Coding Theorems for a $(2,2)$–Threshold Scheme with Detectability of Impersonation Attacks

Mitsugu Iwamoto, *Member, IEEE*, Hiroki Koga, *Member, IEEE*,
and Hirosuke Yamamoto, *Fellow, IEEE*

***Abstract*—Coding theorems on a $(2,2)$–threshold scheme with an opponent are discussed in an asymptotic setup, where the opponent tries to impersonate one of the two participants. A situation is considered where n secrets S^n from a memoryless source is blockwisely encoded to two shares and the two shares are decoded to S^n with permitting negligible decoding error. We introduce correlation level of the two shares and characterize the minimum attainable rates of the shares and a uniform random number for realizing a $(2,2)$–threshold scheme that is secure against the impersonation attack by the opponent. It is shown that, if the correlation level between the two shares equals to an $\ell \geq 0$, the minimum attainable rates coincide with $H(S)+\ell$, where $H(S)$ denotes the entropy of the source, and the maximum attainable exponent of the success probability of the impersonation attack equals to ℓ. It is also shown that a simple scheme using an ordinary $(2,2)$–threshold scheme attains all the bounds as well.**

***Index Terms*—Correlated sources, hypothesis testing, impersonation attack, secret sharing scheme, threshold scheme.**

I. Introduction

A. Background and Motivations

A secret sharing scheme [1], [2] is a well-known cryptographic technique that enables us to share a secret data among users. In (t,m)–threshold schemes, for example, a secret S is encoded to m *shares*, and the m shares are distributed to respective participants. Any t out of m participants can recover S, while $t-1$ or fewer participants cannot obtain any information on S in the sense of *unconditional security*.

In this paper, we focus on the secret sharing scheme in the presence of opponents. The objective of the opponents is cheating honest participants. That is, the opponents forge their shares and try to cheat the honest participants by injecting the forged shares in the recovery phase of S. This problem was firstly discussed by McEliece-Sarwate [3] and Karnin-Greene-Hellman [4] from the viewpoint of error-correcting codes. In particular, Karnin-Greene-Hellman [4] and Tompa-Woll [5] clarified that it is impossible to detect cheating in Shamir's secret sharing scheme [1]. In addition, a construction of a cheating-detectable secret sharing scheme is proposed in [5] as an extension of Shamir's secret sharing scheme although it is much inefficient. So far several schemes have been proposed to overcome such disadvantages [6]–[9]. In particular, Ogata-Kurosawa-Stinson [8] derived a lower bound on sizes of shares under a given maximum success probability ε of cheating and the lower bound is attained if and only if a difference set exists.

In cheating-detectable threshold schemes, the shares must satisfy unforgeablity as well as the ordinary requirements as a threshold scheme. We can actually consider two types of attacks, *impersonation attacks* and *substitution attacks*, similarly to the attacks against secret-key authentication systems [10]. In the impersonation attack, opponents intend to impersonate participants by injecting forged shares without using the legitimate shares. The impersonation attack is regarded as successful if the forged shares are accepted in a recovery phase of a secret. On the other hand, in the substitution attack, some of the participants are malicious and forge their shares by using their shares. The objective of the malicious participants is cheating honest participants who want to recover S from their shares.

For instance, Figure 1 shows the two types of attacks against a $(2,2)$–threshold scheme with two shares X and Y. We assume that the ordinary requirements as a $(2,2)$–threshold schemes, $H(S|X) = H(S|Y) = H(S)$ and $H(S|XY) = 0$, are satisfied. In Fig. 1(a) an opponent generates a forged share $\overline{X}$ without using X and Y and tries to impersonate participant 1 who have a share X. In Fig. 1(b) a participant with X forges $\overline{X}$ by using X, but not using Y. We assume that in both cases $\overline{X}$ is generated probabilistically. Then, it is important to notice that, $\overline{X}$ is independent of (X,Y) in Fig. 1(a), while Y, X and $\overline{X}$ form a Markov chain in this order in Fig. 1(b). Thus, considering the two types of attacks against threshold schemes corresponds to giving two kinds of probabilistic structures for all the shares including the forged share.

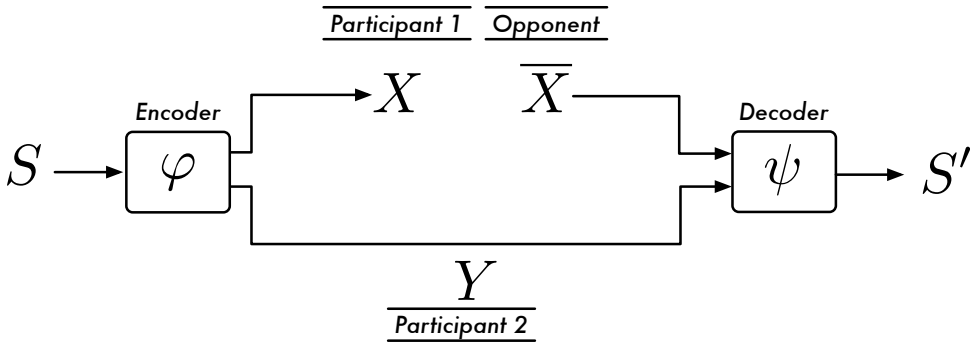
Cheating-detectable secret sharing schemes are usually designed to detect substitution attacks [5]–[9] in a non-asymptotic setup, i.e., the decoding error is not allowed and the block coding is not considered. These studies treat the case where a coalition of more than one malicious participants generates forged shares. However, there exist the following

This paper is presented in part at IEEE International Symposium on Information Theory 2009, and IEEE Information Theory Workshop 2009. The work of M. Iwamoto is partially supported by the MEXT Grant-in-Aid for Young Scientists (B) No. 20760236 and No. 23760330. The work of H. Koga is supported in part by Grant-in-Aid from the Telecommunications Advancement Foundation.

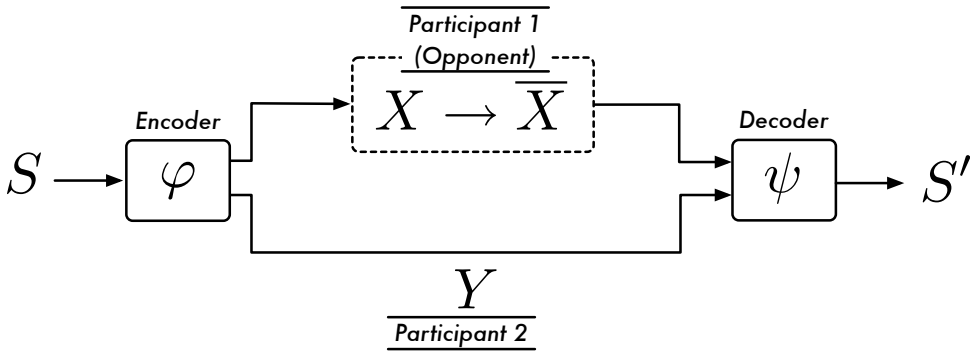
M. Iwamoto is with the Center of Frontier Science and Engineering, University of Electro-Communications, 1–5–1 Chofugaoka, Chofu-shi, Tokyo 182–8585, Japan (e-mail: mitsugu@inf.uec.ac.jp).

