | 1 \leq l \leq n_1\}, \{C_{R_s} | 1 \leq s \leq n_2\})$ is strictly defined as follows. For the given $(e_W, \{M_{S_l} | 1 \leq l \leq n_1\}, \{C_{R_s} | 1 \leq s \leq n_2\})$,

$$\begin{aligned} &\Pr(R_j \text{ decrypts } c \text{ from } S_i \text{ as not } \perp \text{ and not in } M_{S_i} \\ &\qquad | \; e_W, \{M_{S_l} | 1 \leq l \leq n_1\}, \{C_{R_s} | 1 \leq s \leq n_2\}) \\ &:= \sum_{d \in \mathcal{D}_k} \Pr(d) \cdot \chi_{IntP}(S_i, R_j; c, d \,|\, e_W, \\ &\qquad \{M_{S_l} | 1 \leq l \leq n_1\}, \{C_{R_s} | 1 \leq s \leq n_2\}), \\ &\chi_{IntP}(S_i, R_j; c, d \,|\, e_W, \{M_{S_l} | 1 \leq l \leq n_1\}, \end{aligned}$$

$$\{C_{R_s}|1 \leq s \leq n_2\})$$

$$:= \begin{cases} 1 & \text{if the given} \\ & (e_W, \{M_{S_l}|1 \leq l \leq n_1\}, \{C_{R_s}|1 \leq s \leq n_2\}) \\ & \text{can occur with positive probability,} \\ & DEC(d, c, S_i) \neq \perp \text{ and} \\ & DEC(d, c, S_i) \text{ does not appear in } M_{S_i} \\ & \text{for } R_j\text{'s decryption key } d \\ 0 & \text{otherwise} \end{cases}$$

We define $P_{\Pi}^{IntP} := \max_{S_i,R_j,W} P_{\Pi}^{IntP}(S_i, R_j, W)$. Then, the scheme Π is said to be (ω, t_1, t_2)-IntP if $P_{\Pi}^{IntP} \leq \epsilon$.

2.2 A Model of Signature Schemes with Unconditional Security

In this subsection, we consider a model of unconditionally secure signature schemes and describe the security definition considered in [18].

Definition 7 (Signature [12] [18]): A *signature scheme* Λ consists of ($\mathcal{U}$, TA, $\mathcal{M}$, $\mathcal{SK}$, $\mathcal{VK}$, $\mathcal{A}$, *GEN*, *SIG*, *VER*):

- $\mathcal{U} = \{S_1, \ldots, S_{n_1}, V_1, \ldots, V_{n_2}\}$ is a finite set of users, where S_i are signers and V_j are verifiers. Let $\mathcal{U}_S := \{S_1, S_2, \ldots, S_{n_1}\}$ and $\mathcal{U}_V := \{V_1, V_2, \ldots, V_{n_2}\}$. We also use S_i (resp. V_j) as S_i's (resp. V_j's) identity.
- TA is a trusted authority.
- $\mathcal{M} = \{\mathcal{M}_k\}_{k\in\boldsymbol{N}}$ is a sequence of finite sets of possible messages, where $\mathcal{M}_k \subset \{0, 1\}^{l_M(k)}$, and $l_M(k)$ is a polynomial of k. Hereafter, k means a security parameter.
- $\mathcal{SK} = \{\mathcal{SK}_k\}_{k\in\boldsymbol{N}}$ is a sequence of finite sets of possible signing-keys. Here, $\mathcal{SK}_k \subset \{0, 1\}^{l_{SK}(k)}$, and $l_{SK}(k)$ is a polynomial of k.
- $\mathcal{VK} = \{\mathcal{VK}_k\}_{k\in\boldsymbol{N}}$ is a sequence of finite sets of possible verification-keys. Here, $\mathcal{VK}_k \subset \{0, 1\}^{l_{VK}(k)}$, and $l_{VK}(k)$ is a polynomial of k.
- $\mathcal{A} = \{\mathcal{A}_k\}_{k\in\boldsymbol{N}}$ is a sequence of finite sets of possible signatures. Here, $\mathcal{A}_k \subset \{0, 1\}^{l_A(k)}$, and $l_A(k)$ is a polynomial of k.
- *GEN* is a *key generation algorithm* which on input a security parameter 1^k, outputs signing-keys and verification-keys.
- $SIG : \mathcal{SK} \times \mathcal{M} \longrightarrow \mathcal{A}$ is a *signing algorithm*,
- $VER : \mathcal{VK} \times \mathcal{M} \times \mathcal{A} \times \mathcal{U}_S \longrightarrow \{true, false\}$ is a *verification algorithm.*

As in the previous subsection, let t_1 and t_2 be the number up to which each signer is allowed to sign messages and the number up to which each verifier is allowed to verify signatures, respectively, and let ω be the number of possible colluders among users.

In [18], it is mentioned that the strong security of the signature schemes with unconditional security is existential acceptance unforgeability for any verifier against adaptive chosen message attacks and adaptive chosen signature attacks. In the sequel, we briefly call this notion *EAUF against ACMA and ACSA*. On the other hand, the notion of existential unforgeability (EUF), which is currently considered as the strong security notion in public-key signature schemes [11], can also be considered in the unconditional security setting. However, we note that as shown in [18] it is sufficient to consider EAUF against ACMA and ACSA as strong security, since EAUF against ACMA and ACSA always implies EUF against ACMA and ACSA.

Intuitively, the notion of EAUF means that it is difficult for the adversary to create a signature that has not been legally created by the signer but will be accepted as valid by a verifier. Here, note that in the unconditional security setting there may exist a signature which cannot be output by the signing algorithm with a legitimate signing key but will be accepted by the verification algorithm with a legitimate verification key (See [18]). In the following, we describe the formalization of the notion of *EAUF against CMA and CSA* along with our model by the use of probability distribution as in [18]. Here, note that the notion of CMA and CSA is sufficient to consider since there is no difference between adaptive and non-adaptive cases in the following formalization (See also Remark 2).

Definition 8 (EAUF against CMA and CSA [18]): Let Λ be a signature scheme. Let k be a security parameter and $\epsilon(k)$ an exponentially negligible function.

1) For $W \in \mathcal{W}$ such that $S_i, V_j \notin W$, we define

$$P_{\Lambda,1}^{EAUF}(S_i, V_j, W) := \max_{e_W} \max_{M_{S_i}} \max_{M_{V_j}}$$
$$\max_{M_{S_1},\ldots,M_{S_l},\ldots,M_{S_{n_1}} (l\neq i)} \max_{M_{V_1},\ldots,M_{V_s},\ldots,M_{V_{n_2}} (s\neq j)}$$
$$\max_{(m,a)} \Pr(V_j \text{ accepts } (m, a) \text{ as signed by } S_i$$
$$| \, e_W, \{M_{S_l}|1 \leq l \leq n_1\}, \{M_{V_s}|1 \leq s \leq n_2\})$$

