PAPER

Coding Theorems for Secret-Key Authentication Systems*

Hiroki KOGA† *and* **Hirosuke YAMAMOTO**††**,** ***Regular Members***

SUMMARY This paper provides the Shannon theoretic coding theorems on the success probabilities of the impersonation attack and the substitution attack against secret-key authentication systems. Though there are many studies that develop lower bounds on the success probabilities, their tight upper bounds are rarely discussed. This paper characterizes the tight upper bounds in an extended secret-key authentication system that includes blocklength K and permits the decoding error probability tending to zero as $K \to \infty$. In the extended system an encoder encrypts K source outputs to K cryptograms under K keys and transmits K cryptograms to a decoder through a public channel in the presence of an opponent. The decoder judges whether K cryptograms received from the public channel are legitimate or not under K keys shared with the encoder. It is shown that $2^{-KI(W;E)}$ is the minimal attainable upper bound of the success probability of the impersonation attack, where $I(W;E)$ denotes the mutual information between a cryptogram W and a key E. In addition, $2^{-KH(E|W)}$ is proved to be the tight upper bound of the probability that the opponent can correctly guess K keys from transmitted K cryptograms, where $H(E|W)$ denotes the conditional entropy of E given W.

key words: *authentication, impersonation attack, substitution attack, information-theoretic bounds, coding theorem*

1. Introduction

Authentication schemes are used in order to guarantee that a message received by a legitimate receiver is actually transmitted from a legitimate sender in the presence of opponents who try to cheat the legitimate receiver. The authentication schemes, which should be designed so that the cheat hardly succeed, are realized by using secret key cryptography or public key cryptography. This paper focuses on a class of the authentication schemes based on secret key cryptography that yields the unconditional security. The unconditionally secure authentication scheme enables authentication even in the case that the opponents have unlimited computational power and know everything about the scheme except for the secret key.

Many papers that treat secret-key authentication systems usually consider the block diagram shown in Fig. 1. In the figure let $M \in \mathcal{M}$ and $E \in \mathcal{E}$ be random variables from a source and a key generator, respectively. Key E is transmitted to both an encoder and a decoder through a secret channel in advance. A legitimate sender encrypts M to a cryptogram $W \in \mathcal{W}$ under E and transmits W to a legitimate receiver through a public channel. The cardinalities of the alphabets $\mathcal{M}, \mathcal{E}$ and $\mathcal{W}$ are assumed to be finite. When the legitimate receiver receives a cryptogram $\hat{W} \in \mathcal{W}$ from the public channel, he decrypts $\hat{W}$ to $\hat{M}$ under E. In the case that no one attacks the authentication system, the legitimate receiver always reproduces $\hat{M} = M$. An opponent, however, may try to impersonate the legitimate sender by injecting a fraudulent cryptogram $W' \in \mathcal{W}$ into the public channel when W is not transmitted. The opponent may also substitute a fraudulent cryptogram $W' \in \mathcal{W}$ for the legitimate cryptogram W transmitted through the public channel in the hope that W' would be decrypted as a source output $M' \neq M$. The first and the second attacks are usually called the *impersonation attack* and the *substitution attack*, respectively. In the presence of the opponent, $\hat{W}$ is either W or W'.

Let P_I and P_S denote the success probabilities of the impersonation attack and the substitution attack, respectively. After Simmons [1] showed $P_I \geq 2^{-I(W;E)}$, several lower bounds on P_I or P_S, e.g., $P_S \geq 2^{-H(E|W)}$, are derived from the same viewpoints as Simmons' [2]–[4], where $I(W;E)$ denotes the mutual information and $H(E|W)$ denote the conditional entropy. These lower bounds, however, are not attainable in general. In addition, the method establishing the lower bounds suggests neither an operational meaning of the lower bounds nor existences of any tight upper bounds of P_I and P_S. This dissatisfaction may arise from the way establishing the lower bounds. They are usually obtained as a consequence of the convexity of $-t \log_2 t$ for $t \in (0,1)$, and hence, gives little insight into actual en-

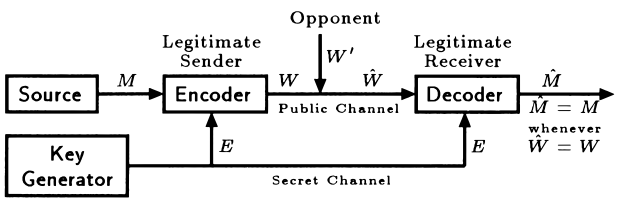

Fig. 1 Block diagram of a secret-key authentication system.

Manuscript received June 1, 1999.
Manuscript revised January 21, 2000.

†The author is with Institute of Engineering Mechanics and Systems, The University of Tsukuba, Tsukuba-shi, 305-8573 Japan.
††The author is with Graduate School of Engineering, The University of Tokyo, Tokyo, 113-8656 Japan.

*This paper was presented at IEEE Information Theory Workshop, Killarney, Ireland, June 22–26, 1998.

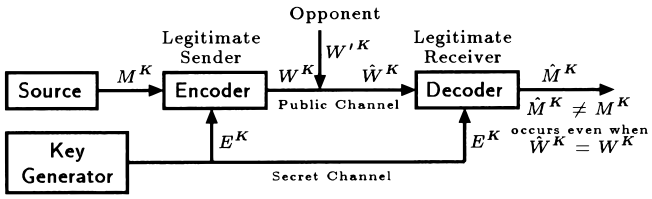

Fig. 2 Block diagram of an extended secret-key authentication system.

coding and decoding schemes. The two probabilities P_I and P_S are also discussed from viewpoints of the combinatorics [5], [6]. It is shown that $P_I \geq |\mathcal{M}|/|\mathcal{W}|$ and $P_S \geq (|\mathcal{M}|-1)/(|\mathcal{W}|-1)$, respectively. However, the optimal construction achieving the equality is limited to a few special cases when there exist certain orthogonal arrays.

In order to unveil another basic properties of the secret-key authentication systems, this paper analyzes them from a viewpoint of the Shannon theory. An extended secret-key authentication system treated throughout this paper is shown in Fig. 2. In the extended system, source output M_k, $k = 1, 2, \ldots, K$, is encrypted to cryptogram W_k under key E_k independently for K times. The legitimate sender transmits $W^K = (W_1, W_2, \ldots, W_K) \in \mathcal{W}^K$ as a block to a legitimate receiver sharing $E^K = (E_1, E_2, \ldots, E_K)$ through a public channel in the presence of an opponent. The opponent may inject $W'^K = (W'_1, W'_2, \ldots, W'_K) \in \mathcal{W}^K$ when W^K is not transmitted or substitute W'^K for W^K when W^K is transmitted. The legitimate receiver receives $\hat{W}^K = (\hat{W}_1, \hat{W}_2, \ldots, \hat{W}_K) \in \mathcal{W}^K$ from the public channel, judges whether $\hat{W}^K = W^K$ or $\hat{W}^K = W'^K$ and tries to reproduce $M^K = (M_1, M_2, \ldots, M_K)$.

There are two big differences between the secret-key authentication systems given in Fig. 1 and Fig. 2. Firstly, the decoder in Fig. 2 is assumed to permit sufficiently small the decoding error probability, which tends to zero as $K \to \infty$, when $\hat{W}^K = W^K$. Permitting this negligible decoding error probability is essential when the extended secret-key authentication system is analyzed from a viewpoint of the Shannon theory. Actually, almost all source coding theorems and channel coding theorems for block coding in the Shannon theory do not hold without permitting decoding error probability tending to zero as the blocklength goes to infinity. Secondly, the decoder in Fig. 2 can statistically check whether $(\hat{W}_k, E_k)$, $k = 1, 2, \ldots, K$, is independently generated according to P_{WE}, where P_{WE} denotes the joint probability distribution of a cryptogram W and a key E. Such decoder can realize a secure secret-key authentication system because it is usually be hard for the opponent not knowing E^K to find W'^K such that (W'_k, E_k), $k = 1, 2, \ldots, K$, is independently generated according to P_{WE}.

This paper attempts to obtain operational meanings of $I(W;E)$ and $H(E|W)$ appearing in the Simmons' lower bounds. Let $P_I^{(K)}$ and $P_S^{(K)}$ denote the success probabilities of the impersonation attack and the substitution attack in the extended secret-key authentication system in Fig. 2, respectively, while let $P_{error}^{(K)}$ be the decoding error probability. We first introduce a class $\mathcal{G}$ of sequences of decoders $\{G_K\}_{K=1}^{\infty}$ that enables to define $P_{error}^{(K)}$ and $P_S^{(K)}$ adequately. We show that $I(W;E)$ is the maximal attainable lower bound of $-\frac{1}{K}\log_2 P_I^{(K)}$ for $\{G_K\}_{K=1}^{\infty} \in \mathcal{G}$ satisfying $P_{error}^{(K)} \to 0$ as $K \to \infty$. We explicitly construct a sequence of decoders $\{G_K^*\}_{K=1}^{\infty} \in \mathcal{G}$ attaining the lower bound and satisfying $P_{error}^{(K)} \leq 2^{-K^{1-\varepsilon}+o(K^{1-\varepsilon})}$, where $\varepsilon \in (0,1)$ is a constant that can be arbitrarily close to zero. Notice that, if the Simmons' bound is applied to the extended secret-key authentication system in Fig. 2, for each $K \geq 1$ only $-\frac{1}{K}\log_2 P_I^{(K)} \leq I(W;E)$ holds for all decoder G_K satisfying $P_{error}^{(K)} = 0$. Notice again that the Simmons' bound does not guarantee the existence of G_K satisfying the inequality with equality.

Compared with $P_I^{(K)}$, the analysis on the asymptotic behavior of $P_S^{(K)}$ is much more difficult. However, we can evaluate the asymptotic behavior of $P_G^{(K)}$, the probability that the opponent can correctly guess E^K from W^K. Usually, $P_G^{(K)}$ gives a lower bound of $P_S^{(K)}$. In this paper, we prove that all $\{G_K\}_{K=1}^{\infty} \in \mathcal{G}$ with $P_{error}^{(K)} \to 0$ satisfy $\limsup_{K\to\infty} -\frac{1}{K}\log_2 P_G^{(K)} \leq H(E|W)$. In particular, $\{G_K^*\}_{K=1}^{\infty}$ turns out to satisfy $-\frac{1}{K}\log_2 P_G^{(K)} \to H(E|W)$ as $K \to \infty$.

We note that a coding theorem on a secret-key authentication system is also discussed by Sgarro [7]. In Sgarro's scenario an encoder compresses a source block $M^K \in \mathcal{M}^K$ by an entropy coding and encrypts M^K to a cryptogram $W \in \mathcal{W}$ under a key $E \in \mathcal{E}$. Here, notice that E and W are not elements of $\mathcal{E}^K$ and $\mathcal{W}^K$, respectively, while M^K belongs to $\mathcal{M}^K$. It is shown that, if $\frac{1}{K}\log_2 |\mathcal{W}| > H(M)$, there exists a pair of an encoder and a decoder that makes both of P_I and the decoding error probability arbitrarily small for sufficiently large K, where $H(M)$ denotes the entropy of M. His coding theorem, however, is not so sharp. In fact, no relationship is clarified between Sgarro's coding theorem and the Simmons' bound.