H. Koga is with Tsukuba University, 1–1–1, Tennoudai, Tsukuba-shi, 305–8577 Japan (e-mail: koga@iit.tsukuba.jp).

H. Yamamoto is with Graduate School of Frontier Sciences, University of Tokyo, 5–1–5 Kashiwanoha, Kashiwa-shi, Chiba 277–8561, Japan (e-mail: Hirosuke@ieee.org)



(a) A $(2,2)$–threshold scheme with an opponent who impersonates a participant who has a share X (impersonation attack)



(b) A $(2,2)$–threshold scheme with an opponent who substitutes a share $\overline{X}$ for X (substitution attack)

Fig. 1. Two $(2,2)$–threshold schemes with an opponent

drawbacks in cheating-detectable secret sharing schemes:

- According to [8], it is easy to derive the lower bounds of share rates, i.e., information bits per secret needed to describe shares, under a given success probability of cheating. Unfortunately, however, this result implies that the optimal share rates increase in order at least $1/\varepsilon$ as $\varepsilon \to 0$, and hence, an arbitrarily small success probability of cheating cannot be realized with fixed finite share rates.
- An extension of Shamir's (t,m)–threshold scheme in [5] can detect both substitution and impersonation attacks. This scheme is simple but inefficient from the viewpoint of share sizes. In addition, the optimal construction [8] is based on a combinatoric structure called a *difference set*, where the difference set exists only in limited cases and therefore restricts sizes of a secret and shares. Hence, even in a $(2,2)$–threshold scheme, we cannot apply the optimal scheme to a secret S of arbitrarily given size.
- Almost all constructions include the assumption that a secret is generated subject to a uniform probability distribution. This means that developing a near-optimum cheating-detectable secret sharing scheme for a secret subject to a non-uniform becomes another problem [9].

In this paper, we focus on the impersonation attack against a $(2,2)$–threshold scheme. Since the impersonation attack is weaker than the substitution attack, the impersonation attack is rarely discussed especially in the framework of secret sharing schemes. However, if we discuss the threshold scheme secure against impersonation attack in a certain asymptotic setup, we can unveil another information-theoretic aspect. In fact, we can find connections to hypothesis testing, authentication codes and Shannon's cipher system. In a practical point of view, we can consider a situation where impersonation attack seems to be valid. Suppose that in a $(2,2)$–threshold scheme one of the shares, say X, is a uniform random number that is independent of a secret S. In this case, the participants having X may generate $\overline{X}$ subject to a distribution close to the uniform distribution because analysis of X gives almost no information to the participant.

B. Contribution of This Study

In this paper, we formulate the problem of a threshold scheme secure against impersonation attacks in Shannon-theoretic asymptotic setup [11], [12], and unveil new features included in the problem. We consider a situation where n secrets that are generated from a discrete memoryless source are blockwisely encoded to two shares and the two shares are decoded to n secrets with permitting negligible decoding error. While we consider impersonation attacks, the asymptotic $(2,2)$–threshold scheme treated in this paper has the following features which resolve the three drawbacks pointed above in cheating-detectable secret sharing schemes:

- An exponentially small success probability of impersonation attack is realized under finite share rates if the blocklength is sufficiently large.

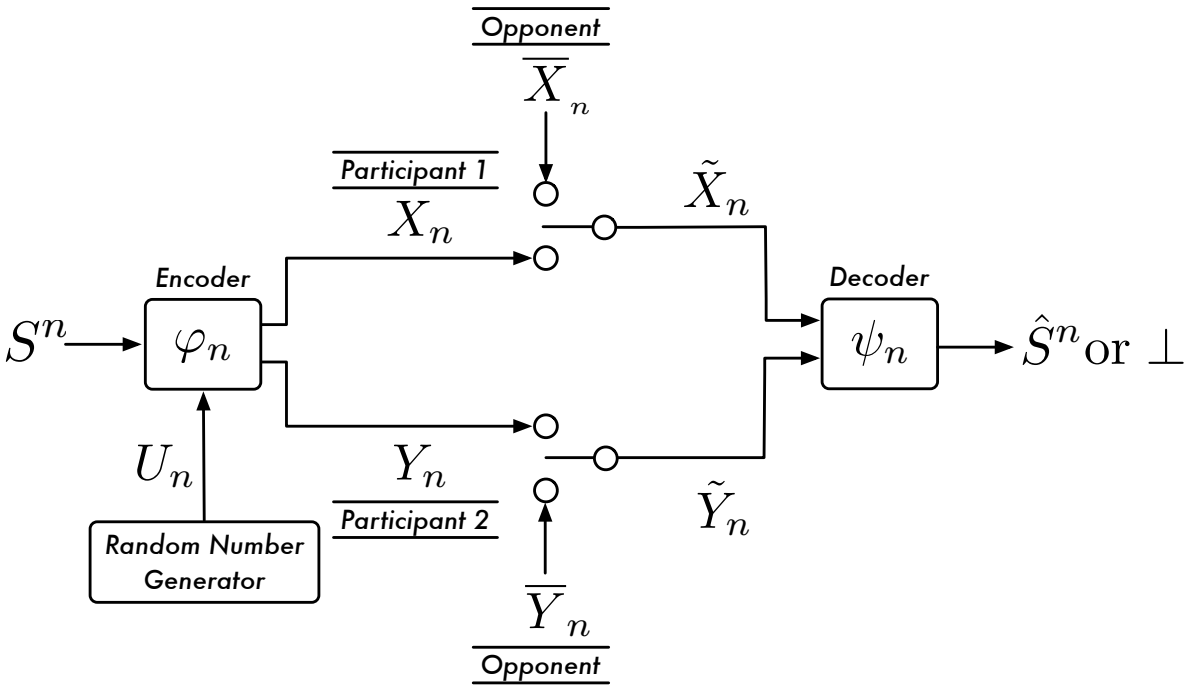


Fig. 2. A system model of $(2,2)$–threshold scheme with detectability of impersonation attacks

- The scheme uses no combinatoric structure and is applicable to arbitrary size of a secret.
- The probability distribution of a secret is arbitrary. In addition, the scheme can be applied to a more general class of sources.

Specifically, we give coding theorems on the $(2,2)$–threshold scheme for two cases of blockwise encoding and symbolwise encoding. In both cases we are interested in the minimum attainable rates for not only the two shares but also the uniform random number needed to a dealer for realizing a cheating-detectable $(2,2)$–threshold scheme in an asymptotic sense. We also evaluate the maximum attainable exponent of the success probability of the impersonation attack. It turns out that, if the two shares are correlated, we can easily realize the $(2,2)$–threshold scheme in an asymptotic sense that is secure against the impersonation attack. This fact motivates us to define a notion of *correlation level* of the two shares as the limit of the normalized mutual information between the two shares. In a non-asymptotic setup, we note that correlated shares are firstly discussed in [13] based on a combinatorial argument.

In the case of blockwise encoding, we consider an encoder that encodes n secrets $S^n = S_1S_2\cdots S_n$ blockwisely to two shares X_n and Y_n by using a uniform random number U_n, where throughout the paper the superscript n denotes the length and the subscripts n indicate dependency of n. The two shares X_n and Y_n are decoded to S^n with decoding error probability P_n^e that satisfies $P_n^e \to 0$ as $n \to \infty$. The two shares are required to satisfy the security criteria $I(S^n;X_n)/n \to 0$ and $I(S^n;Y_n)/n \to 0$ as $n \to \infty$, where $I(\,\cdot\,;\,\cdot\,)$ denotes the mutual information. We can prove that, if the correlation level of the shares is equal to ℓ, none of the rates of X_n, Y_n and U_n cannot be less than $H(S)+\ell$, where $H(S)$ denotes the entropy of the source, and the exponent of the success probability of impersonation attack cannot be greater than ℓ (*converse part*). Furthermore, we can prove the existence of a symbolwise of pairs of an encoder and a decoder that attains all the bounds shown in the converse part (*direct part*). Both claims of the direct and the converse parts are easily extended to the case where S^n is generated from a stationary ergodic source.