where e_W is taken over all possible combination of keys of W; M_{S_i} is taken over $\mathcal{P}(\mathcal{M}_k \times \mathcal{A}_k, t_1)$ such that any element of M_{S_i} is a valid signed message generated by S_i; $M_{S_l}(l \neq i)$ is taken over $\mathcal{P}(\mathcal{M}_k \times \mathcal{A}_k, t_1)$ such that any element of M_{S_l} is a valid signed message generated by S_l; M_{V_j} is taken over $\mathcal{P}(\mathcal{M}_k \times \mathcal{A}_k \times \{true, false\}, t_2 - 1)$ such that any element of M_{V_j} is a pair of a signed message (m_{V_j}, a_{V_j}) and a verification result of (m_{V_j}, a_{V_j}) by V_j; $M_{V_s}(s \neq j)$ is taken over $\mathcal{P}(\mathcal{M}_k \times \mathcal{A}_k \times \{true, false\}, t_2)$ such that any element of M_{V_s} is a pair of a signed message (m_{V_s}, a_{V_s}) and a verification result of (m_{V_s}, a_{V_s}) by V_s; (m, a) is taken over $\mathcal{M}_k \times \mathcal{A}_k$ such that $(m, a) \notin M_{S_i}$ and does not appear in M_{V_j} except $((m, a), false)$; and for given $(e_W, \{M_{S_l}|1 \leq l \leq n_1\}, \{M_{V_s}|1 \leq s \leq n_2\})$, the probability $\Pr(V_j$ accepts (m, a) as signed by $S_i \mid e_W, \{M_{S_l}|1 \leq l \leq n_1\}, \{M_{V_s}|1 \leq s \leq n_2\})$ is strictly defined as follows. For the given $(e_W, \{M_{S_l}|1 \leq l \leq n_1\}, \{M_{V_s}|1 \leq s \leq n_2\})$ and V_j's verification-key $v \in \mathcal{VK}_k$,

$$\Pr(V_j \text{ accepts } (m, a) \text{ as signed by } S_i$$
$$| \, e_W, \{M_{S_l}|1 \leq l \leq n_1\}, \{M_{V_s}|1 \leq s \leq n_2\})$$
$$:= \sum_{v\in\mathcal{VK}_k} \Pr(v) \cdot \chi_{EAUF,1}(S_i, V_j; (m, a), v \mid e_W,$$

$$\{M_{S_l}|1 \le l \le n_1\}, \{M_{V_s}|1 \le s \le n_2\}),$$

$$\chi_{EAUF,1}(S_i, V_j; (m,a), v \mid e_W, \{M_{S_l}|1 \le l \le n_1\}, \{M_{V_s}|1 \le s \le n_2\})$$

$$:= \begin{cases} 1 \text{ if the given } \\ (e_W, \{M_{S_l}|1 \le l \le n_1\}, \{M_{V_s}|1 \le s \le n_2\}) \\ \text{can occur with positive probability and} \\ VER(v, (m,a), S_i) = true \\ 0 \text{ otherwise} \end{cases}$$

We define $P^{EAUF}_{\Lambda,1} := \max_{S_i,V_j,W} P^{EAUF}_{\Lambda,1}(S_i, V_j, W)$.

2) For $W \in \mathcal{W}$ such that $V_j \notin W$ and $S_i \in W$, we define $P^{EAUF}_{\Lambda,2}(S_i, V_j, W)$ as

$$P^{EAUF}_{\Lambda,2}(S_i, V_j, W) := \max_{e_W} \max_{M_{V_j}} \max_{M_{S_1},\ldots,M_{S_l},\ldots,M_{S_{n_1}} (l \neq i)} \max_{M_{V_1},\ldots,M_{V_s},\ldots,M_{V_{n_2}} (s \neq j)} \max_{(m,a)} \Pr(V_j \text{ accepts } (m,a) \text{ as signed by } S_i \; |e_W, \{M_{S_l}|1 \le l \le n_1, l \neq i\}, \{M_{V_s}|1 \le s \le n_2\})$$

where e_W is taken over all possible combination of keys of W; $M_{S_l}(l \neq i)$ is taken over $\mathcal{P}(\mathcal{M}_k \times \mathcal{A}_k, t_1)$ such that any element of M_{S_l} is a valid signed message generated by S_l; M_{V_j} is taken over $\mathcal{P}(\mathcal{M}_k \times \mathcal{A}_k \times \{true, false\}, t_2 - 1)$ such that any element of M_{V_j} is a pair of a signed message (m_{V_j}, a_{V_j}) and a verification result of (m_{V_j}, a_{V_j}) by V_j; $M_{V_s}(s \neq j)$ is taken over $\mathcal{P}(\mathcal{M}_k \times \mathcal{A}_k \times \{true, false\}, t_2)$ such that any element of M_{V_s} is a pair of a signed message (m_{V_s}, a_{V_s}) and a verification result of (m_{V_s}, a_{V_s}) by V_s; (m,a) is taken over invalid signed messages such that (m,a) does not appear in M_{V_j} except $((m,a), false)$; and for given $(e_W, \{M_{S_l}|1 \le l \le n_1, l \neq i\}, \{M_{V_s}|1 \le s \le n_2\})$, the probability $\Pr(V_j$ accepts (m,a) as signed by $S_i \mid e_W, \{M_{S_l}|1 \le l \le n_1, l \neq i\}, \{M_{V_s}|1 \le s \le n_2\})$ is strictly defined as follows. For the given $(e_W, \{M_{S_l}|1 \le l \le n_1, l \neq i\}, \{M_{V_s}|1 \le s \le n_2\})$ and V_j's verification-key $v \in \mathcal{VK}_k$,

$$\Pr(V_j \text{ accepts } (m,a) \text{ as signed by } S_i \mid e_W, \{M_{S_l}|1 \le l \le n_1, l \neq i\}, \{M_{V_s}|1 \le s \le n_2\})$$

$$:= \sum_{v \in \mathcal{VK}_k} \Pr(v) \cdot \chi_{EAUF,2}(S_i, V_j; (m,a), v \mid e_W, \{M_{S_l}|1 \le l \le n_1, l \neq i\}, \{M_{V_s}|1 \le s \le n_2\}),$$

$$\chi_{EAUF,2}(S_i, V_j; (m,a), v \mid e_W, \{M_{S_l}|1 \le l \le n_1, l \neq i\}, \{M_{V_s}|1 \le s \le n_2\})$$

$$:= \begin{cases} 1 \text{ if the given } (e_W, \\ \{M_{S_l}|1 \le l \le n_1, l \neq i\}, \{M_{V_s}|1 \le s \le n_2\}) \\ \text{can occur with positive probability and} \\ VER(v, (m,a), S_i) = true \\ 0 \text{ otherwise} \end{cases}$$

We define $P^{EAUF}_{\Lambda,2} := \max_{S_i,V_j,W} P^{EAUF}_{\Lambda,2}(S_i, V_j, W)$.

Then, the signature scheme Λ is said to be (ω, t_1, t_2)-*EAUF* if $\max\{P^{EAUF}_{\Lambda,1}, P^{EAUF}_{\Lambda,2}\} \le \epsilon$.

3. Relations among Security Notions for Authenticated Encryption

In the previous section, we define the notions of (ω, t_1, t_2)-APS and (ω, t_1, t_2)-NM for confidentiality, and those of (ω, t_1, t_2)-IntC and (ω, t_1, t_2)-IntP for authenticity. Thus, by combining these notions of confidentiality and authenticity, we reach the following four notions for authenticated encryption schemes:

(i) (ω, t_1, t_2)-APS and (ω, t_1, t_2)-IntC, which is briefly denoted by (ω, t_1, t_2)-APS $\wedge$ IntC;
(ii) (ω, t_1, t_2)-APS and (ω, t_1, t_2)-IntP, which is briefly denoted by (ω, t_1, t_2)-APS $\wedge$ IntP;
(iii) (ω, t_1, t_2)-NM and (ω, t_1, t_2)-IntC, which is briefly denoted by (ω, t_1, t_2)-NM $\wedge$ IntC; and
(iv) (ω, t_1, t_2)-NM and (ω, t_1, t_2)-IntP, which is briefly denoted by (ω, t_1, t_2)-NM $\wedge$ IntP.