Maurer [8] points out a relationship between the hypothesis testing and the secret-key authentication systems. If in Fig. 1 the opponent tries to impersonate the legitimate sender by injecting W' generated according to a probability distribution on $\mathcal{W}$, then the decoder can be regarded as a hypothesis tester. In fact, the decoding error and the success of such impersonation attack correspond to the type I error and the type II error of the hypothesis tester, respectively. In [8] $P_I \geq 2^{-I(W;E)}$ is proved by using an inequality on the hypothesis testing and the fact that the type I

error probability is equal to zero. Since the decoder in Fig. 2 can also be regarded as a hypothesis tester with a nonzero type I error probability, the viewpoint from the hypothesis testing is also useful in this paper. In particular, the tightness of $I(W;E)$ in the asymptotic behavior of $-\frac{1}{K}\log_2 P_I^{(K)}$ is proved by using the same inequality.

This paper is organized as follows. In Sect. 2 the authentication coding problem is mathematically formulated with introducing notations. Formal definitions of $P_I^{(K)}$ and $P_{error}^{(K)}$ are given. After defining $P_G^{(K)}$ and a class $\mathcal{G}$ for sequences of decoders, coding theorems that characterize asymptotic behaviors of $P_I^{(K)}$ and $P_G^{(K)}$ are claimed in Sect. 3. They are proved in Sect. 4 by using the theory of the type and the typical sequences.

2. Problem Formulation

This section is devoted to mathematical formulation of the problem to be considered. Let $\mathcal{M}, \mathcal{E}$ and $\mathcal{W}$ be finite sets satisfying $|\mathcal{M}| \le |\mathcal{W}|$. In Fig. 2 let $M^K = (M_1, M_2, \ldots, M_K) \in \mathcal{M}^K$ be a K-tuple of random variables independently generated from a source according to a probability distribution P_M. Without loss of generality, $P_M(m) > 0$ is assumed for all $m \in \mathcal{M}$. Key $E^K = (E_1, E_2, \ldots, E_K) \in \mathcal{E}^K$ is a K-tuple of random variables independently generated from a key generator according to a probability distribution P_E satisfying $P_E(e) > 0$ for all $e \in \mathcal{E}$. Key E^K is transmitted to both an encoder and a decoder in advance through a secret channel perfectly protected against the opponent. Suppose that E_k is independent of M_k for $k = 1, 2, \ldots, K$. The probability distributions of M^K and E^K are denoted by P_{M^K} and P_{E^K}, respectively. Since M^K and E^K are independent random variables, the joint probability distribution $P_{M^K E^K}$ of M^K and E^K is equal to $P_{M^K} P_{E^K}$.

A legitimate sender encrypts M^K to a K-tuple of cryptograms $W^K = (W_1, W_2, \ldots, W_K) \in \mathcal{W}^K$ under E^K by using an encoder $F_K : \mathcal{M}^K \times \mathcal{E}^K \to \mathcal{W}^K$. For all $K \ge 1$ define F_K as a mapping that generates W^K according to

$$W_k = f(M_k, E_k) \quad \text{for all } k = 1, 2, \ldots, K, \tag{1}$$

where $f : \mathcal{M} \times \mathcal{E} \to \mathcal{W}$ is a mapping satisfying $f(m,e) \ne f(m',e)$ for all $(m,e) \ne (m',e)$. That is, $f(\,\cdot\,, e)$ is one-to-one for each $e \in \mathcal{E}$. Notice that such f is easily constructed since $|\mathcal{M}| \le |\mathcal{W}|$ is assumed. The probability distribution of $W = f(M,E)$ is written as

$$P_W(w) = \sum_{m \in \mathcal{M}} \sum_{e \in \mathcal{E}} P_M(m) P_E(e) \chi(w, f(m,e)),\ w \in \mathcal{W},$$

where $\chi(w, f(m,e)) = 1$ if $w = f(m,e)$ and 0 otherwise. Clearly, (W_k, E_k), $k = 1, 2, \ldots, K$, become K pairs of random variables independently generated according to

f	m_1	m_2
e_1	w_1	w_3
e_2	w_1	w_4
e_3	w_2	w_3
e_4	w_2	w_4

g	w_1	w_2	w_3	w_4
e_1	m_1	λ	m_2	λ
e_2	m_1	λ	λ	m_2
e_3	λ	m_1	m_2	λ
e_4	λ	m_1	λ	m_2

Fig. 3 Example of f and g when $|\mathcal{M}| = 2$ and $|\mathcal{E}| = |\mathcal{W}| = 4$.

$P_{WE} = P_W P_{E|W}$, where P_{WE} denotes the joint probability distribution of W and E and $P_{E|W}$ denotes the conditional probability distribution of E given W. The probability distribution of W^K, the joint probability distribution of W^K and E^K, and the conditional probability distribution of E^K given W^K are denoted by $P_{W^K}, P_{W^K E^K}$ and $P_{E^K|W^K}$, respectively.

Throughout this paper $f : \mathcal{M} \times \mathcal{E} \to \mathcal{W}$ is an arbitrarily fixed mapping satisfying $I(W;E) > 0$, where $I(W;E)$ denotes the mutual information defined as

$$I(W;E) = \sum_{w \in \mathcal{W}} \sum_{e \in \mathcal{E}} P_W(w) P_{E|W}(e|w) \log_2 \frac{P_{E|W}(e|w)}{P_E(e)}.$$

The mutual information $I(W;E)$ is also denoted by $I(P_W; P_{E|W})$. Since $f(\,\cdot\,, e)$ is one-to-one for each $e \in \mathcal{E}$, m can be reproduced from $w = f(m,e)$ and e by using the following mapping $g : \mathcal{W} \times \mathcal{E} \to \mathcal{M} \cup \{\lambda\}$:

$$g(w,e) = \begin{cases} m, & \text{if } f(m,e) = w, \\ \lambda, & \text{if } w \notin \{f(m,e) : m \in \mathcal{M}\}. \end{cases} \tag{2}$$

It is easy to check that $g(f(m,e),e) = m$ for all $(m,e) \in \mathcal{M} \times \mathcal{E}$. Actually, f and g can be used as an encoder and a decoder, respectively, in the secret-key authentication system given in Fig. 1. An example of a pair of f and g in case of $\mathcal{M} = \{m_1, m_2\}$, $\mathcal{E} = \{e_1, e_2, e_3, e_4\}$ and $\mathcal{W} = \{w_1, w_2, w_3, w_4\}$ is given in Fig. 3. If M and E are uniformly distributed over $\mathcal{M}$ and $\mathcal{E}$, respectively, W is uniformly distributed over $\mathcal{W}$. Furthermore, in such a case since $P_{W|E}(w|e) = \frac{1}{2}$ for all $(w,e) \in \mathcal{W} \times \mathcal{E}$ satisfying $g(w,e) \ne \lambda$, it is easy to verify $I(W;E) = 1$.

In the presence of an opponent who may inject $W'^K \in \mathcal{W}^K$ into the public channel, a legitimate receiver receives $\hat{W}^K = (\hat{W}_1, \hat{W}_2, \ldots, \hat{W}_K) \in \mathcal{W}^K$ that equals either W^K or W'^K. The legitimate receiver decrypts $\hat{W}^K$ under E^K by using a decoder $G_K : \mathcal{W}^K \times \mathcal{E}^K \to \mathcal{M}^K \cup \{\Lambda\}$. If $G_K(\hat{W}^K, E^K) \in \mathcal{M}^K$, the legitimate receiver accepts $\hat{W}^K = W^K$ and reproduces $\hat{M}^K = G_K(\hat{W}^K, E^K)$. Otherwise, he rejects $\hat{W}^K$ since he judges that the opponent injected fraudulent W'^K.

The opponent is supposed to know anything on the authentication system given in Fig. 2 but M^K and E^K. That is, he knows K, F_K, G_K, P_M, P_E and P_W and he can observe W^K transmitted through the public channel, but he does not know realizations of M^K and E^K. The opponent may impersonate the legitimate sender by injecting $W'^K \in \mathcal{W}^K$ into the public channel when W^K is not transmitted. Such impersonation attack succeeds only when W'^K satisfies $G_K(W'^K, E^K) \in \mathcal{M}^K$

under E^K unknown to the opponent. The success probability of the impersonation attack is defined as

$$P_I^{(K)} = \max_{w'^K \in \mathcal{W}^K} \sum_{e^K \in \mathcal{E}^K} P_{E^K}(e^K)\chi_I(w'^K, e^K), \quad (3)$$

where

$$\chi_I(w'^K, e^K) = \begin{cases} 1, & \text{if } G_K(w'^K, e^K) \in \mathcal{M}^K, \\ 0, & \text{otherwise.} \end{cases}$$

That is, $P_I^{(K)}$ means the probability of the successful impersonation attack for the case that the opponent chooses optimal W'^K.

The opponent may interrupt the transmission of W^K and send W'^K to the legitimate receiver in hope that W'^K would be decrypted as $M'^K = G_K(W'^K, E^K) \in \mathcal{M}^K$ not equal to M^K. In this paper the substitution attack is supposed to succeed when both (i) $G_K(W'^K, E^K) \in \mathcal{M}^K$, and (ii) $(G_K(W'^K, E^K))_k \neq g(W_k, E_k)$ for some $1 \leq k \leq K$, are satisfied, where $(G_K(W'^K, E^K))_k$ denotes the k-th component of $G_K(W'^K, E^K)$. The success probability of the substitution attack is defined as follows:

$$P_S^{(K)} = \sum_{w^K \in \mathcal{W}^K} P_{W^K}(w^K) \cdot \max_{w'^K \in \mathcal{W}^K} \left[\sum_{e^K \in \mathcal{E}^K} P_{E^K|W^K}(e^K|w^K)\chi_S(w'^K, w^K, e^K) \right], \quad (4)$$

where

$$\chi_S(w'^K, w^K, e^K) = \begin{cases} 1, & \text{if all of } G_K(w^K, e^K) \in \mathcal{M}^K, \\ & G_K(w'^K, e^K) \in \mathcal{M}^K \text{ and} \\ & G_K(w^K, e^K) \neq G_K(w'^K, e^K) \\ & \text{are satisfied,} \\ 0, & \text{otherwise.} \end{cases}$$

The second sum in (4) is the probability that w'^K is successfully substituted for w^K. Therefore, $P_S^{(K)}$ means the probability of the successful substitution attack for the case that the opponent choose W'^K optimally according to W^K.

Since $F_K(\cdot, e^K)$ is one-to-one for each $e^K \in \mathcal{E}^K$, construction of G_K satisfying $G_K(F_K(m^K, e^K), e^K) = m^K$ for all $(m^K, e^K) \in \mathcal{M}^K \times \mathcal{E}^K$ is easy. All should be done is to define G_K as $G_K(w^K, e^K) = (g(w_1, e_1), g(w_2, e_2), \ldots, g(w_K, e_K))$ if $(g(w_1, e_1), g(w_2, e_2), \ldots, g(w_K, e_K)) \in \mathcal{M}^K$ and Λ otherwise, where $w^K = (w_1, w_2, \ldots, w_K)$ and $e^K = (e_1, e_2, \ldots, e_K)$. However, we are not interested in such decoder. In fact, if such decoder is used, the secret-key authentication system shown in Fig. 2 can be reduced to the conventional secret-key authentication system in Fig. 1 by replacing $\mathcal{M}^K, \mathcal{E}^K$ and $\mathcal{W}^K$ with $\mathcal{M}, \mathcal{E}$ and $\mathcal{W}$, respectively. For the sake of realizing a secure authentication system, we rather consider decoders that may cause decoding error. The decoding error probability for such decoder G_K is defined as

$$P_{error}^{(K)} = P_{M^K E^K}\left\{G_K(F_K(M^K, E^K), E^K) \neq M^K\right\}. \quad (5)$$

In order to guarantee reliable communication from the legitimate sender to the legitimate receiver, $P_{error}^{(K)}$ should be sufficiently small. To this end, sequences of decoders $\{G_K\}_{K=1}^{\infty}$ satisfying $P_{error}^{(K)} \to 0$ as $K \to \infty$ must be constructed. In the following sections, asymptotic behaviors of $P_I^{(K)}$ and $P_S^{(K)}$ are discussed under the constraint.