In the case of symbolwise encoding, we consider an encoder that encodes n secrets S^n to two shares $X^n = X_1X_2\cdots X_n$ and $Y^n = Y_1Y_2\cdots Y_n$ of length n by using n uniform random numbers $U^n = U_1U_2\cdots U_n$. In fact, X^n and Y^n are generated by $(X_i,Y_i) = f(S_i,U_i)$ for $i = 1,2,\ldots,n$, where f is an arbitrary deterministic encoder of an ordinary $(2,2)$–threshold scheme satisfying $H(S_i|X_i) = H(S_i|Y_i) = H(S_i)$ and $H(S_i|X_iY_i) = 0$. Denote by g a deterministic map satisfying $S_i = g(X_i,Y_i)$. We choose an appropriate f so that (X_i,Y_i), $i = 1,2,\ldots,n$, can be regarded as i.i.d. correlated random variables. It is shown that we can realize a $(2,2)$–threshold scheme in an asymptotic sense in which P_n^e vanishes as $n \to \infty$, X^n and Y^n satisfy a stronger requirement on the secrecy $I(S^n;X^n) = I(S^n;Y^n) = 0$ and the exponent of the success probability of the impersonation attack is optimal. In the proof we construct a decoder of X^n and Y^n by using g and a one-sided test for verifying the joint typicality of X^n and Y^n. This kind of symbolwise setup is first discussed in [14] for authentication code.

C. Related Works, Organization

The $(2,2)$–threshold scheme secure against the impersonation attack is motivated from the Shannon-theoretic authentication codes [10], [14]–[16]. In particular, in [14] the authors discuss the maximum attainable error exponent on the success probability of the impersonation attack subject to the vanishing decoding error probability. However, the results given in this paper is more involved. In fact, in the framework of $(2,2)$–threshold schemes we need to guarantee secrecy of a secret given one of the two shares. In addition, in this paper we succeeded in obtaining not only such a maximum exponent but also the minimum attainable sizes of the shares and the uniform random number.

The $(2,2)$–threshold scheme with detectability of impersonation attacks with the blockwise encoder can be viewed as one version of Shannon's cipher system ([17]–[21] etc.) when one of the shares is an output from a random number generator. In a simple asymptotic setup of Shannon's cipher system [20], n plaintexts S^n generated from a memoryless source are encrypted to a cryptogram W_n under a key U_n and W_n is decrypted to S^n under the same key U_n with permitting decoding error probability P_n^e. The encoder and the decoder are required to satisfy $P_n^e \to 0$ and $I(S^n;W_n)/n \to 0$ as $n \to \infty$. In this setup, the minimum attainable rates of the cryptogram and the key coincide with the entropy $H(S)$ of the plaintext. The coding theorems given in this paper imply the same result under an additional requirement such that the correlation level of W_n and U_n is equal to zero, i.e., $\ell = 0$.

The $(2,2)$–threshold scheme with detectability of impersonation attacks with the symbolwise encoder is related to the problem of secret key agreement [21], [22]. In the secret key agreement problem of the source type model [22], two users have n outputs $X^n = X_1X_2\cdots X_n \in \mathcal{X}^n$ and $Y^n = Y_1Y_2\cdots Y_n \in \mathcal{Y}^n$ from two correlated memoryless source, respectively, where (X_i,Y_i), $i = 1,2,\ldots,n$ are i.i.d. copies of $(X,Y) \in \mathcal{X}\times\mathcal{Y}$ subject to a joint probability distribution P_{XY}. The two user try to share a nearly uniform random number with the maximum rate $I(X;Y)$ by public communications. On the contrary, the symbolwise encoder in the $(2,2)$–threshold scheme with detectability of impersonation attacks can be interpreted as a generator of correlated random variables $X^n = X_1X_2\cdots X_n \in \mathcal{X}^n$ and $Y^n = Y_1Y_2\cdots Y_n \in \mathcal{Y}^n$ given independent random variables S^n and U^n, where (X_i,Y_i), $i = 1,2,\ldots,n$, are regarded as n i.i.d. copies of $(X,Y) \sim P_{XY}$. Since the correlation level X^n and Y^n coincides with $I(X;Y)$, the minimum attainable rate of U^n turns out to be $H(S)+I(X;Y)$. That is, we need an extra cost of $I(X;Y)$ in order to generate correlated two shares.

The rest of this paper is organized as follows: In Section II, a $(2,2)$–threshold scheme with detectability of impersonation attacks with correlation level ℓ in an asymptotic setup is formulated. The coding theorems for the blockwise encoder are given in Section III. Section IV is devoted to the proofs of the coding theorems. A construction of encoders and decoders based on a non-asymptotic $(2,2)$–threshold scheme and its optimality are discussed in Section V.

II. Problem Setting

We consider a $(2,2)$–threshold scheme depicted in Fig. 2. Assume for an integer $n \geq 1$ that a source generates an n–tuple of secrets $S^n = S_1S_2\cdots S_n$ independently subject to a probability distribution P_S on a finite set $\mathcal{S}$. Denote by P_{S^n} the probability distribution of S^n induced by P_S, and let $P_{S^n}(s^n)$ be the probability that $S^n = s^n$ for an $s^n \in \mathcal{S}^n$. Since the source is memoryless, it holds that $P_{S^n}(s^n) = \prod_{i=1}^n P_S(s_i)$ for all $n \geq 1$ where $s^n = s_1s_2\cdots s_n$.

In Fig. 2, let U_n be the random variable subject to the uniform distribution on a finite set $\mathcal{U}_n$. Assume that U_n is independent of S^n. In this paper, we use the subscript n to indicate dependency of n, while the superscript n implies the length. We denote by P_{U_n} a probability distribution of U_n, i.e., it holds that $P_{U_n}(u_n) = 1/|\mathcal{U}_n|$ for all $u_n \in \mathcal{U}_n$ where $|\cdot|$ denotes the cardinality.

An encoder is defined as a deterministic map $\varphi_n : \mathcal{S}^n \times \mathcal{U}_n \to \mathcal{X}_n \times \mathcal{Y}_n$, where $\mathcal{X}_n$ and $\mathcal{Y}_n$ are finite sets in which shares X_n and Y_n take values, respectively. Hence, we can write

$$(X_n, Y_n) = \varphi_n(S^n, U_n) \tag{1}$$

from which we can see that X_n and Y_n are also random variables. The joint probability distribution $P_{X_nY_n}$ of X_n and Y_n is induced from (1). The shares X_n and Y_n are distributed securely to participants 1 and 2, respectively.

Next, consider a situation where an opponent may impersonate one of the two participants. When the opponent impersonates participant 1, the opponent behaves as if he/she were a participant 1 by injecting a forged share $\overline{X}_n \in \mathcal{X}_n$ instead of X_n. This attack is regarded as successful if a decoder fails to detect impersonation attacks and outputs an element of $\mathcal{S}^n$ from $\overline{X}_n$ and Y_n. Here, we assume that the opponent generates $\overline{X}_n$ *without using* X_n. According to [10], [14]–[16], such attack is called *impersonation attack* as opposed to substitution attack. Similarly, in the case of deceiving participant 1, the opponent forges a share $\overline{Y}_n$ without using Y_n, and tries to impersonate participant 2. In this case, the attack succeeds when the decoder outputs an element of $\mathcal{S}^n$ from X_n and $\overline{Y}_n$. Summarizing, letting $\tilde{X}_n$ and $\tilde{Y}_n$ be the inputs to a decoder, the following three cases must be considered:

- (a0) $(\tilde{X}_n, \tilde{Y}_n) = (X_n, Y_n)$
- (a1) $(\tilde{X}_n, \tilde{Y}_n) = (\overline{X}_n, Y_n)$
- (a2) $(\tilde{X}_n, \tilde{Y}_n) = (X_n, \overline{Y}_n)$

A decoder is defined as a deterministic map $\psi_n : \mathcal{X}_n \times \mathcal{Y}_n \to \mathcal{S}^n \cup \{\perp\}$, where $\perp$ is a symbol to declare the detection of an impersonated attack, i.e., (a1) or (a2). We note here that the decoder cannot know in advance which one of (a0)–(a2) actually occurs. On the other hand, we assume that the opponent knows everything about the encoder and the decoder except for realizations of S^n, U_n, X_n and Y_n.