In this section, we analyze relations among the security notions and reveal the strongest notion among them.

First, we start with the following proposition. The proof of Proposition 1 easily follows from the definitions.

Proposition 1: Let Π be an authenticated encryption scheme. Let X$\in$ {APS, NM, IntC, IntP}. If Π is (ω, t_1, t_2)-X, then Π is (ω', t'_1, t'_2)-X for $\omega \ge \omega'$, $t_1 \ge t'_1$ and $t_2 \ge t'_2$.

Next, for authenticity, we show that the notion of IntC always implies that of IntP.

Theorem 1: Let Π be an authenticated encryption scheme. If Π is (ω, t_1, t_2)-IntC, then Π is (ω, t_1, t_2)-IntP.

Proof. We use same notations used in Definitions 5 and 6. For any e_W, $\{M_{S_l}|1 \le l \le n_1\}$, $\{C_{R_s}|1 \le s \le n_2\}$ and c, we have

$$\Pr(R_j \text{ decrypts } c \text{ from } S_i \text{ as not } \perp \text{ and not in } M_{S_i}|e_W, \{M_{S_l}|1 \le l \le n_1\}, \{C_{R_s}|1 \le s \le n_2\})$$
$$\le \Pr(R_j \text{ decrypts } c \text{ from } S_i \text{ as not } \perp \; |e_W, \{M_{S_l}|1 \le l \le n_1\}, \{C_{R_s}|1 \le s \le n_2\}).$$

Thus, $P^{IntP}_{\Pi}(S_i, R_j, W) \le P^{IntC}_{\Pi}(S_i, R_j, W)$ for any S_i, R_j and W. Therefore, we obtain $P^{IntP}_{\Pi} \le P^{IntC}_{\Pi}$. This implies that if $P^{IntC}_{\Pi} \le \epsilon$, it follows that $P^{IntP}_{\Pi} \le \epsilon$. □

From Theorem 1 it is sufficient to consider (i) or (iii), when we are interested in the strongest security notion among the four notions (i)–(iv). The following theorems (Theorems 2 and 3) show that the strongest notion among them is exactly (i).

Theorem 2: Let Π be an authenticated encryption scheme. If Π is (ω, t_1, t_2)-APS $\wedge$ IntC, then Π is (ω, t_1, t_2)-NM $\wedge$ IntC.

Proof. Since Π is already (ω, t_1, t_2)-IntC, it is sufficient to show that it is (ω, t_1, t_2)-NM.

Suppose that $P^{IntC}_{\Pi} \le \epsilon$. Let d be a decryption key of the receiver R_j. Also, let $(e_W, \{M_{S_l}|1 \le l \le n_1\}, \{C_{R_s}|1 \le s \le n_2\}, c, c')$ be arbitrarily given and suppose that it can occur with positive probability. Then, if $\hat{\mathfrak{R}}(DEC(d,c,S_i),DEC(d,c',S_i)) = 1$, we have $DEC(d,c',S_i) \neq \perp$. Therefore,

$$\begin{aligned}
&\chi_{NM}(\hat{\mathfrak{R}};S_i,R_j;DEC(d,c,S_i),DEC(d,c',S_i) \mid \\
&\quad c,e_W,\{M_{S_l}|1\le l\le n_1\},\{C_{R_s}|1\le s\le n_2\}) \\
&\quad \le \chi_{IntC}(S_i,R_j;d,c' \mid c,e_W, \\
&\quad \{M_{S_l}|1\le l\le n_1\},\{C_{R_s}|1\le s\le n_2\})
\end{aligned} \tag{1}$$

On the other hand, we note that for $m \in \mathcal{M}_k$, $\hat{\mathfrak{R}}(m,DEC(d,c',S_i)) = 1$ implies $DEC(d,c',S_i) \neq \perp$. Therefore,

$$\begin{aligned}
&\chi_{NM}(\hat{\mathfrak{R}};S_i,R_j;m,DEC(d,c',S_i)) \\
&\quad \le \chi_{IntC}(S_i,R_j;d,c')
\end{aligned}$$

Thus, we obtain

$$\begin{aligned}
&\sum_{m\in\mathcal{M}_k} \Pr(m)\chi_{NM}(\hat{\mathfrak{R}};S_i,R_j;m,DEC(d,c',S_i)) \\
&\quad \le \sum_{m\in\mathcal{M}_k} \Pr(m)\chi_{IntC}(S_i,R_j;d,c') \\
&\quad = \chi_{IntC}(S_i,R_j;d,c').
\end{aligned} \tag{2}$$

By (1) and (2), it is shown that

$$\begin{aligned}
&\Big|\chi_{NM}(\hat{\mathfrak{R}};S_i,R_j;DEC(d,c,S_i),DEC(d,c',S_i) \\
&\quad \mid c,e_W,\{M_{S_l}|1\le l\le n_1\},\{C_{R_s}|1\le s\le n_2\}) \\
&\quad - \sum_{m\in\mathcal{M}_k} \Pr(m)\chi_{NM}(\hat{\mathfrak{R}};S_i,R_j;m,DEC(d,c',S_i))\Big| \\
&\le \max(\chi_{IntC}(S_i,R_j;d,c'),\chi_{IntC}(S_i,R_j;d,c' \mid \\
&\quad c,e_W,\{M_{S_l}|1\le l\le n_1\},\{C_{R_s}|1\le s\le n_2\})) \\
&\le \chi_{IntC}(S_i,R_j;d,c') + \chi_{IntC}(S_i,R_j;d,c' \mid c,e_W, \\
&\quad \{M_{S_l}|1\le l\le n_1\},\{C_{R_s}|1\le s\le n_2\}).
\end{aligned} \tag{3}$$

From (3) it follows that

$$\begin{aligned}
&\sum_{d\in\mathcal{D}_k} \Pr(d)\cdot\Big|\chi_{NM}(\hat{\mathfrak{R}};S_i,R_j;DEC(d,c,S_i), \\
&\quad DEC(d,c',S_i)|c,e_W,\{M_{S_l}|1\le l\le n_1\}, \\
&\quad \{C_{R_s}|1\le s\le n_2\}) \\
&- \sum_{m\in\mathcal{M}_k} \Pr(m)\chi_{NM}(\hat{\mathfrak{R}};S_i,R_j;m,DEC(d,c',S_i))\Big| \\
&\le \sum_{d\in\mathcal{D}_k} \Pr(d)\cdot\{\chi_{IntC}(S_i,R_j;d,c') + \chi_{IntC}(S_i,R_j;d, \\
&\quad c'|c,e_W,\{M_{S_l}|1\le l\le n_1\},\{C_{R_s}|1\le s\le n_2\})\} \\
&\le 2P_{\Pi}^{IntC},
\end{aligned}$$

where the last inequality follows from the definition of P_{Π}^{IntC}. By taking maximum for e_W, $\{M_{S_l}|1\le l\le n_1\}$, $\{C_{R_s}|1\le s\le n_2\}$, c and c', it follows that

$$P_{\Pi}^{NM}(\mathfrak{R};S_i,R_j,W) \le 2P_{\Pi}^{IntC}.$$

Therefore, $P_{\Pi}^{NM}(\mathfrak{R}) \le 2P_{\Pi}^{IntC}$ for any relation $\mathfrak{R}$. This implies that $P_{\Pi}^{NM}(\mathfrak{R}) \le 2\epsilon$ for any relation $\mathfrak{R}$, since $P_{\Pi}^{IntC} \le \epsilon$. □

Theorem 3: There exists a scheme which is (ω,t_1,t_2)-NM $\wedge$ IntC but is not (ω,t_1,t_2)-APS $\wedge$ IntC.