3. Main Results

In the secret-key authentication system shown in Fig. 2, a decoder G_K may cause decoding error. For given $W^K = F_K(M^K, E^K)$, however, it is important to notice that there are two different kinds of decoding errors as follows:

(A) $G_K(W^K, E^K) \in \mathcal{M}^K$ and $G_K(W^K, E^K) \neq M^K$,
(B) $G_K(W^K, E^K) = \Lambda$.

If the decoding error of case (A) occurs, it cannot be distinguished from the successful substitution attack by the opponent when $W'^K = W^K$. In order to avoid the decoding error of case (A), we first introduce a class $\mathcal{G}_K$ of decoders. For a given decoder G_K define $\mathcal{R}_0^{(K)}$ and $\mathcal{R}_1^{(K)}$ as

$$\mathcal{R}_0^{(K)} = \left\{(w^K, e^K) \in \mathcal{W}^K \times \mathcal{E}^K : G_K(w^K, e^K) = m^K \text{ such that } F_K(m^K, e^K) = w^K\right\},$$

$$\mathcal{R}_1^{(K)} = \left\{(w^K, e^K) \in \mathcal{W}^K \times \mathcal{E}^K : G_K(w^K, e^K) = \Lambda\right\},$$

respectively. If $\mathcal{R}_0^{(K)}$ and $\mathcal{R}_1^{(K)}$ of G_K form a partition of $\mathcal{W}^K \times \mathcal{E}^K$, G_K is supposed to belong to the class $\mathcal{G}_K$. That is, $G_K \in \mathcal{G}_K$ maps (w^K, e^K) satisfying $(g(w_1, e_1), g(w_2, e_2), \ldots, g(w_K, e_K)) \in \mathcal{M}^K$ to either $(g(w_1, e_1), g(w_2, e_2), \ldots, g(w_K, e_K))$ or Λ, while it maps all (w^K, e^K) satisfying $\lambda \in \{g(w_1, e_1), g(w_2, e_2), \ldots, g(w_K, e_K)\}$ to Λ. Notice that the decoding error of case (A) cannot occur for all $G_K \in \mathcal{G}_K$. We call $\mathcal{R}_0^{(K)}$ the *decodable region* of G_K since all elements in $\mathcal{R}_0^{(K)}$ are correctly decoded by G_K. Define a class $\mathcal{G}$ for sequences of decoders $\{G_K\}_{K=1}^{\infty}$ by

$$\mathcal{G} = \left\{\{G_K\}_{K=1}^{\infty} : G_K \in \mathcal{G}_K \text{ for all } K \geq 1\right\}. \quad (6)$$

Now, an important sequence of decoders $\{G_K^*\}_{K=1}^{\infty} \in \mathcal{G}$ is given. Since for each $K \geq 1$ G_K^* belongs to $\mathcal{G}_K$, description of $\mathcal{R}_0^{*(K)}$ corresponding to G_K^* specifies G_K^*.

Before describing $\mathcal{R}_0^{*(K)}$, for an arbitrarily fixed $\theta > 0$ define $\mathcal{A}^{(K)}$ and $\mathcal{B}^{(K)}(w^K)$ as follows:

$$\mathcal{A}^{(K)} = \{w^K \in \mathcal{W}^K : D(P_{w^K}||P_W) < \theta\}, \quad (7)$$

$$\mathcal{B}^{(K)}(w^K) = \{e^K \in \mathcal{E}^K : D(P_{e^K|w^K}||P_{E|W}|P_{w^K}) < \theta\}, \quad (8)$$

where P_{w^K} denotes the type of w^K, $P_{e^K|w^K}$ denotes the conditional type of e^K given w^K, $D(P_{w^K}||P_W)$ and $D(P_{e^K|w^K}||P_{E|W}|P_{w^K})$ are the divergence and the conditional divergence defined as

$$D(P_{w^K}||P_W) = \sum_{w\in\mathcal{W}} P_{w^K}(w)\log_2\frac{P_{w^K}(w)}{P_W(w)}, \quad (9)$$

$$D(P_{e^K|w^K}||P_{E|W}|P_{w^K}) = \sum_{w\in\mathcal{W}} P_{w^K}(w) \cdot \sum_{e\in\mathcal{E}} P_{e^K|w^K}(e|w)\log_2\frac{P_{e^K|w^K}(e|w)}{P_{E|W}(e|w)}, \quad (10)$$

respectively. See [9] or Sect. 4.1 of this paper for definitions of the type and the conditional type. By using $\mathcal{A}^{(K)}$ and $\mathcal{B}^{(K)}(w^K)$, $\mathcal{R}_0^{*(K)}$ is expressed in the following form:

$$\mathcal{R}_0^{*(K)} = \{(w^K, e^K) \in \mathcal{W}^K \times \mathcal{E}^K : w^K \in \mathcal{A}^{(K)}, e^K \in \mathcal{B}^{(K)}(w^K) \text{ and } \lambda \notin \{g(w_1, e_1), g(w_2, e_2)\ldots, g(w_K, e_K)\}\}. \quad (11)$$

If $(w^K, e^K) \in \mathcal{R}_0^{*(K)}$, then $G_K^*(w^K, e^K) = (g(w_1, e_1), g(w_2, e_2), \ldots, g(w_K, e_K))$. Otherwise, $G_K^*(w^K, e^K) = \Lambda$, i.e., (w^K, e^K) is rejected as fraudulent by the decoder G_K^* even if $(g(w_1, e_1), g(w_2, e_2), \ldots, g(w_K, e_K)) \in \mathcal{M}^K$.

If $\mathcal{R}_0^{*(K)}$ is defined by setting $\theta = K^{-\varepsilon}$ with $0 < \varepsilon < 1$ in (7) and (8), the following theorem holds with respect to $P_{error}^{(K)}$ and $P_I^{(K)}$.

Theorem 1: Fix $\varepsilon \in (0, 1)$ arbitrarily and for each $K \geq 1$ construct $\mathcal{R}_0^{*(K)}$ by setting $\theta = K^{-\varepsilon}$ in the definitions of $\mathcal{A}^{(K)}$ and $\mathcal{B}^{(K)}(w^K)$ given in (7) and (8), respectively. If $\hat{W}^K = W^K$ is decrypted by G_K^* corresponding to $\mathcal{R}_0^{*(K)}$, then $P_{error}^{(K)}$ satisfies

$$P_{error}^{(K)} = 2^{-K^{1-\varepsilon}+o(K^{1-\varepsilon})}. \quad (12)$$

In addition, if $\hat{W}^K = W'^K$ is decrypted by the same G_K^*, for any $\delta \in (0, I(W;E))$ there exists an integer $K_0 = K_0(\varepsilon, \delta)$ such that $P_I^{(K)}$ satisfies

$$P_I^{(K)} \leq 2^{-K[I(W;E)-\delta]} \quad (13)$$

for all integers $K \geq K_0$. □

Actually, Theorem 1 claims that both $\lim_{K\to\infty} P_{error}^{(K)} = 0$ and

$$\liminf_{K\to\infty} -\frac{1}{K}\log_2 P_I^{(K)} \geq I(W;E) \quad (14)$$

are satisfied in case that $\{G_K^*\}_{K=1}^{\infty} \in \mathcal{G}$ is used. The following theorem claims, however, that the limit superior of $-\frac{1}{K}\log_2 P_I^{(K)}$ is less than or equal to $I(W;E)$ for all $\{G_K\}_{K=1}^{\infty} \in \mathcal{G}$ as far as they have the decoding error probabilities tending to zero as $K \to \infty$.

Theorem 2: Any sequence of decoders $\{G_K\}_{K=1}^{\infty} \in \mathcal{G}$ with

$$\lim_{K\to\infty} P_{error}^{(K)} = 0 \quad (15)$$

satisfies

$$\limsup_{K\to\infty} -\frac{1}{K}\log_2 P_I^{(K)} \leq I(W;E). \quad (16)$$

□

Now, the asymptotic behavior of $P_S^{(K)}$ is considered. It is easy to see, however, that $P_S^{(K)}$ defined in (4) satisfies $-\frac{1}{K}\log_2 P_S^{(K)} \to 0$ as $K \to \infty$ since the substitution of W^K for W'^K satisfying $G_K(W'^K, E^K) \in \mathcal{M}^K$ and there exists a k with $((G_K(W'^K, E^K))_k \neq (G_K(W^K, E^K))_k$ is defined to be successful. Actually, the probability that W'^K satisfying $W_1' \neq W_1$ and $W_k' = W_k$ for all $k = 2, 3, \ldots, K$ is accepted by G_K does not depend on K and gives a lower bound of $P_S^{(K)}$. In order to clarify a relationship between the asymptotic behavior of $-\frac{1}{K}\log_2 P_S^{(K)}$ and an information theoretic quantity such as $H(E|W)$, the definition of $P_S^{(K)}$ must be modified. Nevertheless, even if the substitution of W^K for W'^K is supposed to succeed when both (i) $G_K(W'^K, E^K) \in \mathcal{M}^K$, and (ii) $((G_K(W'^K, E^K))_k \neq (G_K(W^K, E^K))_k$ for *all* $1 \leq k \leq K$, are satisfied, the analysis of $P_S^{(K)}$ with increasing K is much more difficult than the analysis of $P_I^{(K)}$ unfortunately. Hence, we will focus on another probability on the substitution attack that decays of exponential order of K and whose exponent is related to $H(E|W)$.

Suppose the situation that the opponent tries to guess E^K from W^K correctly. The opponent who knows E^K can always succeed in his substitution attack. All he has to do is to choose his desirable $M'^K = (M_1', M_2', \ldots, M_K')$ satisfying $M'^K \neq M^K$ arbitrarily and to substitute $W'^K = F_K(M'^K, E^K)$ for W^K. When the opponent takes the optimal strategy in guessing E^K from W^K that (W^K, E^K) is decryptable, its success probability is given by

$$P_G^{(K)} = \sum_{w^K\in\mathcal{W}^K} P_{W^K}(w^K) \cdot \max_{e^K:(w^K,e^K)\in\mathcal{R}_0^{(K)}} P_{E^K|W^K}(e^K|w^K), \quad (17)$$

where $\mathcal{R}_0^{(K)}$ denotes the decodable region of $G_K \in \mathcal{G}_K$

and the maximum in (17) is supposed to be zero if $\{e^K \in \mathcal{E}^K : (w^K, e^K) \in \mathcal{R}_0^{(K)}\} = \phi$. It is easy to prove that $P_G^{(K)} \leq P_S^{(K)}$ under a weak assumption on G_K such as $|\mathcal{R}_0^{(K)}(e^K)| > 1$ for all $e^K \in \mathcal{E}^K$, where $\mathcal{R}_0^{(K)}(e^K) = \{w^K \in \mathcal{W}^K : (w^K, e^K) \in \mathcal{R}_0^{(K)}\}$.

The following two theorems characterize the asymptotic behavior of $P_G^{(K)}$. The two theorems claim that $H(E|W)$ is the maximal attainable lower bound of $-\frac{1}{K}\log_2 P_G^{(K)}$ for $\{G_K\}_{K=1}^{\infty} \in \mathcal{G}$ satisfying $P_{error}^{(K)} \to 0$ as $K \to \infty$.