In this situation, we define success probabilities of impersonation attacks. Let $\mathcal{A}_n \subset \mathcal{X}_n \times \mathcal{Y}_n$ be the region that the decoder ψ_n accepts the pair of shares $(\tilde{X}_n, \tilde{Y}_n)$ and outputs an element of $\mathcal{S}^n$, i.e.,

$$\mathcal{A}_n = \{(x_n, y_n) \in \mathcal{X}_n \times \mathcal{Y}_n : \psi_n(x_n, y_n) \in \mathcal{S}^n\}. \tag{2}$$

Now, recall that the impersonation attack succeeds if the decoder outputs an element of $\mathcal{S}^n$ when one of (a1) and (a2) occurs. In the case of (a1), i.e., the opponent impersonates participant 1, we note that he/she generates a forged share $\overline{X}_n$ according to a probability distribution $P_{\overline{X}_n}$ independently from S^n, U_n, X_n, and Y_n. In addition, the opponent tries to optimize $P_{\overline{X}_n}$ so that $(\overline{X}_n, Y_n)$ can be accepted by the decoder with the maximum probability. This motivates us to define a success probability to impersonate participant 1 by

$$P_n^X = \max_{P_{\overline{X}_n}} \Pr\{(\overline{X}_n, Y_n) \in \mathcal{A}_n\} \tag{3}$$

where the maximization of $P_{\overline{X}_n}$ is taken over all probability distributions on $\mathcal{X}_n$, and $\Pr\{\cdot\}$ means the probability with respect to the (joint) probability distribution of random variable(s) between the parentheses, i.e., $(\overline{X}_n, Y_n) \sim P_{\overline{X}_n Y_n} = P_{\overline{X}_n} P_{Y_n}$ in this case. Similarly, the maximum success probability for the impersonation to participant 2 can be defined as

$$P_n^Y = \max_{P_{\overline{Y}_n}} \Pr\{(X_n, \overline{Y}_n) \in \mathcal{A}_n\} \tag{4}$$

where $\Pr\{\cdot\}$ is taken with respect to $(X_n, \overline{Y}_n) \sim P_{X_n \overline{Y}_n} = P_{X_n} P_{\overline{Y}_n}$.

The decoding error occurs when S^n is not correctly decoded from legitimate shares in the case of (a0). Hence, the decoding error probability can be written as

$$P_n^e = \Pr\{\psi_n(\varphi_n(S^n, U_n)) \neq S^n\}. \tag{5}$$

It is easy to see that if $(x_n, y_n) \notin \mathcal{A}_n$, then $\psi_n(x_n, y_n) = \perp \notin \mathcal{S}^n$. Hence, we have

$$P_n^e \geq \Pr\{(X_n, Y_n) \notin \mathcal{A}_n\} \tag{6}$$

for any pair of an encoder φ_n and a decoder ψ_n.

Now, we can define a $(2,2)$–threshold scheme in an asymptotic setup as follows:

Definition 1: We say that a sequence $\{(\varphi_n, \psi_n)\}_{n=1}^\infty$ of an encoder φ_n and a decoder ψ_n asymptotically realizes a $(2,2)$–threshold scheme if it satisfies

$$\lim_{n\to\infty} P_n^e = 0 \tag{7}$$

and

$$\lim_{n\to\infty} \frac{1}{n} I(S^n; X_n) = \lim_{n\to\infty} \frac{1}{n} I(S^n; Y_n) = 0 \tag{8}$$

where $I(\cdot;\cdot)$ denotes the mutual information.

The condition (7) guarantees that the decoding error probability is negligible if the blocklength n is sufficiently large. Note that Fano's inequality [23, Theorem 2.10.1] tells us that

$$\frac{1}{n} H(S^n | X_n Y_n) \leq \frac{1}{n} h(P_n^e) + P_n^e \log |\mathcal{S}| \tag{9}$$

where $\log(\cdot) = \log_2(\cdot)$ throughout the paper, and $H(\cdot|\cdot)$ and $h(\cdot)$ are the conditional and the binary entropies, respectively. Hence, if (7) is satisfied, then we have

$$\lim_{n\to\infty} \frac{1}{n} H(S^n | X_n Y_n) = 0 \tag{10}$$

due to the non-negativity of the conditional entropy. On the other hand, the condition (8) ensures that S^n is secure against the leakage from one of X_n and Y_n if n is sufficiently large. That is, S^n and either one of the shares are almost independent under such a condition. We also note that, since S^n is generated from a memoryless source, (8) implies that

$$\lim_{n\to\infty} \frac{1}{n} H(S^n | X_n) = \lim_{n\to\infty} \frac{1}{n} H(S^n | Y_n) = H(S) \tag{11}$$

where $H(\cdot)$ denotes the entropy.

We conclude this section with introducing a notion of *correlation level*. The mutual information of two shares plays a crucial role in detecting impersonation attacks, which will be clarified in the following sections.

Definition 2: Let $\{(X_n, Y_n)\}_{n=1}^\infty$ be a pair of shares generated by a sequence of encoders $\{\varphi_n\}_{n=1}^\infty$. Then, a non-negative number ℓ is said to be a correlation level of $\{(X_n, Y_n)\}_{n=0}^\infty$ if it holds that

$$\lim_{n\to\infty} \frac{1}{n} I(X_n; Y_n) = \ell. \tag{12}$$

In particular, if a sequence $\{(\varphi_n, \psi_n)\}_{n=1}^\infty$ of an encoder φ_n and a decoder ψ_n satisfies Definition 1 and the sequence of shares $\{(X_n, Y_n)\}_{n=0}^\infty$ generated from $\{\varphi_n\}_{n=1}^\infty$ satisfies (12), we say that $\{(\varphi_n, \psi_n)\}_{n=1}^\infty$ asymptotically realizes a $(2,2)$–threshold scheme with correlation level ℓ.

Remark 1: Note that the sequence $\{I(X_n; Y_n)/n\}_{n=1}^\infty$ in (12) does not have a limit in general if $\{(X_n, Y_n)\}_{n=1}^\infty$ is generated by an arbitrary sequence of encoders $\{\varphi_n\}_{n=1}^\infty$. Hence, (12) actually requires the existence of the limit for the sequence $\{I(X_n; Y_n)/n\}_{n=1}^\infty$, and the limit equals to ℓ.

III. Coding Theorems for a $(2,2)$–Threshold Scheme with Detectability of Impersonation Attacks

In this section, we give coding theorems for $\{(\varphi_n, \psi_n)\}_{n=1}^\infty$ that asymptotically realizes a $(2,2)$–threshold scheme with correlation level ℓ. We are interested in not only the rates of X_n, Y_n and U_n but also the exponents of P_n^X and P_n^Y of the sequence $\{(\varphi_n, \psi_n)\}_{n=1}^\infty$. The following theorem is the converse part of the coding theorem with respect to such rates and exponents.

Theorem 1: For any sequence $\{(\varphi_n, \psi_n)\}_{n=1}^\infty$ of an encoder φ_n and a decoder ψ_n that asymptotically realizes a $(2,2)$–threshold scheme with correlation level ℓ, it holds that

$$\liminf_{n\to\infty} \frac{1}{n} \log |\mathcal{X}_n| \geq H(S) + \ell \tag{13}$$

$$\liminf_{n\to\infty} \frac{1}{n} \log |\mathcal{Y}_n| \geq H(S) + \ell \tag{14}$$

$$\liminf_{n\to\infty} \frac{1}{n} \log |\mathcal{U}_n| \geq H(S) + \ell \tag{15}$$

and

$$\limsup_{n\to\infty} \max\left\{ -\frac{1}{n} \log P_n^X, -\frac{1}{n} \log P_n^Y \right\} \leq \ell. \tag{16}$$

Theorem 1 is proved in Section IV-A. Theorem 1 tells us that for an arbitrarily small $\gamma > 0$ the rates of X_n, Y_n and U_n cannot be less than $H(S) + \ell - \gamma$ for all sufficiently large n, where ℓ is an arbitrarily given correlation level. In fact, by noticing that $H(S) + \ell \geq H(S)$ for any $\ell \geq 0$, the bounds on the right hand sides of (13)–(15) coincide with the bounds in [12, Theorem 1] for $(2, 2)$–threshold schemes when $\ell = 0$. Theorem 1 also indicates that the correlation level of shares is an upper bound on the exponents of P_n^X and P_n^Y.