Proof. Let Λ be a signature scheme which meets (ω,t_1,t_2)-EAUF. Then, by the definitions of P_{Λ}^{IntC} and P_{Λ}^{EAUF}, it easily follows that $P_{\Lambda}^{IntC} \le P_{\Lambda}^{EAUF}$. Thus, $P_{\Lambda}^{IntC} \le \epsilon$ if $P_{\Lambda}^{EAUF} \le \epsilon$, which means that Λ is (ω,t_1,t_2)-IntC. Moreover, from the proof of Theorem 2, it follows that the scheme Λ meets (ω,t_1,t_2)-NM. Thus, it is (ω,t_1,t_2)-NM $\wedge$ IntC. On the other hand, the scheme Λ does not obviously meet (ω,t_1,t_2)-APS. □

It should be noted that the strongest security notion for authenticated encryption is clearly the combined notion (ω,t_1,t_2)-APS $\wedge$ NM $\wedge$ IntC $\wedge$ IntP, that is, the one which includes all the notions for confidentiality and authenticity. However, from the above relations among the notions, we can simply define the strongest security notion for authenticated encryption in unconditional setting as follows:

Definition 9 (Strong Security): Let Π be an authenticated encryption. Then, Π is said to be (ω,t_1,t_2)-*secure* if Π meets both (ω,t_1,t_2)-APS and (ω,t_1,t_2)-IntC.

4. Analysis of Generic Composition Methods in Unconditional Security Setting

4.1 Generic Composition Methods

Let Π be an encryption scheme specified by an encryption algorithm ENC_{Π} and a decryption algorithm DEC_{Π}. Let Λ be a signature scheme specified by a signing algorithm SIG_{Λ} and a verification algorithm VER_{Λ}. We define typical three types of composition methods to construct an authenticated encryption $\bar{\Pi}$ based on Π and Λ in the sequel. Consider the case that a sender S_i generates a ciphertext $\tilde{c}$ of a plaintext m and then sends it to a receiver R_j in our model in Sect. 2. Here, let e and s be S_i's encryption key in Π and S_i's signing key in Λ, respectively. Also, let d and v be R_j's decryption key in Π and R_j's verification key in Λ, respectively. Then, S_i's encryption key in $\bar{\Pi}$ is $\tilde{e} := (e,s)$, and R_j's decryption key in $\bar{\Pi}$ is $\tilde{d} := (d,v)$. The typical three types of composition methods, denoted by *Encrypt-and-Sign*, *Sign-then-Encrypt* and *Encrypt-then-Sign*, are defined as follows:

- *Encrypt-and-Sign*:
  $\tilde{c} = ENC_{\bar{\Pi}}(\tilde{e},m,R_j) = (c,a)$, where $c = ENC_{\Pi}(e,m,R_j)$ and $a = SIG_{\Lambda}(s,m)$. $DEC_{\bar{\Pi}}$ is performed by first performing DEC_{Π} to recover m and then verifying the signature a. If DEC_{Π} outputs $\perp$ or VER_{Λ} outputs $false$, $DEC_{\bar{\Pi}}$ outputs $\perp$ implying that the ciphertext is invalid.
- *Sign-then-Encrypt*:
  $\tilde{c} = ENC_{\bar{\Pi}}(\tilde{e},m,R_j) = ENC_{\Pi}(e,(m,a),R_j)$, where $a = SIG_{\Lambda}(s,m)$. $DEC_{\bar{\Pi}}$ is performed by first performing DEC_{Π} to recover (m,a) and then verifying the signature a. If DEC_{Π} outputs $\perp$ or VER_{Λ} outputs $false$, $DEC_{\bar{\Pi}}$ outputs $\perp$ implying that the ciphertext is invalid.
- *Encrypt-then-Sign*:

$\tilde{c} = ENC_{\bar{\Pi}}(\tilde{e}, m, R_j) = (c, a)$, where $c = ENC_{\Pi}(e, m, R_j)$ and $a = SIG_{\Lambda}(s, c)$. $DEC_{\bar{\Pi}}$ is performed by first verifying the signature a and then performing DEC_{Π} to recover m. If VER_{Λ} outputs $false$ or DEC_{Π} outputs $\perp$, $DEC_{\bar{\Pi}}$ outputs $\perp$ implying that the ciphertext is invalid.

In the rest of this section, we analyze the security of the typical three types of composition methods mentioned above.

4.2 Encrypt-and-Sign

The following theorems show that the Encrypt-and-Sign composition method is not always secure even if the given encryption meets APS and the given signature meets EAUF. The proofs are similar to those of [4].

Theorem 4: Given an encryption scheme Π which meets (ω, t_1, t_2)-APS and a signature scheme Λ which meets (ω, t_1, t_2)-EAUF, there exists a signature scheme Λ' such that Λ' meets (ω, t_1, t_2)-EAUF, but the scheme $\bar{\Pi}$ formed by the Encrypt-and-Sign composition method based on Π and Λ' is not (ω, t_1, t_2)-APS.

Proof. Let $\Pi = (GEN_{\Pi}, ENC_{\Pi}, DEC_{\Pi})$ be the given encryption scheme and $\Lambda = (GEN_{\Lambda}, SIG_{\Lambda}, VER_{\Lambda})$ the given signature scheme. We construct a signature scheme $\Lambda' = (GEN_{\Lambda'}, SIG_{\Lambda'}, VER_{\Lambda'})$ as follows: (i) $GEN_{\Lambda'}$: $GEN_{\Lambda'} = GEN_{\Lambda}$; (ii) $SIG_{\Lambda'}$: for a message m, $SIG_{\Lambda'}(s, m) := m \| SIG_{\Lambda}(s, m)$. Consequently, the signed message is $(m, SIG_{\Lambda'}(s, m))$; and (iii) $VER_{\Lambda'}$: for a signed message (m, a), parse a as $a_1 \| a_2$ where $|a_1| = |m|$. If $m = a_1$ and $VER_{\Lambda}(v, (m, a_2), S_i) = true$, $VER_{\Lambda'}(v, (m, a), S_i) = true$. Otherwise, $VER_{\Lambda'}(v, (m, a), S_i) = false$. Then, it is shown that Λ' is (ω, t_1, t_2)-EAUF if Λ is (ω, t_1, t_2)-EAUF. Then, however, in $\bar{\Pi}$ which is formed by the Encrypt-and-Sign composition method based on Π and Λ',

$$\begin{aligned} & ENC_{\bar{\Pi}}(\tilde{e}, m, R_j) \\ & \quad = (ENC_{\Pi}(e, m, R_j), SIG_{\Lambda'}(s, m)) \\ & \quad = (ENC_{\Pi}(e, m, R_j), m \| SIG_{\Lambda}(s, m)). \end{aligned}$$

Obviously, $\bar{\Pi}$ is not (ω, t_1, t_2)-APS. □

Theorem 5: Given an encryption scheme Π which meets (ω, t_1, t_2)-APS and a signature scheme Λ which meets (ω, t_1, t_2)-EAUF, there exists an encryption scheme Π' such that Π' meets (ω, t_1, t_2)-APS, but the scheme $\bar{\Pi}$ formed by the Encrypt-and-Sign composition method based on Π' and Λ is not (ω, t_1, t_2)-IntC.