Theorem 3: Fix $\varepsilon \in (0,1)$ arbitrarily and for each $K \geq 1$ construct G_K^* in the same way as Theorem 1. If $\hat{W}^K = W^K$ is decrypted by G_K^*, then $P_{error}^{(K)}$ satisfies

$$P_{error}^{(K)} = 2^{-K^{1-\varepsilon}+o(K^{1-\varepsilon})}. \tag{18}$$

Moreover, for any $\delta \in (0, H(E|W))$ there exists an integer $K_0 = K_0(\varepsilon, \delta)$ such that $P_G^{(K)}$ satisfies

$$P_G^{(K)} \leq 2^{-K[H(E|W)-\delta]} \tag{19}$$

for all integers $K \geq K_0$. □

Theorem 4: Any sequence of decoders $\{G_K\}_{K=1}^{\infty} \in \mathcal{G}$ with

$$\lim_{K\to\infty} P_{error}^{(K)} = 0 \tag{20}$$

satisfies

$$\limsup_{K\to\infty} -\frac{1}{K}\log_2 P_G^{(K)} \leq H(E|W). \tag{21}$$

□

Notice that Theorem 3 guarantees that $\{G_K^*\}_{K=1}^{\infty} \in \mathcal{G}$ satisfies

$$\liminf_{K\to\infty} -\frac{1}{K}\log_2 P_G^{(K)} \geq H(E|W). \tag{22}$$

Hence, Theorems 1–4 claim that $\{G_K^*\}_{K=1}^{\infty} \in \mathcal{G}$ satisfies both

$$\lim_{K\to\infty} -\frac{1}{K}\log_2 P_I^{(K)} = I(W;E) \tag{23}$$

and

$$\lim_{K\to\infty} -\frac{1}{K}\log_2 P_G^{(K)} = H(E|W). \tag{24}$$

In the secret-key authentication system in Fig. 2, e^K is transmitted to both the encoder and the decoder in advance. Since the ordinary source coding theorem claims that e^K can be transmitted with about $KH(E)$ bits, sharing e^K can be regarded to sharing $KH(E)$ bits in common. From the relation $H(E) = I(W;E) + H(E|W)$, we can intuitively interpret G_K^* as a decoder that uses $KI(W;E)$ random bits to protect W^K against the impersonation attack and $KH(E|W)$ bits to hide E^K from the opponent.

4. Proofs

4.1 Properties of the Type and the Typical Sequences

This subsection briefly summarizes basic properties of the type, the conditional type and the typical sequences used in the proofs of theorems given in the preceding section. Several formulae that play important roles in the proofs are given without proving each of them. See [9] for their proofs.

The type P_{w^K} of $w^K = (w_1, w_2, \ldots, w_K) \in \mathcal{W}^K$ is a probability distribution on $\mathcal{W}$ defined as

$$P_{w^K}(a) = \frac{1}{K}|\{k : w_k = a\}|, \quad a \in \mathcal{W}, \tag{25}$$

where $|\cdot|$ denotes the cardinality of the set. Let $\mathcal{T}_{\mathcal{W}}^{(K)}$ denote the set composed of all the types of $w^K \in \mathcal{W}^K$. The cardinality of $\mathcal{T}_{\mathcal{W}}^{(K)}$ satisfies

$$|\mathcal{T}_{\mathcal{W}}^{(K)}| \leq (K+1)^{|\mathcal{W}|}. \tag{26}$$

For any given $Q_W \in \mathcal{T}_{\mathcal{W}}^{(K)}$ define $\mathcal{W}^K(Q_W)$ as follows:

$$\mathcal{W}^K(Q_W) = \{w^K \in \mathcal{W}^K : P_{w^K} = Q_W\}, \tag{27}$$

which is the subset of $\mathcal{W}^K$ whose all elements have type Q_W. It is known that $\mathcal{W}^K(Q_W)$ satisfies

$$\frac{1}{(K+1)^{|\mathcal{W}|}} \cdot 2^{KH(Q_W)} \leq |\mathcal{W}^K(Q_W)| \leq 2^{KH(Q_W)} \tag{28}$$

for any $Q_W \in \mathcal{T}_{\mathcal{W}}^{(K)}$, where $H(Q_W)$ is the entropy defined as

$$H(Q_W) = \sum_{w\in\mathcal{W}} -Q_W(w)\log_2 Q_W(w). \tag{29}$$

The probability that $w^K \in \mathcal{W}^K(Q_W)$, $Q_W \in \mathcal{T}_{\mathcal{W}}^{(K)}$ is independently generated according to the probability distribution P_W is written as

$$P_{W^K}(w^K) = 2^{-K[H(Q_W)+D(Q_W||P_W)]}, \tag{30}$$

where $D(\cdot||\cdot)$ is the divergence defined in (9).

The conditional type is defined by way of the joint type. The joint type $P_{w^K e^K}$ of $w^K = (w_1, w_2, \ldots, w_K) \in \mathcal{W}^K$ and $e^K = (e_1, e_2, \ldots, e_K) \in \mathcal{E}^K$ is a joint probability distribution on $\mathcal{W}\times\mathcal{E}$ defined as

$$P_{w^K e^K}(a,b) = \frac{1}{K}|\{k : (w_k, e_k) = (a,b)\}| \tag{31}$$

for $(a,b) \in \mathcal{W}\times\mathcal{E}$. The conditional type $P_{e^K|w^K}$ is defined as the stochastic matrices from $\mathcal{W}$ to $\mathcal{E}$ whose all components are determined by

$$P_{w^K}(a)P_{e^K|w^K}(b|a) = P_{w^K e^K}(a,b) \tag{32}$$

for $(a,b) \in \mathcal{W}\times\mathcal{E}$. Let $\mathcal{T}_{\mathcal{E}|\mathcal{W}}^{(K)}$ denote the set composed

of all the conditional types from $\mathcal{W}^K$ to $\mathcal{E}^K$. The cardinality of $\mathcal{T}^{(K)}_{\mathcal{E}|\mathcal{W}}$ is bounded as follows:

$$|\mathcal{T}^{(K)}_{\mathcal{E}|\mathcal{W}}| \le (K+1)^{|\mathcal{W}||\mathcal{E}|}. \tag{33}$$

For any given $Q_W \in \mathcal{T}^{(K)}_{\mathcal{W}}, w^K \in \mathcal{W}^K(Q_W)$ and $Q_{E|W} \in \mathcal{T}^{(K)}_{\mathcal{E}|\mathcal{W}}$ define $\mathcal{E}^K(Q_{E|W}|w^K)$ as

$$\mathcal{E}^K(Q_{E|W}|w^K) = \{e^K \in \mathcal{E}^K : P_{e^K|w^K} = Q_{E|W}\}. \tag{34}$$

Then, $\mathcal{E}^K(Q_{E|W}|w^K)$ satisfies

$$\frac{1}{(K+1)^{|\mathcal{W}||\mathcal{E}|}} \cdot 2^{KH(Q_{E|W}|Q_W)} \le |\mathcal{E}^K(Q_{E|W}|w^K)| \le 2^{KH(Q_{E|W}|Q_W)}, \tag{35}$$

where $H(Q_{E|W}|Q_W)$ is the conditional entropy defined as

$$H(Q_{E|W}|Q_W) = \sum_{w\in\mathcal{W}}\sum_{e\in\mathcal{E}} -Q_W(w)Q_{E|W}(e|w)\log_2 Q_{E|W}(e|w). \tag{36}$$

For any given $Q_W \in \mathcal{T}^{(K)}_{\mathcal{W}}, w^K \in \mathcal{W}^K(Q_W)$ and $Q_{E|W} \in \mathcal{T}^{(K)}_{\mathcal{E}|\mathcal{W}}$, it is easy to prove that

$$P_{E^K|W^K}(e^K|w^K) = 2^{-K[H(Q_{E|W}|Q_W)+D(Q_{E|W}||P_{E|W}|Q_W)]} \tag{37}$$

for all $e^K \in \mathcal{E}^K(Q_{E|W}|w^K)$, where $D(\cdot||\cdot|\cdot)$ is the conditional divergence defined in (10).

Now, define $T^{(K)}_W$ and $T^{(K)}_{E|W}(w^K)$ as follows:

$$T^{(K)}_W = \big\{w^K \in \mathcal{W}^K : |P_{w^K}(a) - P_W(a)| < \delta_K \text{ for all } a \in \mathcal{W} \text{ and } P_{w^K}(a) = 0 \text{ whenever } P_W(a) = 0\big\}, \tag{38}$$

$$T^{(K)}_{E|W}(w^K) = \big\{e^K \in \mathcal{E}^K : |P_{w^Ke^K}(a,b) - P_{w^K}(a)P_{E|W}(b|a)| < \delta_K \text{ for all } (a,b) \in \mathcal{W}\times\mathcal{E} \text{ and } P_{w^Ke^K}(a,b) = 0 \text{ whenever } P_{E|W}(b|a) = 0\big\}, \tag{39}$$

where $\{\delta_K\}_{K=1}^{\infty}$ is an arbitrary positive sequence satisfying $\delta_K \to 0$ and $\sqrt{K}\delta_K \to \infty$ as $K \to \infty$. It is known that $T^{(K)}_W$ and $T^{(K)}_{E|W}(w^K)$ satisfy

$$\lim_{K\to\infty} P_{W^K}\left\{W^K \in T^{(K)}_W\right\} = 1, \tag{40}$$

$$\lim_{K\to\infty} P_{E^K|W^K}\left\{E^K \in T^{(K)}_{E|W}(w^K) \;\middle|\; w^K\right\} = 1 \tag{41}$$

for an arbitrary $w^K \in \mathcal{W}^K$. By using (40) and (41), it is easy to prove that

$$\lim_{K\to\infty} P_{W^KE^K}\left\{(W^K,E^K) \in T^{(K)}\right\} = 1, \tag{42}$$

where $T^{(K)}$ is defined as

$$T^{(K)} = \big\{(w^K,e^K) \in \mathcal{W}^K\times\mathcal{E}^K : w^K \in T^{(K)}_W \text{ and } e^K \in T^{(K)}_{E|W}(w^K)\big\}. \tag{43}$$

In addition, it is important to notice that (30), (37) and the definition of $\{\delta_K\}_{K=1}^{\infty}$ lead to

$$P_{W^K}(w^K) = 2^{-KH(W)+o(K)}, \tag{44}$$

$$P_{E^K|W^K}(e^K|w^K) = 2^{-KH(E|W)+o(K)}, \tag{45}$$

for $w^K \in T^{(K)}_W$ and $(w^k,e^K) \in T^{(K)}$, respectively, where $H(E|W) = H(P_{E|W}|P_W)$.

4.2 Proof of Theorem 1

Theorem 1 is proved by using four lemmas that are shown in this subsection. While Lemmas 1–3 help evaluating $P^{(K)}_{error}$, Lemma 4 is used for evaluating $P^{(K)}_I$.

The decoding error probability $P^{(K)}_{error}$ in (5) is originally defined with respect to the joint probability distribution $P_{M^KE^K}$. Lemma 1 claims that $P_{W^KE^K}$ can also be used to express $P^{(K)}_{error}$ if $G_K \in \mathcal{G}_K$.

Lemma 1: Suppose that $\{G_K\}_{K=1}^{\infty} \in \mathcal{G}$ and let $(\mathcal{R}^{(K)}_0, \mathcal{R}^{(K)}_1)$ be the partition of $\mathcal{W}^K\times\mathcal{E}^K$ corresponding to G_K. Then,

$$P^{(K)}_{error} = P_{W^KE^K}\left\{(W^K,E^K) \in \mathcal{R}^{(K)}_1\right\} \tag{46}$$

for all $K \ge 1$.