The direct part of the coding theorem corresponding to Theorem 1 is as follows:

Theorem 2: For an arbitrarily given non-negative number $\ell \geq 0$, there exists a sequence $\{(\varphi_n^*, \psi_n^*)\}_{n=1}^{\infty}$ of an encoder φ_n^* and a decoder ψ_n^* that asymptotically realizes a $(2, 2)$–threshold scheme with correlation level ℓ satisfying

$$\limsup_{n\to\infty} \frac{1}{n} \log |\mathcal{X}_n| \leq H(S) + \ell \tag{17}$$

$$\limsup_{n\to\infty} \frac{1}{n} \log |\mathcal{Y}_n| \leq H(S) + \ell \tag{18}$$

$$\limsup_{n\to\infty} \frac{1}{n} \log |\mathcal{U}_n| \leq H(S) + \ell \tag{19}$$

and

$$\liminf_{n\to\infty} \min \left\{ -\frac{1}{n} \log P_n^X, -\frac{1}{n} \log P_n^Y \right\} \geq \ell. \tag{20}$$

In particular, the above $\{(\varphi_n^*, \psi_n^*)\}_{n=1}^{\infty}$ also satisfies

$$I(S^n; X_n) = I(S^n; Y_n) = 0 \quad \text{for all} \quad n \geq 1 \tag{21}$$

which is stronger than the condition in (8).

The proof of Theorem 2 is given in Section IV-B.

Remark 2: Theorem 1 guarantees that $\{(\varphi_n^*, \psi_n^*)\}_{n=1}^{\infty}$ in Theorem 2 attains the minimum rates of X_n, Y_n, and U_n, and the maximum exponents of P_n^X and P_n^Y. Furthermore, the limits exist for these rates and exponents, i.e., it holds that

$$\begin{aligned} \lim_{n\to\infty} \frac{1}{n} \log |\mathcal{X}_n| = \lim_{n\to\infty} \frac{1}{n} \log |\mathcal{Y}_n| = \lim_{n\to\infty} \frac{1}{n} \log |\mathcal{U}_n| \\ = H(S) + \ell \end{aligned} \tag{22}$$

and

$$\lim_{n\to\infty} -\frac{1}{n} \log P_n^X = \lim_{n\to\infty} -\frac{1}{n} \log P_n^Y = \ell. \tag{23}$$

IV. Proofs of Theorems 1 and 2

This section is devoted to the proofs of Theorems 1 and 2. In the proof of Theorem 1, we use a relationship between hypothesis testing and the $(2, 2)$–threshold scheme with detectability of impersonation attacks with correlation level ℓ, which originates from [16] and developed by [14], [15].

A. Proof of Theorem 1

Fix $\ell \geq 0$ arbitrarily. We first prove (13). From the basic properties of the entropy and the mutual information, it holds that

$$\begin{aligned} H(X_n) &= I(X_n; Y_n) + H(X_n|Y_n) \\ &\geq I(X_n; Y_n) + H(X_n|Y_n) - H(X_n|Y_n S^n) \\ &= I(X_n; Y_n) + I(X_n; S^n|Y_n) \\ &= I(X_n; Y_n) + H(S^n|Y_n) - H(S^n|X_n Y_n). \end{aligned} \tag{24}$$

Hence, (13) is established because

$$\begin{aligned} \liminf_{n\to\infty} \frac{1}{n} \log |\mathcal{X}_n| &\geq \liminf_{n\to\infty} \frac{1}{n} H(X_n) \\ &\geq \liminf_{n\to\infty} \frac{1}{n} I(X_n; Y_n) \\ &\quad + \liminf_{n\to\infty} \frac{1}{n} H(S^n|Y_n) \\ &\quad - \limsup_{n\to\infty} \frac{1}{n} H(S^n|X_n Y_n) \\ &= \ell + H(S) \end{aligned} \tag{25}$$

where the last inequality and the equality are due to (24) and (10)–(12), respectively. We can establish (14) in essentially the same way.

Next, we prove (15). Since the encoder φ_n is deterministic for each $n \geq 1$, we have

$$\begin{aligned} H(X_n Y_n) &\leq H(S^n U_n) \\ &= nH(S) + H(U_n) \end{aligned} \tag{26}$$

for all $n \geq 1$, where the equality follows because S^n is independent of U_n and is generated from a memoryless source. On the other hand, recalling that

$$H(X_n Y_n) = H(X_n) + H(Y_n) - I(X_n; Y_n) \tag{27}$$

it follows from (26) and (27) that

$$\begin{aligned} \frac{1}{n} \log |\mathcal{U}_n| &= \frac{1}{n} H(U_n) \\ &= \frac{1}{n} H(X_n Y_n) - H(S) \\ &\geq \frac{1}{n} \{H(X_n) + H(Y_n) - I(X_n; Y_n)\} - H(S) \\ &\qquad \text{for all} \quad n \geq 1 \end{aligned} \tag{28}$$

where the first equality follows from the uniformity of $U_n \in \mathcal{U}_n$. Therefore, we have

$$\begin{aligned} \liminf_{n\to\infty} \frac{1}{n} \log |\mathcal{U}_n| &\geq \liminf_{n\to\infty} \frac{1}{n} H(X_n) + \liminf_{n\to\infty} \frac{1}{n} H(Y_n) \\ &\quad - \limsup_{n\to\infty} \frac{1}{n} I(X_n; Y_n) - H(S) \\ &\geq H(S) + \ell \end{aligned} \tag{29}$$

where the last inequality follows from (12) and (25). Note that we have $\liminf_{n\to\infty} H(Y_n) \geq H(S) + \ell$ in the same way as (25).

To prove (16), we use the fact that the decoding error probability and the success probabilities of impersonation attack in a $(2, 2)$–threshold scheme with correlation level ℓ are closely related to the error probabilities of the first kind

and the second kind in hypothesis testing, respectively, which is pointed out in [14]–[16]. Let us consider a simple hypothesis test with the following two hypotheses:

$$H_0 : (\tilde{X}_n, \tilde{Y}_n) \sim P_{X_nY_n} \tag{30}$$
$$H_1 : (\tilde{X}_n, \tilde{Y}_n) \sim P_{X_n}P_{Y_n}. \tag{31}$$

Let $\mathcal{A}_n \subset \mathcal{X}_n \times \mathcal{Y}_n$ denote an acceptance region for the null hypothesis H_0. Then, the error probability of the first kind and the error probability of the second kind of the above hypothesis testing are given by

$$\alpha_n \stackrel{\text{def}}{=} \sum_{(x_n,y_n)\in\mathcal{A}_n^c} P_{X_nY_n}(x_n, y_n) = \Pr\{(X_n, Y_n) \notin \mathcal{A}_n\} \tag{32}$$

$$\beta_n \stackrel{\text{def}}{=} \sum_{(x_n,y_n)\in\mathcal{A}_n} P_{X_n}(x_n)P_{Y_n}(y_n) \tag{33}$$

where $\mathcal{A}_n^c$ denotes the complement set of $\mathcal{A}_n$. It is easy to see from (6) that $P_n^e \geq \alpha_n$ holds for any $n \geq 1$. Hence, in view of (7), we have

$$\lim_{n\to\infty} \alpha_n = 0. \tag{34}$$

Furthermore, it follows from (3) that

$$\begin{aligned} P_n^X &= \max_{P_{\overline{X}_n}} \Pr\{(\overline{X}_n, Y_n) \in \mathcal{A}_n\} \\ &= \max_{P_{\overline{X}_n}} \sum_{(x_n,y_n)\in\mathcal{A}_n} P_{\overline{X}_n}(x_n)P_{Y_n}(y_n) \\ &\geq \beta_n. \end{aligned} \tag{35}$$