Proof. Let $\Pi = (GEN_{\Pi}, ENC_{\Pi}, DEC_{\Pi})$ be the given encryption scheme and $\Lambda = (GEN_{\Lambda}, SIG_{\Lambda}, VER_{\Lambda})$ the given signature scheme. We construct an encryption scheme $\Pi' = (GEN_{\Pi'}, ENC_{\Pi'}, DEC_{\Pi'})$ as follows: (i) $GEN_{\Pi'}$: $GEN_{\Pi'} = GEN_{\Pi}$; (ii) $ENC_{\Pi'}$: for a plaintext m, let $c = ENC_{\Pi}(e, m, R_j)$. Then, choose $r \in \{0, 1\}$ uniformly at random. Then, $ENC_{\Pi'}(e, m, R_j) := r \| c$; (iii) $DEC_{\Pi'}$: for a ciphertext c, parse c as $r \| c'$ where r is a bit. Then, $DEC_{\Pi'}(d, c, S_i) := DEC_{\Pi}(d, c', S_i)$. Then, it is shown that Π' is (ω, t_1, t_2)-APS if Π is (ω, t_1, t_2)-APS. Then, however, $\bar{\Pi}$ formed by the Encrypt-and-Sign composition method based on Π' and Λ,

$$\begin{aligned} & ENC_{\bar{\Pi}}(\tilde{e}, m, R_j) \\ & \quad = (ENC_{\Pi'}(e, m, R_j), SIG_{\Lambda}(s, m)) \\ & \quad = (r \| ENC_{\Pi}(e, m, R_j), SIG_{\Lambda}(s, m)). \end{aligned}$$

Let $(r \| c, a)$ be a ciphertext generated by the sender S_i. Then, $DEC_{\bar{\Pi}}(d, (r' \| c, a), S_i) \neq \perp$, where $r' = 1$ if $r = 0$ and $r' = 0$ if $r = 1$. Thus, $\bar{\Pi}$ is not (ω, t_1, t_2)-IntC. □

4.3 Sign-then-Encrypt

The following theorem shows that the Sign-then-Encrypt composition method is not always secure even if the given encryption meets APS and the given signature meets EAUF. The proof is similar to that of [4].

Theorem 6: Given an encryption scheme Π which meets (ω, t_1, t_2)-APS and a signature scheme Λ which meets (ω, t_1, t_2)-EAUF, there exists an encryption scheme Π' such that Π' meets (ω, t_1, t_2)-APS, but the scheme $\bar{\Pi}$ formed by the Sign-then-Encrypt composition method based on Π' and Λ is neither (ω, t_1, t_2)-APS nor (ω, t_1, t_2)-IntC.

Proof. Let $\Pi = (GEN_{\Pi}, ENC_{\Pi}, DEC_{\Pi})$ be the given encryption scheme and $\Lambda = (GEN_{\Lambda}, SIG_{\Lambda}, VER_{\Lambda})$ the given signature scheme. We construct the encryption scheme $\Pi' = (GEN_{\Pi'}, ENC_{\Pi'}, DEC_{\Pi'})$ as in the proof of Theorem 5. Then, it is shown that Π' is (ω, t_1, t_2)-APS if Π is (ω, t_1, t_2)-APS. However, in $\bar{\Pi}$ formed by the Sign-then-Encrypt composition method based on Π' and Λ,

$$\begin{aligned} & ENC_{\bar{\Pi}}(\tilde{e}, m, R_j) \\ & \quad = ENC_{\Pi'}(e, (m, SIG_{\Lambda}(s, m)), R_j) \\ & \quad = r \| ENC_{\Pi}(e, (m, SIG_{\Lambda}(s, m)), R_j). \end{aligned}$$

Obviously, as in the proof of Theorem 5, $\bar{\Pi}$ is not (ω, t_1, t_2)-IntC. Let $(r \| c)$ be a target ciphertext. Then, the adversary can obtain the answer of the query $(r' \| c)$, where $r' = 1$ if $r = 0$ and $r' = 0$ if $r = 1$, by asking the receiver R_j the query, regarding R_j as a decryption-oracle. Therefore, $\bar{\Pi}$ is not (ω, t_1, t_2)-APS. □

4.4 Encrypt-then-Sign

The following theorem shows that the Encrypt-then-Sign composition method is always secure if the given encryption meets APS and the given signature meets EAUF.

Theorem 7: Given an encryption scheme Π which meets (ω, t_1, t_2)-APS, and a signature scheme Λ which meets (ω, t_1, t_2)-EAUF, then the scheme $\bar{\Pi}$ formed by the Encrypt-then-Sign composition method based on Π and Λ meets both (ω, t_1, t_2)-APS and (ω, t_1, t_2)-IntC.

Proof. Let $\Pi = (GEN_\Pi, ENC_\Pi, DEC_\Pi)$ be the given encryption scheme and $\Lambda = (GEN_\Lambda, SIG_\Lambda, VER_\Lambda)$ the given signature scheme. Then

$$ENC_{\bar{\Pi}}(\tilde{e}, m, R_j) = (c, a),$$

where $c = ENC_\Pi(e, m, R_j)$ and $a = SIG_\Lambda(s, c)$. Since Π is (ω, t_1, t_2)-APS and Λ is (ω, t_1, t_2)-EAUF, without loss of generality we can assume that $P_{\Pi}^{PS} \le \epsilon$ and $P_{\Lambda}^{EAUF} \le \epsilon$, where $P_{\Lambda}^{EAUF} := \max\{P_{\Lambda,1}^{EAUF}, P_{\Lambda,2}^{EAUF}\}$.

First, by the definitions of $P_{\bar{\Pi}}^{IntC}$ and P_{Λ}^{EAUF}, it easily follows that $P_{\bar{\Pi}}^{IntC} \le P_{\Lambda}^{EAUF}$. Thus, $P_{\bar{\Pi}}^{IntC} \le \epsilon$ if $P_{\Lambda}^{EAUF} \le \epsilon$, which implies that $\bar{\Pi}$ is (ω, t_1, t_2)-IntC if Λ is (ω, t_1, t_2)-EAUF.