Proof: Fix $K \ge 1$ and $G_K \in \mathcal{G}_K$ arbitrarily. It is sufficient for proving (46) to establish

$$P_{M^KE^K}\left\{(M^K,E^K) \in \mathcal{D}^{(K)}\right\} = P_{W^KE^K}\left\{(W^K,E^K) \in \mathcal{R}^{(K)}_0\right\}, \tag{47}$$

where

$$\mathcal{D}^{(K)} = \big\{(m^K,e^K) \in \mathcal{M}^K\times\mathcal{E}^K : G_K(F_K(m^K,e^K),e^K) = m^K\big\}.$$

For an arbitrarily fixed $e^K \in \mathcal{E}^K$ define $\mathcal{D}^{(K)}(e^K)$ and $\mathcal{R}^{(K)}_0(e^K)$ as follows:

$$\mathcal{D}^{(K)}(e^K) = \left\{m^K \in \mathcal{M}^K : (m^K,e^K) \in \mathcal{D}^{(K)}\right\}, \tag{48}$$

$$\mathcal{R}^{(K)}_0(e^K) = \left\{w^K \in \mathcal{W}^K : (w^K,e^K) \in \mathcal{R}^{(K)}_0\right\}. \tag{49}$$

It is important to note that $F_K(\cdot,e^K)$ is a bijective from $\mathcal{D}^{(K)}(e^K)$ to $\mathcal{R}^{(K)}_0(e^K)$. In fact, $F_K(\cdot,e^K)$ is clearly one-to-one from the definitions of f and F_K. On the other hand, for any $w^K \in \mathcal{R}^{(K)}_0(e^K)$ there exists $m^K \in \mathcal{M}^K$ such that $F_K(m^K,e^K) = w^K$ and $G_K(w^K,e^K) = m^K$. Such m^K satisfies $G_K(F_K(m^K,e^K),e^K) = m^K$ and therefore belongs to

$\mathcal{D}^{(K)}(e^K)$. This argument establishes the fact that $\mathcal{R}_0^{(K)}(e^K) \subseteq \{F_K(m^K, e^K) : m^K \in \mathcal{D}^{(K)}(e^K)\}$, which implies $F_K(\cdot, e^K)$ is onto.

Since for each $e^K \in \mathcal{E}^K$ $F_K(\cdot, e^K)$ is a bijective from $\mathcal{D}^{(K)}(e^K)$ to $\mathcal{R}_0^{(K)}(e^K)$, $w^K \in \mathcal{R}_0^{(K)}(e^K)$ is generated by the encoder only when $m^K \in \mathcal{D}^{(K)}(e^K)$ satisfying $F_K(m^K, e^K) = w^K$ is the source output. Accordingly,

$$P_{M^K}(m^K) = P_{W^K|E^K}(F_K(m^K, e^K)|e^K) \tag{50}$$

for all $m^K \in \mathcal{D}^{(K)}(e^K)$. Then, the left hand side of (47) is evaluated in the following way:

$$\begin{aligned}
&P_{M^K E^K}\left\{(M^K, E^K) \in \mathcal{D}^{(K)}\right\} \\
&\quad \overset{1)}{=} \sum_{(m^K, e^K) \in \mathcal{D}^{(K)}} P_{M^K}(m^K) P_{E^K}(e^K) \\
&\quad \overset{2)}{=} \sum_{e^K \in \mathcal{E}^K} P_{E^K}(e^K) \sum_{m^K \in \mathcal{D}^{(K)}(e^K)} P_{M^K}(m^K) \\
&\quad \overset{3)}{=} \sum_{e^K \in \mathcal{E}^K} P_{E^K}(e^K) \cdot \\
&\qquad \sum_{m^K \in \mathcal{D}^{(K)}(e^K)} P_{W^K|E^K}(F_K(m^K, e^K)|e^K) \\
&\quad \overset{4)}{=} \sum_{e^K \in \mathcal{E}^K} P_{E^K}(e^K) \sum_{w^K \in \mathcal{R}_0^{(K)}(e^K)} P_{W^K|E^K}(w^K|e^K) \\
&\quad \overset{5)}{=} P_{W^K E^K}\left\{(W^K, E^K) \in \mathcal{R}_0^{(K)}\right\},
\end{aligned} \tag{51}$$

where the marked equalities in (51) follow since

1): E^K is independent of M^K,
2): $\mathcal{D}^{(K)}(e^K)$ is defined by (48),
3): (50) holds for all $m^K \in \mathcal{D}^{(K)}(e^K)$,
4): $\{F_K(m^K, e^K) : m^K \in \mathcal{D}^{(K)}(e^K)\} = \mathcal{R}_0^{(K)}(e^K)$ for each $e^K \in \mathcal{E}^K$,
5): $\mathcal{R}_0^{(K)}(e^K)$ is defined by (49). □

The following two lemmas, Lemma 2 and Lemma 3, are used for evaluating $P_{error}^{(K)}$ caused by $\{G_K^*\}_{K=1}^{\infty}$. Though these two lemmas are obtained as consequences of the Sanov's lemma (see e.g. [10], [11]), proofs of the lemmas are given in Appendix in order to make this paper self-contained.

Lemma 2: Fix $\theta > 0$ arbitrarily and let $\mathcal{A}^{(K)}$ be the set defined by (7). Then,

$$P_{W^K}\left\{W^K \in \overline{\mathcal{A}^{(K)}}\right\} \le (K+1)^{|\mathcal{W}|} \cdot 2^{-K\theta} \tag{52}$$

for all $K \ge 1$, where $\overline{\mathcal{A}^{(K)}}$ denotes the complement of $\mathcal{A}^{(K)}$.

Lemma 3: Fix $\theta > 0$ arbitrarily and for any given $w^K \in \mathcal{W}^K$ let $\mathcal{B}^{(K)}(w^K)$ be the set defined by (8). Then,

$$\begin{aligned}
&P_{E^K|W^K}\left\{E^K \in \overline{\mathcal{B}^{(K)}(w^K)} \;\middle|\; w^K\right\} \\
&\qquad \le (K+1)^{|\mathcal{W}||\mathcal{E}|} \cdot 2^{-K\theta}
\end{aligned} \tag{53}$$

for all $K \ge 1$, where $\overline{\mathcal{B}^{(K)}(w^K)}$ denotes the complement of $\mathcal{B}^{(K)}(w^K)$.

The following lemma gives an upper bound of $P_I^{(K)}$. Hereafter, let $\mathcal{P}_{\mathcal{W}}$ be the set of all probability distributions on $\mathcal{W}$ and $\mathcal{P}_{\mathcal{E}|\mathcal{W}}$ be the set of all stochastic matrices from $\mathcal{W}$ to $\mathcal{E}$.

Lemma 4: Fix $\theta > 0$ arbitrarily. For a given $Q_W \in \mathcal{P}_{\mathcal{W}}$ define $\mathcal{A}_P$ and $\mathcal{B}_P(Q_W)$ as

$$\mathcal{A}_P = \{Q_W \in \mathcal{P}_{\mathcal{W}} : D(Q_W||P_W) < \theta\}, \tag{54}$$

$$\begin{aligned}
\mathcal{B}_P(Q_W) = \{&Q_{E|W} \in \mathcal{P}_{\mathcal{E}|\mathcal{W}} : \\
&D(Q_{E|W}||P_{E|W}|Q_W) < \theta\},
\end{aligned} \tag{55}$$

respectively. If $\hat{W}^K$ is decrypted by G_K^* in the secret-key authentication system given in Fig. 2, $P_I^{(K)}$ satisfies

$$\begin{aligned}
P_I^{(K)} \le (K+1)^{|\mathcal{W}||\mathcal{E}|} \cdot \exp_2\Big[-K \min_{Q_W \in \mathcal{A}_P} \\
\min_{Q_{E|W} \in \mathcal{B}_P(Q_W)} [I(Q_W; Q_{E|W}) + D(Q_E||P_E)]\Big]
\end{aligned} \tag{56}$$

for all $K \ge 1$, where for given $Q_W \in \mathcal{A}_P$ and $Q_{E|W} \in \mathcal{B}_P(Q_W)$ Q_E means the marginal probability distribution on $\mathcal{E}$ determined by

$$Q_E(e) = \sum_{w \in \mathcal{W}} Q_W(w) Q_{E|W}(e|w), \quad e \in \mathcal{E}.$$

Proof: Fix $K \ge 1$ arbitrarily. For all $({w'}^K, e^K) \in \mathcal{W}^K \times \mathcal{E}^K$ define $\tilde{\chi}_I({w'}^K, e^K)$ as

$$\tilde{\chi}_I({w'}^K, e^K) = \begin{cases} 1, & \text{if } {w'}^K \in \mathcal{A}^{(K)} \text{ and} \\ & \quad e^K \in \mathcal{B}^{(K)}({w'}^K), \\ 0, & \text{otherwise.} \end{cases} \tag{57}$$

When G_K^* is used, $\chi_I({w'}^K, e^K)$ in (3) equals one if all of (i) ${w'}^K \in \mathcal{A}^{(K)}$, (ii) $e^K \in \mathcal{B}^{(K)}({w'}^K)$ and (iii) $\lambda \notin \{g(w'_1, e_1), g(w'_2, e_2), \ldots, g(w'_K, e_K)\}$ are satisfied and zero otherwise. Therefore,

$$\chi_I({w'}^K, e^K) \le \tilde{\chi}_I({w'}^K, e^K) \tag{58}$$

for all $({w'}^K, e^K) \in \mathcal{W}^K \times \mathcal{E}^K$, which leads to

$$P_I^{(K)} \le \max_{{w'}^K \in \mathcal{W}^K} \sum_{e^K \in \mathcal{E}^K} P_{E^K}(e^K) \tilde{\chi}_I({w'}^K, e^K). \tag{59}$$

Note that $\tilde{\chi}_I({w'}^K, e^K) = 0$ for all $e^K \in \mathcal{E}^K$ if ${w'}^K \in \overline{\mathcal{A}^{(K)}}$. In addition, if ${w'}^K \in \mathcal{A}^{(K)}$, $\tilde{\chi}_I({w'}^K, e^K) = 0$ for all $e^K \in \overline{\mathcal{B}^{(K)}({w'}^K)}$. By using these facts, (59) can be bounded in the following form:

$$P_I^{(K)} \le \max_{{w'}^K \in \mathcal{A}^{(K)}} \sum_{e^K \in \mathcal{B}^{(K)}({w'}^K)} P_{E^K}(e^K) \tilde{\chi}_I({w'}^K, e^K)$$

$$= \max_{Q_W \in \mathcal{A}_T^{(K)}} \max_{w'^K \in \mathcal{W}^K(Q_W)} \sum_{Q_{E|W} \in \mathcal{B}_T^{(K)}(Q_W)} \sum_{e^K \in \mathcal{E}^K(Q_{E|W}|w'^K)} P_{E^K}(e^K)\tilde{\chi}_I(w'^K, e^K), \quad (60)$$

where $\mathcal{A}_T^{(K)}$ and $\mathcal{B}_T^{(K)}(Q_W)$ are the sets defined as

$$\mathcal{A}_T^{(K)} = \{Q_W \in \mathcal{T}_{\mathcal{W}}^{(K)} : D(Q_W||P_W) < \theta\}, \quad (61)$$

$$\mathcal{B}_T^{(K)}(Q_W) = \{Q_{E|W} \in \mathcal{T}_{\mathcal{E}|\mathcal{W}}^{(K)} : D(Q_{E|W}||P_{E|W}|Q_W) < \theta\}, \quad (62)$$

respectively.