Similarly, we also have $P_n^Y \geq \beta_n$. Therefore, it holds that

$$-\frac{1}{n}\log\beta_n \geq \max\left\{-\frac{1}{n}\log P_n^X, -\frac{1}{n}\log P_n^Y\right\} \quad \text{for all} \quad n \geq 1. \tag{36}$$

According to [24, Theorem 4.4.1] and [14, Theorem 2], we have

$$\begin{aligned} I(X_n;Y_n) &= \sum_{\substack{(x_n,y_n)\\ \in\mathcal{X}_n\times\mathcal{Y}_n}} P_{X_nY_n}(x_n, y_n)\log\frac{P_{X_nY_n}(x_n,y_n)}{P_{X_n}(y_n)P_{Y_n}(y_n)} \\ &= \sum_{(x_n,y_n)\in\mathcal{A}_n} P_{X_nY_n}(x_n, y_n)\log\frac{P_{X_nY_n}(x_n,y_n)}{P_{X_n}(x_n)P_{Y_n}(y_n)} \\ &\quad + \sum_{(x_n,y_n)\in\mathcal{A}_n^c} P_{X_nY_n}(x_n, y_n)\log\frac{P_{X_nY_n}(x_n,y_n)}{P_{X_n}(x_n)P_{Y_n}(y_n)} \\ &\geq \left(\sum_{\mathcal{A}_n} P_{X_nY_n}(x_n, y_n)\right)\log\frac{\sum_{\mathcal{A}_n} P_{X_nY_n}(x_n,y_n)}{\sum_{\mathcal{A}_n} P_{X_n}(x_n)P_{Y_n}(y_n)} \\ &\quad + \left(\sum_{\mathcal{A}_n^c} P_{X_nY_n}(x_n, y_n)\right)\log\frac{\sum_{\mathcal{A}_n^c} P_{X_nY_n}(x_n,y_n)}{\sum_{\mathcal{A}_n^c} P_{X_n}(x_n)P_{Y_n}(y_n)} \\ &= (1-\alpha_n)\log\frac{1-\alpha_n}{\beta_n} + \alpha_n\log\frac{\alpha_n}{1-\beta_n} \\ &= -h(\alpha_n) - (1-\alpha_n)\log\beta_n - \alpha_n\log(1-\beta_n) \\ &\geq -h(\alpha_n) - (1-\alpha_n)\log\beta_n \end{aligned} \tag{37}$$

where the first inequality follows from the log sum inequality, and the second inequality holds because $-\alpha_n\log(1-\beta_n) \geq 0$. Hence, it follows from (36) and (37) that

$$\frac{1}{n}I(X_n;Y_n) \geq -\frac{h(\alpha_n)}{n} + (1-\alpha_n)\max\left\{-\frac{1}{n}\log P_n^X, -\frac{1}{n}\log P_n^Y\right\} \quad \text{for all} \quad n \geq 1. \tag{38}$$

Therefore, we have (16) by taking the limit superior of both sides of (38) and noticing (34). □

Remark 3: The claim of Theorem 1 can be easily extended to the case where S^n is generated from a stationary source. For the case of the stationary source, the entropy $H(S)$ in the statement of Theorem 1 is replaced with the entropy rate $H \stackrel{\text{def}}{=} \lim_{n\to\infty} H(S^n)/n$. By recalling the existence of the limit of $\{H(S^n)/n\}_{n=1}^\infty$ [23, Theorem 4.2.1], we can easily check that both the left hand sides of (25) and (29) are bounded by $H + \ell$.

B. Proof of Theorem 2

We choose arbitrarily a sequence $\{\gamma_n\}_{n=1}^\infty$ of positive numbers that satisfies $\lim_{n\to\infty}\gamma_n = 0$ and $\lim_{n\to\infty}\sqrt{n}\gamma_n = \infty$. Let $\mathcal{T}_{\gamma_n}$ be the typical set defined by

$$\mathcal{T}_{\gamma_n} = \left\{s^n \in \mathcal{S}^n : \left|\frac{1}{n}\log\frac{1}{P_{S^n}(s^n)} - H(S)\right| \leq \gamma_n\right\}. \tag{39}$$

Then, it is well-known that (e.g., see [23, Theorem 3.1.2]) $\mathcal{T}_{\gamma_n}$ satisfies the following properties:

$$\lim_{n\to\infty}\Pr\{S^n \in \mathcal{T}_{\gamma_n}\} = 1 \tag{40}$$
$$|\mathcal{T}_{\gamma_n}| \leq 2^{n\{H(S)+\gamma_n\}} \quad \text{for all} \quad n \geq 1. \tag{41}$$

For an arbitrary $\ell \geq 0$, let $\mathcal{L}_n \stackrel{\text{def}}{=} \{0, 1, \ldots, L_n - 1\}$ and $\mathcal{M}_n \stackrel{\text{def}}{=} \{0, 1, \ldots, M_n - 1\}$ be sets of integers where $L_n \stackrel{\text{def}}{=} \lfloor 2^{n\ell}\rfloor$ and $M_n \stackrel{\text{def}}{=} |\mathcal{T}_{\gamma_n}|$.

In the following, we construct a sequence $\{(\varphi_n^*, \psi_n^*)\}_{n=1}^\infty$ of an encoder φ_n^* and a decoder ψ_n^* that asymptotically realizes a $(2,2)$–threshold scheme with correlation level ℓ satisfying $|\mathcal{X}_n| = |\mathcal{Y}_n| = |\mathcal{U}_n| = L_n(M_n + 1)$.

The encoder φ_n^* can be constructed as follows: Since $M_n = |\mathcal{T}_{\gamma_n}|$, there exists a bijection $\xi_n : \mathcal{T}_{\gamma_n} \to \mathcal{M}_n$. Furthermore, define a map $\xi_n^+ : \mathcal{S}^n \to \mathcal{M}_n^+$ where $\mathcal{M}_n^+ \stackrel{\text{def}}{=} \mathcal{M}_n \cup \{M_n\}$ by

$$\xi_n^+(s^n) = \begin{cases} \xi_n(s^n), & \text{if } s^n \in \mathcal{T}_{\gamma_n} \\ M_n, & \text{otherwise} \end{cases} \tag{42}$$

and let $Z_n \stackrel{\text{def}}{=} \xi_n^+(S^n)$. Denote by $U_n^{\mathcal{L}}$ and $U_n^{\mathcal{M}}$ the random variables subject to the uniform distribution on $\mathcal{L}_n$ and $\mathcal{M}_n^+$, respectively, and define $U_n = (U_n^{\mathcal{L}}, U_n^{\mathcal{M}})$. In addition, we define two shares by

$$X_n = \left(X_n^{\mathcal{L}}, X_n^{\mathcal{M}}\right) = \left(U_n^{\mathcal{L}}, Z_n \ominus U_n^{\mathcal{M}}\right) \in \mathcal{L}_n \times \mathcal{M}_n^+ \tag{43}$$
$$Y_n = \left(U_n^{\mathcal{L}}, U_n^{\mathcal{M}}\right) \in \mathcal{L}_n \times \mathcal{M}_n^+ \tag{44}$$

where $\ominus$ represents the subtraction of modulo $M_n + 1$.