Secondly, we will show that $\bar{\Pi}$ is (ω, t_1, t_2)-APS if Π is (ω, t_1, t_2)-APS and Λ is (ω, t_1, t_2)-EAUF. Before providing a formal proof, we briefly explain the idea of the proof. Let (c, a) be a target ciphertext in $\bar{\Pi}$. The ciphertext which is different from (c, a) has the form (c', a') with $c' \ne c$, or (c, a'') with $a'' \ne a$. Even if the adversary asks the receiver R_j, regarding him as a decryption-oracle, the query of the form (c', a') with $c' \ne c$, the adversary cannot obtain any partial information on the plaintext underlying c since Π is (ω, t_1, t_2)-APS. On the other hand, even if the adversary asks the receiver R_j, regarding him as a decryption-oracle, the query of the form (c, a'') with $a'' \ne a$, the adversary cannot obtain the meaningful answer since Λ is (ω, t_1, t_2)-EAUF. Thus, the queries of this form cannot help him to derive any partial information on the plaintext underlying c. Therefore, the adversary cannot eventually obtain any partial information on the plaintext underlying c, even if he adaptively asks queries.

Now, we show the formal proof that $\bar{\Pi}$ is (ω, t_1, t_2)-APS if Π is (ω, t_1, t_2)-APS and Λ is (ω, t_1, t_2)-EAUF. We note that $P_{\bar{\Pi}}^{PS}(S_i, R_j, W)$ is defined as follows.

$$\begin{aligned} P_{\bar{\Pi}}^{PS}(S_i, R_j, W) &:= \max_{e_W} \max_{\tilde{M}_{S_i}} \max_{\tilde{C}_{R_j}} \\ &\max_{\tilde{M}_{S_1},\ldots,\tilde{M}_{S_l},\ldots,\tilde{M}_{S_{n_1}} (l \ne i)} \max_{\tilde{C}_{R_1},\ldots,\tilde{C}_{R_s},\ldots,\tilde{C}_{R_{n_2}} (s \ne j)} \\ &\max_{\tilde{c}=(c,a)} \Bigg\{ \sum_{m \in \mathcal{M}_k} \Big| \Pr(m|\tilde{c}, e_W, \\ &\{\tilde{M}_{S_l} | 1 \le l \le n_1\}, \{\tilde{C}_{R_s} | 1 \le s \le n_2\}) - \Pr(m) \Big| \Bigg\}. \end{aligned}$$

Here, in the above, any element of $\tilde{M}_{S_l}$ $(1 \le l \le n_1)$ is a pair of a plaintext m_{S_l} and a corresponding ciphertext $\tilde{c}_{S_l} = (c_{S_l}, a_{S_l})$ encrypted by S_l. Then, we define $M_{S_l} := \{(m_{S_l}, c_{S_l})\}$; Any element of $\tilde{C}_{R_s}$ $(1 \le s \le n_2)$ is a pair of a ciphertext $\tilde{c}_{R_s} = (c_{R_s}, a_{R_s})$ and a decryption result of $\tilde{c}_{R_s}$ using $DEC_{\bar{\Pi}}$ by R_s. Then, for $\tilde{C}_{R_s} = \{(\tilde{c}_{R_s}, \text{decryption result of } \tilde{c}_{R_s} \text{ using } DEC_{\bar{\Pi}} \text{ by } R_s)\}$, we define $C_{R_s} := \{(c_{R_s}, \bar{m}_{R_s})\}$, where $\bar{m}_{R_s}$ is defined as follows. If the verification result of $\tilde{c}_{R_s} = (c_{R_s}, a_{R_s})$ using VER_Λ by R_s is *true*, let $\bar{m}_{R_s}$ be the decryption result of c_{R_s} using DEC_Π by R_s. If the verification result of $\tilde{c}_{R_s} = (c_{R_s}, a_{R_s})$ using VER_Λ by R_s is *false*, let $\bar{m}_{R_s} := \emptyset$, where $\emptyset$ means empty-information; and the target ciphertext $\tilde{c} = (c, a)$ is taken over valid ciphertexts from S_i to R_j.

Let d be a decryption key of Π held by R_j, and v a verification key of Λ held by R_j. Also, let $\tilde{d} = (d, v)$ be a decryption key of $\bar{\Pi}$ held by R_j. For $\tilde{C}_{R_j}$ and the target ciphertext $\tilde{c} = (c, a)$, we set

$$\tilde{C}'_{R_j} := \{((c, a'), DEC_{\bar{\Pi}}(\tilde{d}, (c, a'), S_i)) | a' \ne a\} \subset \tilde{C}_{R_j}$$

We consider the following two cases: (i) There exists some $((c, a'), DEC_{\bar{\Pi}}(\tilde{d}, (c, a'), S_i)) \in \tilde{C}'_{R_j}$ such that $DEC_{\bar{\Pi}}(\tilde{d}, (c, a'), S_i) \ne \bot$; (ii) Otherwise, that is, $\tilde{C}'_{R_j} = \{((c, a'), \bot) | a' \ne a\}$ or $\tilde{C}'_{R_j} = \emptyset$.

(i) In this case, the plaintext $m_0 := DEC_{\bar{\Pi}}(\tilde{d}, (c, a'), S_i) = DEC_\Pi(d, c, S_i)$ is revealed. Then, for any e_W, $\{\tilde{M}_{S_l} | 1 \le l \le n_1\}$, and $\{\tilde{C}_{R_s} | 1 \le s \le n_2, s \ne j\}$,

$$\begin{aligned} &\sum_{m \in \mathcal{M}_k} \Big| \Pr(m|\tilde{c} = (c, a), e_W, \{\tilde{M}_{S_l} | 1 \le l \le n_1\}, \\ &\qquad \tilde{C}_{R_j}, \{\tilde{C}_{R_s} | 1 \le s \le n_2, s \ne j\}) - \Pr(m) \Big| \\ &= \sum_{m \ne m_0} \Big| 0 - \Pr(m) \Big| + (1 - \Pr(m_0)) \\ &= 2(1 - \Pr(m_0)) \\ &= 2\delta, \end{aligned} \tag{4}$$

where $\delta = 1 - \Pr(m_0)$ $(0 \le \delta \le 1)$.

(ii) In this case, for any e_W, $\{\tilde{M}_{S_l} | 1 \le l \le n_1\}$, and $\{\tilde{C}_{R_s} | 1 \le s \le n_2, s \ne j\}$,

$$\begin{aligned} &\sum_{m \in \mathcal{M}_k} \Big| \Pr(m|\tilde{c} = (c, a), e_W, \{\tilde{M}_{S_l} | 1 \le l \le n_1\}, \\ &\qquad \tilde{C}_{R_j}, \{\tilde{C}_{R_s} | 1 \le s \le n_2, s \ne j\}) - \Pr(m) \Big| \\ &\le \sum_{m \in \mathcal{M}_k} \Bigg\{ \Big| \Pr(m|\tilde{c} = (c, a), e_W, \{\tilde{M}_{S_l} | 1 \le l \le n_1\}, \\ &\qquad \tilde{C}_{R_j}, \{\tilde{C}_{R_s} | 1 \le s \le n_2, s \ne j\}) \\ &\qquad - \Pr(m|c, e_W, \{M_{S_l} | 1 \le l \le n_1\}, \\ &\qquad C_{R_j}, \{C_{R_s} | 1 \le s \le n_2, s \ne j\}) \Big| \\ &\qquad + \Big| \Pr(m|c, e_W, \{M_{S_l} | 1 \le l \le n_1\}, \\ &\qquad C_{R_j}, \{C_{R_s} | 1 \le s \le n_2, s \ne j\}) \\ &\qquad - \Pr(m) \Big| \Bigg\} \\ &= \sum_{m \in \mathcal{M}_k} \Big| \Pr(m|c, e_W, \{M_{S_l} | 1 \le l \le n_1\}, C_{R_j}, \\ &\qquad \{C_{R_s} | 1 \le s \le n_2, s \ne j\}) - \Pr(m) \Big| \qquad (5) \\ &\le P_{\Pi}^{PS}(S_i, R_j, W) \\ &\le P_{\Pi}^{PS} \\ &\le \epsilon, \qquad (6) \end{aligned}$$

where the equality (5) follows from Lemma 1 in Appendix.