Now, fix $Q_W \in \mathcal{A}_T^{(K)}$ and $w'^K \in \mathcal{W}^K(Q_W)$ arbitrarily. It is important to notice that $\tilde{\chi}_I(w'^K, e^K) = 1$ for all $Q_{E|W} \in \mathcal{B}_T^{(K)}(Q_W)$ and $e^K \in \mathcal{E}^K(Q_{E|W}|w'^K)$ from the definition of $\tilde{\chi}_I(w'^K, e^K)$ in (57). This fact enables to evaluate the right hand side of (60) as follows:

$$\begin{aligned} P_I^{(K)} &\overset{1)}{\le} \max_{Q_W \in \mathcal{A}_T^{(K)}} \max_{w'^K \in \mathcal{W}^K(Q_W)} \sum_{Q_{E|W} \in \mathcal{B}_T^{(K)}(Q_W)} |\mathcal{E}^K(Q_{E|W}|w'^K)| \cdot 2^{-K[H(Q_E)+D(Q_E||P_E)]} \\ &\overset{2)}{\le} \max_{Q_W \in \mathcal{A}_T^{(K)}} \max_{w'^K \in \mathcal{W}^K(Q_W)} \sum_{Q_{E|W} \in \mathcal{B}_T^{(K)}(Q_W)} 2^{KH(Q_{E|W}|Q_W)} \cdot 2^{-K[H(Q_E)+D(Q_E||P_E)]} \\ &\overset{3)}{=} \max_{Q_W \in \mathcal{A}_T^{(K)}} \sum_{Q_{E|W} \in \mathcal{B}_T^{(K)}(Q_W)} 2^{-K[I(Q_W;Q_{E|W})+D(Q_E||P_E)]}, \end{aligned} \quad (63)$$

where the marked equality and inequalities in (63) are established from

1): for any given $Q_W \in \mathcal{A}_T^{(K)}, w'^K \in \mathcal{W}^K(Q_W)$ and $Q_{E|W} \in \mathcal{B}_T^{(K)}(Q_W)$, $\tilde{\chi}_I(w'^K, e^K) = 1$ for all $e^K \in \mathcal{E}^K(Q_{E|W}|w'^K)$ and equality $P_{E^K}(e^K) = 2^{-K[H(Q_E)+D(Q_E||P_E)]}$ that is established in the same way as (30),
2): inequality (35),
3): $I(Q_W; Q_{E|W}) = H(Q_E) - H(Q_{E|W}|Q_W)$ and the sum no longer depends on $w'^K \in \mathcal{W}^K(Q_W)$.

Finally, the right hand side of (56) is obtained in the following way:

$$\begin{aligned} P_I^{(K)} &\overset{4)}{\le} \max_{Q_W \in \mathcal{A}_T^{(K)}} (K+1)^{|\mathcal{W}||\mathcal{E}|} \exp_2\Big[-K \min_{Q_{E|W} \in \mathcal{B}_T^{(K)}(Q_W)} [I(Q_W; Q_{E|W}) + D(Q_E||P_E)]\Big] \\ &\overset{5)}{\le} (K+1)^{|\mathcal{W}||\mathcal{E}|} \cdot \exp_2\Big[-K \min_{Q_W \in \mathcal{A}_P} \min_{Q_{E|W} \in \mathcal{B}_P(Q_W)} [I(Q_W; Q_{E|W}) + D(Q_E||P_E)]\Big], \end{aligned} \quad (64)$$

where the marked inequalities in (64) follow from

4): inequality (33),
5): $\mathcal{A}_T^{(K)} \subset \mathcal{A}_P$ and $\mathcal{B}_T^{(K)}(Q_W) \subset \mathcal{B}_P(Q_W)$. □

Proof of Theorem 1:
Theorem 1 has two claims. One is on $P_{error}^{(K)}$ and the other is on $P_I^{(K)}$. Firstly, the claim on $P_{error}^{(K)}$ in (12) is established. Fix $\varepsilon \in (0,1)$ arbitrarily and define θ as $\theta = K^{-\varepsilon}$. In case that $\hat{W}^K = W^K$ is decrypted by G_K^*, the decoding error occurs when $W^K \in \overline{\mathcal{A}^{(K)}}$ or $E^K \in \overline{\mathcal{B}^{(K)}(W^K)}$. It is clear that $\lambda \notin \{g(W_1, E_1), g(W_2, E_2), \ldots, g(W_K, E_K)\}$ from the definition of F_K. Therefore, by using Lemma 1 $P_{error}^{(K)}$ can be evaluated in the following form:

$$P_{error}^{(K)} \le P_{W^K}\left\{W^K \in \overline{\mathcal{A}^{(K)}}\right\} + \sum_{w^K \in \mathcal{A}^{(K)}} P_{W^K}(w^K) \cdot P_{E^K|W^K}\left\{E^K \in \overline{\mathcal{B}^{(K)}(w^K)} \mid w^K\right\}. \quad (65)$$

Lemma 2 implies that the first term in the right hand side of (65) can be bounded as follows:

$$P_{W^K}\left\{W^K \in \overline{\mathcal{A}^{(K)}}\right\} \le (K+1)^{|\mathcal{W}|} \cdot 2^{-K^{1-\varepsilon}}. \quad (66)$$

Moreover, Lemma 3 yields

$$\begin{aligned} &\sum_{w^K \in \mathcal{A}^{(K)}} P_{W^K}(w^K) P_{E^K|W^K}\left\{E^K \in \overline{\mathcal{B}^{(K)}(w^K)} \mid w^K\right\} \\ &\quad \le \sum_{w^K \in \mathcal{A}^{(K)}} P_{W^K}(w^K) \cdot (K+1)^{|\mathcal{W}||\mathcal{E}|} \cdot 2^{-K^{1-\varepsilon}} \\ &\quad \le (K+1)^{|\mathcal{W}||\mathcal{E}|} \cdot 2^{-K^{1-\varepsilon}}. \end{aligned} \quad (67)$$

Inequality (12) is obtained by combining (65) with (66) and (67).

Secondly, the claim on $P_I^{(K)}$ in (13) is developed. Lemma 4 is a key to the proof. Since $\theta = K^{-\varepsilon}$ is a monotone decreasing function of K, $\mathcal{A}_P$ and $\mathcal{B}_P(Q_W)$ shrink to the neighborhoods of P_W and $P_{E|W}$ as K increases, respectively. Therefore, for any $\delta \in (0, I(W;E))$, the continuities of the mutual information and the divergence guarantee the existence of an integer $K_0(\varepsilon, \delta)$ satisfying

$$\min_{Q_W \in \mathcal{A}_P} \min_{Q_{E|W} \in \mathcal{B}_P(Q_W)} [I(Q_W; Q_{E|W}) + D(Q_E||P_E)] + \frac{\log_2(K+1)^{|\mathcal{W}||\mathcal{E}|}}{K} \ge I(W;E) - \delta \quad (68)$$

for all integers $K > K_0(\varepsilon, \delta)$. Combining Lemma 4 with (68) yields (13). □

4.3 Proof of Theorem 2

Proof of Theorem 2:
Assume that there exists $\{G_K\}_{K=1}^{\infty} \in \mathcal{G}$ satisfying both (15) and

$$\limsup_{K\to\infty} -\frac{1}{K}\log_2 P_I^{(K)} > I(W;E). \tag{69}$$

We show that this assumption leads to a contradiction. Notice that inequality (69) means the existence of a $\delta > 0$ and a subsequence $\{K_j\}_{j=1}^{\infty}$ such that

$$-\frac{1}{K_j}\log_2 P_I^{(K_j)} \geq I(W;E) + \delta \text{ for all } j \geq 1 \tag{70}$$

and $K_j \to \infty$ as $j \to \infty$.

To this end, let $(\mathcal{R}_0^{(K)}, \mathcal{R}_1^{(K)})$, $K \geq 1$, be the partition of $\mathcal{W}^K \times \mathcal{E}^K$ corresponding to G_K. It is important to note that $P_{error}^{(K)}$ and $P_I^{(K)}$ can be expressed as follows, respectively:

$$P_{error}^{(K)} = P_{W^K E^K}\left\{(W^K, E^K) \in \mathcal{R}_1^{(K)}\right\}, \tag{71}$$

$$P_I^{(K)} = \max_{w'^K \in \mathcal{W}^K} P_{E^K}\left\{(w'^K, E^K) \in \mathcal{R}_0^{(K)}\right\}. \tag{72}$$

If the opponent generates $W'^K \in \mathcal{W}^K$ according to a probability distribution Q_{W^K} on $\mathcal{W}^K$ and injects W'^K into the public channel, G_K accept W'^K as legitimate with probability $\tilde{P}_I^{(K)}$ given by

$$\begin{aligned}\tilde{P}_I^{(K)} &= Q_{W^K} P_{E^K}\left\{(W'^K, E^K) \in \mathcal{R}_0^{(K)}\right\} \\ &= \sum_{w'^K \in \mathcal{W}^K} Q_{W^K}(w'^K) P_{E^K}\left\{(w'^K, E^K) \in \mathcal{R}_0^{(K)}\right\}.\end{aligned} \tag{73}$$

Clearly, (72) and (73) imply

$$\tilde{P}_I^{(K)} \leq P_I^{(K)} \tag{74}$$

for all $K \geq 1$ and $Q_{W^K} \in \mathcal{P}_{\mathcal{W}^K}$.

It is important to notice that, if the opponent injects W'^K generated according to Q_{W^K}, the decoder can be considered as a hypothesis tester with the null hypothesis H_0 and the alternative hypothesis H_1 defined as

$$H_0 : (\hat{W}^K, E^K) \sim P_{W^K E^K}, \tag{75}$$

$$H_1 : (\hat{W}^K, E^K) \sim Q_{W^K} P_{E^K}. \tag{76}$$

Here, K-tuple of cryptograms $\hat{W}^K$ received by the decoder is regarded as an input to the hypothesis tester. The hypothesis tester accepts H_0 when $(\hat{W}^K, E^K) \in \mathcal{R}_0^{(K)}$. Otherwise, it accepts H_1 though it has no knowledge on Q_{W^K}. Denote by α and β the probability of the type I error and the type II error of the hypothesis tester, respectively. Obviously from (71) and (73), $\alpha = P_{error}^{(K)}$ and $\beta = \tilde{P}_I^{(K)}$. It is known that for any $K \geq 1, Q_{W^K}$ and partition $(\mathcal{R}_0^{(K)}, \mathcal{R}_1^{(K)})$, the following inequality holds:

$$\begin{aligned}&\alpha\log_2\frac{\alpha}{1-\beta} + (1-\alpha)\log_2\frac{1-\alpha}{\beta} \\ &\quad\leq D(P_{W^K E^K}||Q_{W^K}P_{E^K})\end{aligned} \tag{77}$$

[11, Theorem 4.4.1], where $D(P_{W^K E^K}||Q_{W^K}P_{E^K})$ is the divergence between $P_{W^K E^K}$ and $Q_{W^K}P_{E^K}$ defined as

$$\begin{aligned}D(P_{W^K E^K}||Q_{W^K}P_{E^K}) = &\sum_{w^K \in \mathcal{W}^K}\sum_{e^K \in \mathcal{E}^K} \\ &\cdot P_{W^K E^K}(w^K, e^K)\log_2\frac{P_{W^K E^K}(w^K, e^K)}{Q_{W^K}(w^K)P_{E^K}(e^K)}.\end{aligned} \tag{78}$$