Next, let us define the decoder ψ_n^*. Let $x_n = (x_n^{\mathcal{L}}, x_n^{\mathcal{M}}) \in \mathcal{L}_n \times \mathcal{M}_n^+$ and $y_n = (y_n^{\mathcal{L}}, y_n^{\mathcal{M}}) \in \mathcal{L}_n \times \mathcal{M}_n^+$ be the inputs to the decoder. Then, the decoder ψ_n^* first checks whether $x_n^{\mathcal{L}} = y_n^{\mathcal{L}}$ holds or not. If $x_n^{\mathcal{L}} \neq y_n^{\mathcal{L}}$, the decoder judges that impersonation attack has occurred and outputs $\perp$. On the other hand, if $x_n^{\mathcal{L}} = y_n^{\mathcal{L}}$, the decoder computes $x_n^{\mathcal{M}} \oplus y_n^{\mathcal{M}}$, where $\oplus$ denotes the addition of modulo $M_n + 1$. If $x_n^{\mathcal{M}} \oplus y_n^{\mathcal{M}} = M_n$, the decoder outputs $\perp$ since the decoding error occurs in such a case. Otherwise, the decoder outputs $\xi_n^{-1}(x_n^{\mathcal{M}} \oplus y_n^{\mathcal{M}})$ where $\xi_n^{-1} : \mathcal{M}_n \to \mathcal{T}_{\gamma_n}$ is the inverse map of ξ_n. Summarizing, the decoder ψ_n^* is written as

$$\psi_n^*(x_n, y_n) = \begin{cases} \xi_n^{-1}(x_n^{\mathcal{M}} \oplus y_n^{\mathcal{M}}), & \text{if } x_n^{\mathcal{L}} = y_n^{\mathcal{L}} \text{ and} \\ & x_n^{\mathcal{M}} \oplus y_n^{\mathcal{M}} \neq M_n \text{ are satisfied} \\ \perp, & \text{otherwise} \end{cases} \tag{45}$$

and the acceptance region of ψ_n^* is given by

$$\mathcal{A}_n = \{(x_n, y_n) \in \mathcal{X}_n \times \mathcal{Y}_n : x_n^{\mathcal{L}} = y_n^{\mathcal{L}} \text{ and } x_n^{\mathcal{M}} \oplus y_n^{\mathcal{M}} \in \mathcal{M}_n\}. \tag{46}$$

Hereafter, we prove that the above sequence $\{(\varphi_n^*, \psi_n^*)\}_{n=1}^{\infty}$ realizes the optimal $(2,2)$–threshold scheme with correlation level ℓ that asymptotically attains all the bounds in (17)–(20). It suffices to prove Claims 1–5 below.

Claim 1: For an arbitrarily small $\gamma > 0$, the rates of X_n, Y_n and U_n can be less than $H(S) + \ell + \gamma$ for all sufficiently large n, i.e., (17)–(19) hold.

Claim 2: The limit inferior of the minimum exponent in the success probabilities of impersonation attacks is at least ℓ, i.e., (20) holds.

Claim 3: The decoding error probability for the legitimate shares vanishes as n goes to infinity, i.e., (7) holds.

Claim 4: For all $n \geq 1$, the n source outputs S^n are secure against the leakage from one of X_n and Y_n, i.e., (21) holds.

Claim 5: The correlation level between X_n and Y_n equals to ℓ, i.e., (12) holds.

Proof of Claim 1: In order to evaluate the share rates and the randomness given by (17)–(19), observe that

$$\begin{aligned} \log|\mathcal{X}_n| &= \log|\mathcal{Y}_n| = \log|\mathcal{U}_n| \\ &= \log\{L_n(M_n+1)\} \\ &= \log\left\{\lfloor 2^{n\ell}\rfloor(|\mathcal{T}_{\gamma_n}|+1)\right\} \\ &\leq n\{H(S)+\ell+\gamma_n\}+1 \end{aligned} \tag{47}$$

where the last inequality follows from (41). Hence, it holds that

$$\frac{1}{n}\log|\mathcal{X}_n| = \frac{1}{n}\log|\mathcal{Y}_n| = \frac{1}{n}\log|\mathcal{U}_n| \leq H(S)+\ell+\gamma_n+\frac{1}{n}. \tag{48}$$

Taking the limit superior of both sides in (48), Claim 1 is established. □

Proof of Claim 2: We evaluate P_n^X in the following way:

$$\begin{aligned} P_n^X &= \max_{P_{\overline{X}_n}} \Pr\left\{(\overline{X}_n, Y_n) \in \mathcal{A}_n\right\} \\ &= \max_{P_{\overline{X}_n}} \Pr\left\{\overline{X}_n^{\mathcal{L}} = Y_n^{\mathcal{L}} \text{ and } \overline{X}_n^{\mathcal{M}} \oplus Y_n^{\mathcal{M}} \in \mathcal{T}_{\gamma_n}\right\} \\ &\leq \max_{P_{\overline{X}_n}} \Pr\left\{\overline{X}_n^{\mathcal{L}} = Y_n^{\mathcal{L}}\right\} = \max_{P_{\overline{X}_n^{\mathcal{L}}}} \Pr\left\{\overline{X}_n^{\mathcal{L}} = U_n^{\mathcal{L}}\right\} \\ &\overset{\text{(a)}}{=} \max_{P_{\overline{X}_n^{\mathcal{L}}}} \sum_{x_n^{\mathcal{L}} \in \mathcal{L}_n} P_{\overline{X}_n^{\mathcal{L}}}(x_n^{\mathcal{L}}) P_{U_n^{\mathcal{L}}}(x_n^{\mathcal{L}}) \\ &\overset{\text{(b)}}{=} \frac{1}{L_n} \max_{P_{\overline{X}_n^{\mathcal{L}}}} \sum_{x_n^{\mathcal{L}} \in \mathcal{L}_n} P_{\overline{X}_n^{\mathcal{L}}}(x_n^{\mathcal{L}}) = \frac{1}{L_n} \end{aligned} \tag{49}$$

where $\overline{X}_n \overset{\text{def}}{=} (\overline{X}_n^{\mathcal{L}}, \overline{X}_n^{\mathcal{M}}) \in \mathcal{L}_n \times \mathcal{M}_n^+$ and $Y_n \overset{\text{def}}{=} (Y_n^{\mathcal{L}}, Y_n^{\mathcal{M}}) = (U_n^{\mathcal{L}}, U_n^{\mathcal{M}}) \in \mathcal{L}_n \times \mathcal{M}_n^+$, and the marked equalities follow from the following reasons:

(a) $\overline{X}_n^{\mathcal{L}}$ and $U_n^{\mathcal{L}}$ are independent.
(b) $P_{U_n^{\mathcal{L}}}(x_n^{\mathcal{L}}) = 1/L_n$ holds for all $x_n^{\mathcal{L}} \in \mathcal{L}_n$.

Similarly, noticing the fact that $X_n^{\mathcal{L}} = U_n^{\mathcal{L}}$, we also have $P_n^Y \leq 1/L_n$, and therefore, we conclude that

$$\begin{aligned} \liminf_{n\to\infty} \min\left\{-\frac{1}{n}\log P_n^X, -\frac{1}{n}\log P_n^Y\right\} \\ \geq \liminf_{n\to\infty} \frac{1}{n}\log L_n = \ell. \end{aligned} \tag{50}$$

□

Proof of Claim 3: Since every legitimate pair $(x_n, y_n) \in \mathcal{A}_n$ of shares is decoded by φ_n^* without error, the decoding error happens only if the decoder ψ_n^* outputs $\perp$ for a pair of legitimate shares (x_n, y_n). Hence, the decoding error probability P_n^e can be written as

$$\begin{aligned} P_n^e &= \Pr\{\psi_n^*(X_n, Y_n) = \perp\} \\ &= \Pr\{\xi_n^+(S^n) = M_n\} \\ &= \Pr\{S^n \notin \mathcal{T}_{\gamma_n}\}. \end{aligned}$$

Therefore, it follows from (40) that $\lim_{n\to\infty} P_n^e = 1 - \lim_{n\to\infty} \Pr\{S^n \in \mathcal{T}_{\gamma_n}\} = 0$. □

Proof of Claim 4: First, we note that Z_n and $X_n^{\mathcal{M}} = Z_n \ominus U_n^{\mathcal{M}}$ are independent because of non-negativity of the mutual information and

$$\begin{aligned} I(Z_n; Z_n \ominus U_n^{\mathcal{M}}) &= H(Z_n) + H(Z_n \ominus U_n^{\mathcal{M}}) \\ &\quad - H(Z_n, Z_n \ominus U_n^{\mathcal{M}}) \\ &= H(Z_n) + H(Z_n \ominus U_n^{\mathcal{M}}) - H(Z_n, U_n^{\mathcal{M}}) \\ &= H(Z_n \ominus U_n^{\mathcal{M}}) - H(U_n^{\mathcal{M}}) \\ &\leq 0 \end{aligned} \tag{51}$$

where the last inequality holds because $Z_n \ominus U_n^{\mathcal{M}} \in \mathcal{M}_n^+$ and $U_n^{\mathcal{M}}$ is subject to the uniform distribution on $\mathcal{M}_n^+$. Hence, Z_n and $X_n = (X_n^{\mathcal{L}}, X_n^{\mathcal{M}})$ are also independent because

$$\begin{aligned} I(Z_n; X_n) &= I(Z_n; X_n^{\mathcal{L}} X_n^{\mathcal{M}}) \\ &= I(Z_n; X_n^{\mathcal{M}}) + I(Z_n; X_n^{\mathcal{L}} | X_n^{\mathcal{M}}) \\ &= 0 \end{aligned} \tag{52}$$

where the last equality follows since $I(Z_n; X_n^{\mathcal{M}}) = 0$, and Z_n, $X_n^{\mathcal{M}}$, and $X_n^{\mathcal{L}}$ form a Markov chain in this order.