Let E be the event that the case (i) occurs. Then, for S_i, R_j and W,

$$\begin{aligned} P^{PS}_{\bar{\Pi}}(S_i, R_j, W) &\le \Pr(E)\cdot 2\delta + \Pr(\neg E)\cdot\epsilon \qquad (7)\\ &\le P^{EAUF}_{\Lambda}\cdot 2\delta + \epsilon \\ &\le 3\epsilon, \end{aligned}$$

where the inequalty (7) follows from (4) and (6). From the above, it follows that $P^{PS}_{\bar{\Pi}} \le 3\epsilon$. Therefore, $\bar{\Pi}$ is (ω, t_1, t_2)-APS. □

Acknowledgment

The authors would like to thank the anonymous reviewers for their valuable comments.

References

[1] J. An, Y. Dodis, and T. Rabin, "On the security of joint signature and encryption," Advances in Cryptology—EUROCRYPT 2002, LNCS 2332, pp.83–107, Springer-Verlag, 2002.

[2] J. Baek, R. Steinfeld, and Y. Zheng, "Formal proofs for the security of signcryption," PKC 2002, LNCS 2274, pp.80–98, Springer-Verlag, 2002.

[3] M. Bellare, A. Desai, D. Pointcheval, and P. Rogaway, "Relations among notions of security for public-key encryption schemes," Advances in Cryptology—CRYPTO '98, LNCS 1462, pp.26–45, Springer-Verlag, 1998.

[4] M. Bellare and C. Namprempre, "Authenticated encryption: Relations among notions and analysis of the generic composition paradigm," Advances in Cryptology—ASIACRYPT 2000, LNCS 1976, pp.531–545, Springer-Verlag, 2000.

[5] M. Bellare and P. Rogaway, "Encode-then-encipher encryption: How to exploit nonces or redundancy in plaintexts for efficient cryptography," Advances in Cryptology—ASIACRYPT 2000, LNCS 1976, pp.317–330, Springer-Verlag, 2000.

[6] M. De Soete, "Some constructions for authentication-secrecy codes," Advances in Cryptology—EUROCRYPT '88, LNCS 330, pp.57–75, Springer, 1988.

[7] M. De Soete, "Bounds and constructions for authentication-secrecy codes with splitting," Advances in Cryptology—CRYPTO '88, LNCS 403, pp.311–317, Springer, 1990.

[8] D. Dolev, D. Dwork, and M. Naor, "Non-malleable cryptography," 23rd Annual ACM Symposium on Theory of Computing, pp.542–552, 1991.

[9] D. Dolev, D. Dwork, and M. Naor, "Non-malleable cryptography," SIAM J. Comput., vol.30, no.2, pp.391–437, 2000.

[10] S. Goldwasser and S. Micali, "Probabilistic encryption," J. Comput. Syst. Sci., vol.28, pp.270–299, 1984.

[11] S. Goldwasser, S. Micali, and R. Rivest, "A digital signature scheme secure against adaptive chosen message attacks," SIAM J. Comput., vol.17, no.2, pp.281–308, 1988.

[12] G. Hanaoka, J. Shikata, Y. Zheng, and H. Imai, "Unconditionally secure digital signature schemes admitting transferability," Advances in Cryptology—ASIACRYPT 2000, LNCS 1976, pp.130–142, Springer-Verlag, 2000.

[13] G. Hanaoka, J. Shikata, Y. Hanaoka, and H. Imai, "Unconditionally secure anonymous encryption and group authentication," Advances in Cryptology—ASIACRYPT 2002, LNCS 2501, pp.81–99, Springer-Verlag, 2002.

[14] J. Katz and M. Yung, "Unforgeable encryption and chosen ciphertext secure modes of operation," FSE 2000, LNCS 1978, pp.284–299, Springer-Verlag, 2001.

[15] H. Krawczyk, "The order of encryption and authentication for protecting communications (or: how secure is SSL?)," Advances in Cryptology—CRYPTO 2001, LNCS 2139, pp.310–331, Springer-Verlag, 2001.

[16] B. Smeets, P. Vanroose, and Z. Wan, "On the construction of authentication codes with secrecy and codes withstanding spoofing attacks of order $L \ge 2$," Advances in Cryptology—EUROCRYPT '90, LNCS 473, pp.306–312, Springer-Verlag, 1991.

[17] C.E. Shannon, "Communication theory of secrecy systems," Bell Syst. Tech. J., vol.28, pp.656–715, 1949.

[18] 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-Verlag, 2002.

[19] D.R. Stinson, "A construction for authentication codes/secrecy codes from certain combinatorial designs," J. Cryptol., vol.1, pp.119–127, 1988.

[20] Y. Zheng, "Digital signcryption or how to achieve cost (signature & encryption) ≪ cost(signature) + cost (encryption)," Advances in Cryptology—CRYPTO '97, LNCS 1294, pp.165–179, Springer-Verlag, 1997.

Appendix

Lemma 1: With the notations in the proof of Theorem 7,

$$\begin{aligned} &\Pr(m|c, e_W, \{M_{S_l}|1 \le l \le n_1\}, C_{R_j},\\ &\qquad \{C_{R_s}|1 \le s \le n_2, s \ne j\})\\ &= \Pr(m|(c,a), e_W, \{\tilde{M}_{S_l}|1 \le l \le n_1\}, \tilde{C}_{R_j},\\ &\qquad \{\tilde{C}_{R_s}|1 \le s \le n_2, s \ne j\}) \end{aligned}$$

Proof.

$$\begin{aligned} &\Pr(m|c, e_W, \{M_{S_l}|1 \le l \le n_1\}, C_{R_j},\\ &\qquad \{C_{R_s}|1 \le s \le n_2, s \ne j\})\\ &\quad - \Pr(m|(c,a), e_W, \{\tilde{M}_{S_l}|1 \le l \le n_1\}, \tilde{C}_{R_j},\\ &\qquad \{\tilde{C}_{R_s}|1 \le s \le n_2, s \ne j\})\\ &= \Big\{ \Pr(m|c, e_W, \{M_{S_l}|1 \le l \le n_1\}, C_{R_j},\\ &\qquad \{C_{R_s}|1 \le s \le n_2, s \ne j\})\\ &\quad - \Pr(m|c, e_W, \{\tilde{M}_{S_l}|1 \le l \le n_1\}), \tilde{C}_{R_j},\\ &\qquad \{\tilde{C}_{R_s}|1 \le s \le n_2, s \ne j\})\Big\}\\ &\quad + \Big\{ \Pr(m|c, e_W, \{\tilde{M}_{S_l}|1 \le l \le n_1\}), \tilde{C}_{R_j},\\ &\qquad \{\tilde{C}_{R_s}|1 \le s \le n_2, s \ne j\})\\ &\quad - \Pr(m|(c,a), e_W, \{\tilde{M}_{S_l}|1 \le l \le n_1\}), \tilde{C}_{R_j},\\ &\qquad \{\tilde{C}_{R_s}|1 \le s \le n_2, s \ne j\})\Big\}. \qquad (\text{A}\cdot 1) \end{aligned}$$