Moreover, the left hand side of (77) can be written as

$$\begin{aligned}&\alpha\log_2\frac{\alpha}{1-\beta} + (1-\alpha)\log_2\frac{1-\alpha}{\beta} \\ &\quad= -h(\alpha) + \alpha\log_2\frac{1}{1-\beta} + (1-\alpha)\log_2\frac{1}{\beta},\end{aligned} \tag{79}$$

where $h(\alpha) = -\alpha\log_2\alpha - (1-\alpha)\log_2(1-\alpha)$ denotes the binary entropy. By using $h(\alpha) \leq 1$ and $\alpha\log_2\frac{1}{1-\beta} \geq 0$ for all $\alpha \in (0,1)$ and $\beta \in (0,1)$ in (79), we obtain

$$-1 + (1-\alpha)\log_2\frac{1}{\beta} \leq D(P_{W^K E^K}||Q_{W^K}P_{E^K}). \tag{80}$$

Hereafter, we consider the case of $K = K_j$, $j \geq 1$. Since (70) and (74) mean

$$\beta = \tilde{P}_I^{(K_j)} \leq P_I^{(K_j)} \leq 2^{-K_j[I(W;E)+\delta]}, \tag{81}$$

(80) is evaluated as

$$\begin{aligned}&-1 + (1-\alpha)K_j[I(W;E)+\delta] \\ &\quad\leq D(P_{W^{K_j}E^{K_j}}||Q_{W^{K_j}}P_{E^{K_j}})\end{aligned} \tag{82}$$

for all $j \geq 1$. Note that the left hand side of (82) no longer depends on $Q_{W^{K_j}}$ and therefore the inequality (82) can be tightened as

$$\begin{aligned}&-1 + (1-\alpha)K_j[I(W;E)+\delta] \\ &\quad\leq \min_{Q_{W^{K_j}} \in \mathcal{P}_{\mathcal{W}^{K_j}}} D(P_{W^{K_j}E^{K_j}}||Q_{W^{K_j}}P_{E^{K_j}}),\end{aligned} \tag{83}$$

where $\mathcal{P}_{\mathcal{W}^{K_j}}$ denotes the set of all probability distributions on $\mathcal{W}^{K_j}$. By using well-known facts such as

$$\begin{aligned}&D(P_{W^{K_j}E^{K_j}}||Q_{W^{K_j}}P_{E^{K_j}}) \\ &\quad= I(W^{K_j};E^{K_j}) + D(P_{W^{K_j}}||Q_{W^{K_j}}),\end{aligned}$$

$D(P_{W^{K_j}}||Q_{W^{K_j}}) \geq 0$ and $D(P_{W^{K_j}}||Q_{W^{K_j}}) = 0$ if and only if $P_{W^{K_j}} = Q_{W^{K_j}}$, the right hand side of (83) is evaluated as $I(W^{K_j};E^{K_j}) = K_j I(W;E)$. Hence, (83) is equivalent to

$$-1 + (1-\alpha)K_j[I(W;E)+\delta] \leq K_j I(W;E), \tag{84}$$

which implies

$$\alpha = P_{error}^{(K_j)} \geq \frac{\delta - \frac{1}{K_j}}{I(W;E) + \delta} \tag{85}$$

for all $j \geq 1$. Since δ is a positive number satisfying (70) and $K_j \to \infty$ as $j \to \infty$, (85) claims that $P_{error}^{(K)}$ does not converge to zero as $K \to \infty$. Inequality (85) contradicts the assumption on $\{G_K\}_{K=1}^{\infty}$ that is assumed to satisfy both (15) and (69). □

4.4 Proofs of Theorem 3 and Theorem 4

Proof of Theorem 3:
Since (18) is proved in the same way as in the proof of Theorem 1, only (19) is proved here. For a decoder G_K^* $P_G^{(K)}$ can be expressed as follows:

$$\begin{aligned} P_G^{(K)} &= \sum_{w^K \in \mathcal{A}^{(K)}} P_{W^K}(w^K) \\ &\quad \cdot \max_{e^K \in \mathcal{B}^{(K)}(w^K)} P_{E^K|W^K}(e^K|w^K) \\ &= \sum_{Q_W \in \mathcal{A}_T^{(K)}} \sum_{w^K \in \mathcal{W}^K(Q_W)} P_{W^K}(w^K) \cdot \max_{Q_{E|W} \in \mathcal{B}_T^{(K)}(Q_W)} \\ &\quad \cdot \max_{e^K \in \mathcal{E}^K(Q_{E|W}|w^K)} P_{E^K|W^K}(e^K|w^K), \end{aligned} \tag{86}$$

where $\mathcal{A}_T^{(K)}$ and $\mathcal{B}_T^{(K)}(Q_W)$ are sets defined in (61) and (62), respectively. By using the properties of the types and the conditional types, $P_G^{(K)}$ is evaluated in the following way:

$$\begin{aligned} P_G^{(K)} &\overset{1)}{=} \sum_{Q_W \in \mathcal{A}_T^{(K)}} \sum_{w^K \in \mathcal{W}^K(Q_W)} P_{W^K}(w^K) \\ &\quad \cdot \max_{Q_{E|W} \in \mathcal{B}_T^{(K)}(Q_W)} 2^{-K[H(Q_{E|W}|Q_W) + D(Q_{E|W}||P_{E|W}|Q_W)]} \\ &\overset{2)}{=} \sum_{Q_W \in \mathcal{A}_T^{(K)}} |\mathcal{W}^K(Q_W)| \cdot 2^{-K[H(Q_W) + D(Q_W||P_W)]} \\ &\quad \cdot \max_{Q_{E|W} \in \mathcal{B}_T^{(K)}(Q_W)} 2^{-K[H(Q_{E|W}|Q_W) + D(Q_{E|W}||P_{E|W}|Q_W)]} \\ &\overset{3)}{\leq} \sum_{Q_W \in \mathcal{A}_T^{(K)}} 2^{-KD(Q_W||P_W)} \\ &\quad \cdot \max_{Q_{E|W} \in \mathcal{B}_T^{(K)}(Q_W)} 2^{-K[H(Q_{E|W}|Q_W) + D(Q_{E|W}||P_{E|W}|Q_W)]} \\ &\leq |\mathcal{A}_T^{(K)}| \cdot \max_{Q_W \in \mathcal{A}_T^{(K)}} 2^{-KD(Q_W||P_W)} \\ &\quad \cdot \max_{Q_{E|W} \in \mathcal{B}_T^{(K)}(Q_W)} 2^{-K[H(Q_{E|W}|Q_W) + D(Q_{E|W}||P_{E|W}|Q_W)]} \\ &\overset{4)}{\leq} (K+1)^{|\mathcal{W}|} \cdot \exp_2\Big[-K \min_{Q_W \in \mathcal{A}_T^{(K)}} \min_{Q_{E|W} \in \mathcal{B}_T^{(K)}(Q_W)} \\ &\quad \cdot [H(Q_{E|W}|Q_W) + D(Q_W||P_W) \\ &\quad + D(Q_{E|W}||P_{E|W}|Q_W)]\Big] \\ &\overset{5)}{\leq} (K+1)^{|\mathcal{W}|} \cdot \exp_2\Big[-K \min_{Q_W \in \mathcal{A}_P} \min_{Q_{E|W} \in \mathcal{B}_P(Q_W)} \\ &\quad \cdot [H(Q_{E|W}|Q_W) + D(Q_W||P_W) \\ &\quad + D(Q_{E|W}||P_{E|W}|Q_W)]\Big] \end{aligned} \tag{87}$$

where $\mathcal{A}_P$ and $\mathcal{B}_P(Q_W)$ are the sets defined in (54) and (55), respectively, and the marked equalities and inequalities in (87) are obtained since

1): for any $Q_W \in \mathcal{A}_T^{(K)}, w^K \in \mathcal{W}^K(Q_W)$ and $Q_{E|W} \in \mathcal{B}_T^{(K)}(Q_W)$, (37) holds for all $e^K \in \mathcal{E}^K(Q_{E|W}|w^K)$,
2): (30) holds for all $w^K \in \mathcal{W}^K(Q_W)$,
3): (28) holds for all $Q_W \in \mathcal{A}_T^{(K)}$,
4): $\mathcal{A}_T^{(K)} \subset \mathcal{T}_{\mathcal{W}}^{(K)}$ and (26) gives an upper bound of $|\mathcal{T}_{\mathcal{W}}^{(K)}|$,
5): $\mathcal{A}_T^{(K)} \subset \mathcal{A}_P$ and $\mathcal{B}_T^{(K)}(Q_W) \subset \mathcal{B}_P(Q_W)$.

Since $\theta = K^{-\varepsilon}$, $\mathcal{A}_P$ and $\mathcal{B}_P(Q_W)$ depend on K and shrink to the neighborhoods of P_W and $P_{E|W}$, respectively. The continuity of the conditional entropy, the divergence and the conditional divergence imply the existence of an integer $K_0(\varepsilon, \delta)$ satisfying

$$\begin{aligned} &\min_{Q_W \in \mathcal{A}_P} \min_{Q_{E|W} \in \mathcal{B}_P(Q_W)} [H(Q_{E|W}|Q_W) + D(Q_W||P_W) \\ &\qquad + D(Q_{E|W}||P_{E|W}|Q_W)] + \frac{\log_2(K+1)^{|\mathcal{W}|}}{K} \\ &\quad \geq H(E|W) - \delta \end{aligned} \tag{88}$$

for all $K \geq K_0$. The claim of Theorem 3 is obtained by combining (88) with (87). □

Proof of Theorem 4:
Consider a sequence of decoders $\{G_K\}_{K=1}^{\infty} \in \mathcal{G}$ satisfying (20). For each $K \geq 1$ let $(\mathcal{R}_0^{(K)}, \mathcal{R}_1^{(K)})$ be the partition of $\mathcal{W}^K \times \mathcal{E}^K$ corresponding to G_K. Then, Lemma 1 guarantees that (20) yields

$$P_{W^K E^K}\left\{(W^K, E^K) \in \mathcal{R}_0^{(K)}\right\} \to 1 \text{ as } K \to \infty. \tag{89}$$

Let $T^{(K)}$ be the set defined in (43). Since $T^{(K)}$ satisfies (42), combination of (89) and (42) gives rise to

$$P_{W^K E^K}\left\{(W^K, E^K) \in \mathcal{R}_0^{(K)} \cap T^{(K)}\right\} \to 1 \tag{90}$$

as $K \to \infty$. That is, (90) guarantees that for any $\eta \in (0,1)$ there exists an integer $K_1 = K_1(\eta)$ satisfying

$$\begin{aligned} &\sum_{w^K \in T_W^{(K)}} P_{W^K}(w^K) \\ &\quad \cdot \sum_{e^K \in \mathcal{R}_0^{(K)}(w^K) \cap T_{E|W}^{(K)}(w^K)} P_{E^K|W^K}(e^K|w^K) \geq 1 - \eta \end{aligned} \tag{91}$$

for all $K \geq K_1$, where $T_W^{(K)}$ and $T_{E|W}^{(K)}(w^K)$ are the sets defined in (38) and (39), respectively, and $\mathcal{R}_0^{(K)}(w^K)$ is defined as

$$\mathcal{R}_0^{(K)}(w^K) \stackrel{\text{def}}{=} \left\{ e^K \in \mathcal{E}^K \,:\, (w^K, e^K) \in \mathcal{R}_0^{(K)} \right\}.$$

Furthermore, the inner sum in (91) is supposed to be zero if $\mathcal{R}_0^{(K)}(w^K) \cap T_{E|W}^{(K)}(w^K) = \phi$ for $w^K \in T_W^{(K)}$.

It is important to note that (91) yields

$$\sum_{w^K \in \mathcal{U}^{(K)}} P_{W^K}(w^K) \geq 1 - \eta \text{ for all } K \geq K_1, \quad (92)$$

where

$$\mathcal{U}^{(K)} \stackrel{\text{def}}{=} \{ w^K \in T_W^{(K)} \,: \mathcal{R}_0^{(K)}(w^K) \cap T_{E|W}^{(K)}(w^K) \neq \phi \}. \quad (93)$$

A lower bound of $P_G^{(K)}$ is obtained in the following way:

$$\begin{aligned} P_G^{(K)} &\stackrel{1)}{=} \sum_{w^K \in \mathcal{W}^K} P_{W^K}(w^K) \cdot \max_{e^K \in \mathcal{R}_0^{(K)}(w^K)} P_{E^K|W^K}(e^K|w^K) \\ &\stackrel{2)}{\geq} \sum_{w^K \in \mathcal{U}^{(K)}} P_{W^K}(w^K) \cdot \max_{e^K \in \mathcal{R}_0^{(K)}(w^K)} P_{E^K|W^K}(e^K|w^K) \\ &\stackrel{3)}{\geq} \sum_{w^K \in \mathcal{U}^{(K)}} P_{W^K}(w^K) \cdot \max_{e^K \in \mathcal{R}_0^{(K)}(w^K) \cap T_{E|W}^{(K)}(w^K)} P_{E^K|W^K}(e^K|w^K), \end{aligned} \quad (94)$$

where the marked equality and inequalities in (94) follow from

1): the definition of $P_G^{(K)}$,
2): $\mathcal{U}^{(K)} \subset \mathcal{W}^K$,
3): $\mathcal{R}_0^{(K)}(w^K) \cap T_{E|W}^{(K)}(w^K) \subseteq \mathcal{R}_0^{(K)}(w^K)$ for all $w^K \in \mathcal{U}^{(K)}$.

Since (45) implies that

$$P_{E^K|W^K}(e^K|w^K) = 2^{-KH(E|W)+o(K)} \quad (95)$$

for all $w^K \in T_W^{(K)}$ and $e^K \in T_{E|W}^{(K)}(w^K)$, (94) yields

$$\begin{aligned} P_G^{(K)} &\geq \sum_{w^K \in \mathcal{U}^{(K)}} P_{W^K}(w^K) \cdot 2^{-KH(E|W)+o(K)} \\ &\geq (1-\eta) \cdot 2^{-KH(E|W)+o(K)} \end{aligned} \quad (96)$$

for all $K \geq K_1$, where the last inequality is obtained from (92). Inequality (96) implies that for any $\delta > 0$ there exists an integer $K_2 = K_2(\eta, \delta)$ satisfying

$$-\frac{1}{K} \log_2 P_G^{(K)} \leq H(E|W) + \delta \text{ for all } K \geq K_2, \quad (97)$$

which establishes (21). □

Acknowledgement

The authors are grateful to anonymous reviewers for careful reading of the paper and constructive comments especially on the proof of Theorem 2. This study is supported by Grant-in-Aid for Encouragement of Young Scientists from the Ministry of Education, Science, Sports and Culture of Japan (09750397).

References

[1] G.J. Simmons, "Authentication theory/coding theory," Advance of Cryptography—CRYPTO 84, Lecture Note in Computer Science, eds. G.R. Blakley and D. Chaum, vol.196, pp.411–431, Springer Verlag, 1985.
[2] R. Johannesson and A. Sgarro, "Strengthening Simmons' bound on impersonation," IEEE Trans. Inf. Theory, vol.37, no.4, pp.1182–1185, 1991.
[3] T. Johansson, "Lower bounds on the probability of deception in authentication with arbitration," IEEE Trans. Inf. Theory, vol.40, no.5, pp.1573–1585, 1994.
[4] B. Smeets, "Bounds on the probability of deception in multiple authentication," IEEE Trans. Inf. Theory, vol.40, no.5, pp.1586–1591, 1994.
[5] D.R. Stinson, "Some constructions and bounds for authentication codes," J. Cryptology, vol.1, pp.37–51, 1988.
[6] M. Jimbo and R. Fuji-hara, "Optimal authentication systems and combninatorial design," IEEE Trans. Inf. Theory, vol.36, no.1, pp.54–62, 1990.
[7] A. Sgarro, "A Shannon theoretic coding theorem in authentication theory," Eurocode '90, eds. G. Cohen and P. Charpin, pp.282–291, Springer-Verlag, 1991.
[8] U. Maurer, "A unified and generalized treatment of authentication theory," Proc. 13th Symposium on Theoretical Aspects of Computer Science, Lecture Notes in Computer Science, vol.1046, pp.387–398, Springer-Verlag, 1996.
[9] I. Csiszár and J. Körnor, Information Theory: Coding Theorem for Discrete Memoryless Systems, Academic Press, 1981.
[10] T.M. Cover and J.A. Thomas, Elements of Information Theory, Wiley, 1991.
[11] R.E. Blahut, Principles and Practice of Information Theory, Addison Wesley, 1987.

Appendix: Proofs of Lemma 2 and Lemma 3

Proof of Lemma 2:
Let $\mathcal{A}_T^{(K)}$ be the set defined in (61) and denote by $\overline{\mathcal{A}_T^{(K)}}$ the complement of $\mathcal{A}_T^{(K)}$. For an arbitrarily fixed $Q_W \in \overline{\mathcal{A}_T^{(K)}}$, the probability that W^K belongs to $\mathcal{W}^K(Q_W)$ is evaluated in the following way:

$$\begin{aligned} P_{W^K}\left\{W^K \in \mathcal{W}^K(Q_W)\right\} &= \sum_{w^K \in \mathcal{W}^K(Q_W)} P_{W^K}(w^K) \\ &\stackrel{1)}{=} |\mathcal{W}^K(Q_W)| \cdot 2^{-K[H(Q_W)+D(Q_W||P_W)]} \\ &\stackrel{2)}{\leq} 2^{-KD(Q_W||P_W)}, \end{aligned} \quad (\text{A}\cdot 1)$$

where the marked equality and inequality in (A·1) are

obtained since

1): equality (30) holds for all $w^K \in \mathcal{W}^K(Q_W)$,
2): inequality (28) holds for type Q_W.

Since $\overline{\mathcal{A}^{(K)}}$ is the union of $\mathcal{W}^K(Q_W)$ for $Q_W \in \overline{\mathcal{A}_T^{(K)}}$, the left hand side of (52) is bounded in the following manner:

$$\begin{aligned} P_{W^K}\left\{W^K \in \overline{\mathcal{A}^{(K)}}\right\} &\overset{3)}{\leq} \sum_{Q_W \in \overline{\mathcal{A}_T^{(K)}}} 2^{-KD(Q_W||P_W)} \\ &\overset{4)}{\leq} (K+1)^{|\mathcal{W}|} \cdot \exp_2\Big[-K \min_{Q_W \in \overline{\mathcal{A}_T^{(K)}}} D(Q_W||P_W)\Big] \\ &\overset{5)}{\leq} (K+1)^{|\mathcal{W}|} \cdot 2^{-K\theta}, \end{aligned} \tag{A·2}$$

where $\exp_2[t] = 2^t$ and the marked inequalities in (A·2) are obtained from

3): inequality (A·1),
4): inequality (26),
5): the definition of $\overline{\mathcal{A}_T^{(K)}}$. □

Proof of Lemma 3:
The proof of this lemma is essentially the same as the proof of Lemma 2. Fix $Q_W \in \mathcal{T}_{\mathcal{W}}^{(K)}$ and $w^K \in \mathcal{W}^K(Q_W)$ arbitrarily and define $\mathcal{B}_T^{(K)}(Q_W)$ by (62). Denote by $\overline{\mathcal{B}_T^{(K)}(Q_W)}$ the complement of $\mathcal{B}_T^{(K)}(Q_W)$. For any $Q_{E|W} \in \overline{\mathcal{B}_T^{(K)}(Q_W)}$ it is easy to check that

$$\begin{aligned} P_{E^K|W^K}\left\{E^K \in \mathcal{E}^K(Q_{E|W}|w^K) \;\middle|\; w^K\right\} &\overset{1)}{=} |\mathcal{E}^K(Q_{E|W}|w^K)| \\ &\quad \cdot 2^{-K[H(Q_{E|W}|Q_W)+D(Q_{E|W}||P_{E|W}|Q_W)]} \\ &\overset{2)}{\leq} 2^{-KD(Q_{E|W}||P_{E|W}|Q_W)}, \end{aligned} \tag{A·3}$$

where the marked equality and inequality in (A·3) are obtained since

1): equation (37) holds for all $e^K \in \mathcal{E}^K(Q_{E|W}|w^K)$,
2): inequality (35) holds for $Q_{E|W} \in \mathcal{T}_{\mathcal{E}|\mathcal{W}}^{(K)}$.

By combining

$$\overline{\mathcal{B}^{(K)}(w^K)} = \bigcup_{Q_{E|W} \in \overline{\mathcal{B}_T^{(K)}(Q_W)}} \mathcal{E}^K(Q_{E|W}|w^K)$$

with (A·3), the left hand side of (A·3) can be bounded in the following manner:

$$\begin{aligned} P_{E^K|W^K}\left\{E^K \in \overline{\mathcal{B}^{(K)}(w^K)} \;\middle|\; w^K\right\} &\overset{3)}{\leq} \sum_{Q_{E|W} \in \overline{\mathcal{B}_T^{(K)}(w^K)}} 2^{-KD(Q_{E|W}||P_{E|W}|Q_W)} \\ &\overset{4)}{\leq} (K+1)^{|\mathcal{W}||\mathcal{E}|} \\ &\quad \cdot \exp_2\Big[-K \min_{Q_{E|W} \in \overline{\mathcal{B}_T^{(K)}(Q_W)}} D(Q_{E|W}||P_{E|W}|Q_W)\Big] \\ &\overset{5)}{\leq} (K+1)^{|\mathcal{W}||\mathcal{E}|} \cdot 2^{-K\theta}, \end{aligned} \tag{A·4}$$

where the marked inequalities in (A·4) hold because of

3): inequality (A·3),
4): inequality (33),
5): the definition of $\overline{\mathcal{B}_T^{(K)}(Q_W)}$. □

Hiroki Koga was born in Fukuoka, Japan, on November 2, 1967. He received the B.E., M.E. and Dr.E. degrees from The University of Tokyo, Japan, in 1990, 1992 and 1995, respectively. He was an Assistant Professor at The University of Tokyo during 1995–1999. From April 1999 he is a lecturer at Institute of Engineering Mechanics and Systems, University of Tsukuba. His research interest includes the Shannon theory, data compression and information security.

Hirosuke Yamamoto was born in Wakayama, Japan, on November 15, 1952. He received the B.E. degree from Shizuoka University, Shizuoka, Japan, in 1975 and the M.E. and Dr.E. degrees from The University of Tokyo, Tokyo, Japan, in 1977 and 1980, respectively, all in electrical engineering. In 1980 he joined Tokushima University, Tokushima, Japan. He was an Associate Professor at Tokushima University, University of Electro-Communications, and The University of Tokyo, during 1983–1987, 1987–1993, and 1993–1999, respectively. Since March 1999, he is a professor in the Department of Mathematical Engineering and Information Physics, Graduate School of Engineering, The University of Tokyo. In 1989–1990, he was a Visiting Scholar at the Information Systems Laboratory, Stanford University. His research interests are in Shannon theory, coding theory, cryptology, and communication theory.