We first note that

$$\begin{aligned} &\Pr(m|c, e_W, \{\tilde{M}_{S_l}|1 \le l \le n_1\}), \tilde{C}_{R_j},\\ &\qquad \{\tilde{C}_{R_s}|1 \le s \le n_2, s \ne j\})\\ &\quad - \Pr(m|(c,a), e_W, \{\tilde{M}_{S_l}|1 \le l \le n_1\}), \tilde{C}_{R_j},\\ &\qquad \{\tilde{C}_{R_s}|1 \le s \le n_2, s \ne j\})\\ &= 0. \qquad (\text{A}\cdot 2) \end{aligned}$$

This is because m and a are independent after $(c, e_W, \{\tilde{M}_{S_l}|1$

$\leq l \leq n_1\}), \tilde{C}_{R_j}, \{\tilde{C}_{R_s} | 1 \leq s \leq n_2, s \neq j\})$ being given.

Next, we note that the following equality also holds:

$$\begin{aligned}
&\Pr(m|c, e_W, \{M_{S_l}|1 \leq l \leq n_1\}, C_{R_j},\\
&\qquad \{C_{R_s}|1 \leq s \leq n_2, s \neq j\})\\
&- \Pr(m|c, e_W, \{\tilde{M}_{S_l}|1 \leq l \leq n_1\}), \tilde{C}_{R_j},\\
&\qquad \{\tilde{C}_{R_s}|1 \leq s \leq n_2, s \neq j\})\\
&= 0. \qquad (\mathrm{A}\cdot 3)
\end{aligned}$$

In fact, the above equality (A· 3) follows from the definitions of $\tilde{M}_{S_l}$, M_{S_l}, $\tilde{C}_{R_s}$ and C_{R_s} $(1 \leq l \leq n_1, 1 \leq s \leq n_2)$. Thus, from (A· 1), (A· 2) and (A· 3), it follows that

$$\begin{aligned}
&\Pr(m|c, e_W, \{M_{S_l}|1 \leq l \leq n_1\}, C_{R_j},\\
&\qquad \{C_{R_s}|1 \leq s \leq n_2, s \neq j\})\\
&- \Pr(m|(c, a), e_W, \{\tilde{M}_{S_l}|1 \leq l \leq n_1\}, \tilde{C}_{R_j},\\
&\qquad \{\tilde{C}_{R_s}|1 \leq s \leq n_2, s \neq j\})\\
&= 0.
\end{aligned}$$

Therefore, the proof is completed. □

Junji Shikata received the B.S. and M.S. degrees in mathematics from Kyoto University, Japan, in 1994 and 1997, respectively, and the Ph.D. degree in mathematics from Osaka University, Japan, in 2000. From 2000 to 2002 he was a postdoctoral fellow at the Institute of Industrial Science, the University of Tokyo, Japan. Since 2002 he has been with the Graduate School of Environment and Information Sciences, Yokohama National University, Japan. Currently, he is Lecturer of Yokohama National University. His research interests include cryptography, information security, computational number theory and computer science.

Goichiro Hanaoka is currently a Research Fellow of Japan Society for the Promotion of Science (JSPS). He received his bachelors degree in Electronic engineering from the University of Tokyo in 1997, and received his masters and Ph.D. degrees in Information and communication engineering from the University of Tokyo in 1999 and 2002, respectively. He was awarded the excellent paper prize from SITA in 2000. His research interests are in the fields of cryptography, electronic payments and network security.

Yuliang Zheng received his B.Sc. degree in computer science from Nanjing Institute of Technology, China, in 1982, and the M.E. and Ph.D. degrees, both in electrical and computer engineering, from Yokohama National University, Japan, in 1988 and 1991 respectively. From 1982 to 1984 he was with the Guangzhou Research Institute for Communications, Guangzhou (Canton), China. From 1991 to 2001 he was on the faculty of Australian Defence Force Academy, University of Wollongong and Monash University, all in Australia. Currently he is a Professor of Software and Information Systems, University of North Carolina at Charlotte, USA. He has chaired a number of international conferences and is a co-founder of the PKC international workshop series dedicated to the practice and theory in public key cryptography. Dr Zheng is widely known as the inventor of the signcryption public key cryptographic algorithm. His research interests include cryptography, network security, and the protection of critical infrastructures. Dr. Zheng is a member of IACR and ACM, and a senior member of IEEE.

Tsutomu Matsumoto was born in Maebashi, Japan, on October 20, 1958. He received the Dr. Eng. Degree from the University of Tokyo in 1986 and since then his base has been in Yokohama National University where he is enjoying research and teaching in the field of cryptography and information security as a Professor in Graduate School of Environment and Information Sciences. He is a member of Cryptography Research and Evaluation Committee of Japan. He served as the general chair of ASIACRYPT 2000. He is on the board of International Association for Cryptologic Research. He is a member of IEICE Technical Group on Information Security and of IPSJ Special Interest Group on Computer Security and of IEICE Technical Group on Biometrics Security. He received Achievement Award from the IEICE in 1996.

Hideki Imai was born in Shimane, Japan on May 31, 1943. He received the B.E., M.E., and Ph.D. degrees in electrical engineering from the University of Tokyo in 1966, 1968, 1971, respectively. From 1971 to 1992 he was on the faculty of Yokohama National University. In 1992 he joined the faculty of the University of Tokyo, where he is currently a Full Professor in the Institute of Industrial Science. His current research interests include information theory, coding theory, cryptography, spread spectrum systems and their applications. From IEICE (the Institute of Electronics, Information and Communication Engineers) he received Best Book Awards in 1976 and 1991, Best Paper Awards in 1992 and 2003, Yonezawa Memorial Paper Award in 1992, Achievement Award in 1995, Inose Award in 2003, and Distinguished Achievement and Contributions Award in 2004. He also received Golden Jubilee Paper Award from the IEEE Information Theory Society in 1998, and official Commendations from the Minster of Public Management, Home Affairs, Posts and Telecommunications in June 2002 and from the Minister of Economy, Trade and Industry in October 2002. He was awarded Honor Doctor Degree by Soonchunhyang University, Korea in 1999 and Docteur Honoris Causa by the University of Toulon Var, France in 2002. He was elected an IEEE Fellow in 1992 and an IEICE Fellow in 2001. He chaired several committees of scientific societies and organized many international conferences such as IEEE-ITW, IEEE-ISIT, AAECC, PKC, FSE, and WPMC. He served as the leader of research projects supported by JSPS (Japan Society for the Promotion of Science), IPA (Information-technology Promotion Agency, Japan) etc. and as the editor for scientific journals of IEICE, IEEE etc. Dr. Imai was on the board of IEICE (1992–1994, 1996–1999), the IEEE Information Theory Society (IT-SOC, 1993–1998), Japan Society of Security Management (1988–present) and the Society of Information Theory and Its Applications (SITA, 1981–1997). He served as the president of SITA (1997), IEICE Engineering Sciences Society (1998–1999), IEEE Information Theory Society (2004–present), and as the chairman of CRYPTREC (Cryptography Techniques Research and Evaluation Committee of Japan) (2000–present).