In order to show (21), it is sufficient to prove that $I(S^n; X_n) = 0$ for all $n \geq 1$ because $I(S^n; Y_n) = 0$ for any $n \geq 1$ trivially holds from the fact that S^n and $Y_n = (U_n^{\mathcal{L}}, U_n^{\mathcal{M}})$ are independent. In addition, $I(S_n; X_n) = 0$ is established from $I(S^n; X_n) \leq I(Z_n; X_n) = 0$ which is obtained by the information processing inequality [23, Theorem 2.8.1] for a Markov chain $S_n \to Z_n \to X_n$, and recalling (52). □

Proof of Claim 5: The correlation level can be evaluated as follows. Note that the mutual information of shares X_n and Y_n satisfies

$$\begin{aligned} I(X_n; Y_n) &= I(X_n^{\mathcal{L}} X_n^{\mathcal{M}}; Y_n^{\mathcal{L}} Y_n^{\mathcal{M}}) \\ &= I(U_n^{\mathcal{L}} X_n^{\mathcal{M}}; U_n^{\mathcal{L}} U_n^{\mathcal{M}}) \\ &= H(U_n^{\mathcal{L}} X_n^{\mathcal{M}}) - H(X_n^{\mathcal{M}} | U_n^{\mathcal{L}} U_n^{\mathcal{M}}) \\ &\quad - H(U_n^{\mathcal{L}} | X_n^{\mathcal{M}} U_n^{\mathcal{L}} U_n^{\mathcal{M}}) \\ &\overset{\text{(c)}}{=} H(U_n^{\mathcal{L}}) + H(X_n^{\mathcal{M}}) - H(X_n^{\mathcal{M}} | U_n^{\mathcal{M}}) \\ &\overset{\text{(d)}}{=} H(U_n^{\mathcal{L}}) + H(X_n^{\mathcal{M}}) - H(Z_n) \end{aligned} \tag{53}$$

where the marked equalities hold because of the following reasons:

(c) $U_n^{\mathcal{L}}$ and $X_n^{\mathcal{M}}$ are independent, and $U_n^{\mathcal{L}}$, $U_n^{\mathcal{M}}$, and $X_n^{\mathcal{M}}$ form a Markov chain in this order.

(d) It follows that $H(X_n^{\mathcal{M}} | U_n^{\mathcal{M}}) = H\left(Z_n \ominus U_n^{\mathcal{M}} | U_n^{\mathcal{M}}\right) = H\left(Z_n | U_n^{\mathcal{M}}\right) = H\left(Z_n\right)$ due to the independence of S^n and U_n.

Hereafter, we evaluate the terms on the right hand side of (53). It is easy to see that

$$H(U_n^{\mathcal{L}}) = \log L_n = \log \lfloor 2^{n\ell} \rfloor. \tag{54}$$

The second term in the right hand side of (53) can be evaluated as

$$\begin{aligned} H(X_n^{\mathcal{M}}) &\leq \log(M_n + 1) \\ &= \log(|\mathcal{T}_{\gamma_n}| + 1) \\ &\leq n\{H(S) + \gamma_n\} + 1 \end{aligned} \tag{55}$$

where the last inequality follows from (41). In order to evaluate the last term on the right hand side of (53), we set $\delta_n = \Pr\{\xi_n^+(S^n) = M_n\} = \Pr\{S^n \notin \mathcal{T}_{\gamma_n}\}$. Clearly, $\lim_{n\to\infty} \delta_n = 0$ from (40). Since the map $\xi_n : \mathcal{T}_{\gamma_n} \to \mathcal{M}_n$ is bijective, we have

$$\begin{aligned} H(Z_n) &= H(\xi_n^+(S^n)) \\ &= \sum_{s^n \in \mathcal{T}_{\gamma_n}} P_{S^n}(s^n) \log \frac{1}{P_{S^n}(s^n)} + \delta_n \log \frac{1}{\delta_n} \\ &\geq \sum_{s^n \in \mathcal{T}_{\gamma_n}} P_{S^n}(s^n) n\{H(S) - \gamma_n\} - \delta_n \log \delta_n \\ &= (1 - \delta_n) n\{H(S) - \gamma_n\} - \delta_n \log \delta_n \end{aligned} \tag{56}$$

where the inequality holds because of (41). Hence, we have from (55) and (56) that

$$\begin{aligned} H(X_n^{\mathcal{M}}) - H(Z_n) \\ \leq n\delta_n H(S) + n(2 - \delta_n)\gamma_n + \delta_n \log \delta_n + 1. \end{aligned} \tag{57}$$

On the other hand, it is easy to see with the same reason for the equality (d) in (53) that

$$H(X_n^{\mathcal{M}}) - H(Z_n) \geq H(X_n^{\mathcal{M}} | U_n^{\mathcal{M}}) - H(Z_n) = 0. \tag{58}$$

Summarizing, we have from (53), (54), (57), and (58) that

$$\begin{aligned} \frac{1}{n} \log \lfloor 2^{n\ell} \rfloor &\leq \frac{1}{n} I(X_n; Y_n) \\ &\leq \frac{1}{n} \log \lfloor 2^{n\ell} \rfloor + \delta_n H(S) \\ &\quad + (2 - \delta_n)\gamma_n + \frac{1}{n}\left(\delta_n \log \delta_n + 1\right). \end{aligned} \tag{59}$$

By taking the limit of both sides of (59) and noticing that $\lim_{n\to\infty} \gamma_n = \lim_{n\to\infty} \delta_n = 0$, we have

$$\lim_{n\to\infty} \frac{1}{n} I(X_n; Y_n) = \ell. \tag{60}$$

□

Since Claims 1–5 are verified, Theorem 2 is proved. □

Remark 4: The claim of Theorem 2 is valid for the class of stationary ergodic sources if the entropy $H(S)$ in Theorem 2 is replaced with the entropy rate $H \overset{\text{def}}{=} \lim_{n\to\infty} H(S^n)/n$. This fact is obtained by a slight modification of the proof of Theorem 2 followed by the diagonal line argument [25, Theorem 1.8.2]. First, by the asymptotic equipartition property [23, Theorem 3.1.2], we have

$$\lim_{n\to\infty} \Pr\{S^n \in \mathcal{T}_{n,\gamma}\} = 1 \tag{61}$$

for any constant $\gamma > 0$, where

$$\mathcal{T}_{n,\gamma} \overset{\text{def}}{=} \left\{ s^n \in \mathcal{S}^n \,:\, \left| \frac{1}{n} \log \frac{1}{P_{S^n}(s^n)} - H \right| \leq \gamma \right\} \tag{62}$$

and H denotes the entropy rate of the source. We construct an encoder $\varphi_{n,\gamma}^*$ and a decoder $\psi_{n,\gamma}^*$ in the same way as in the proof of Theorem 2. It is easily checked that $\{(\varphi_{n,\gamma}^*, \psi_{n,\gamma}^*)\}_{n=1}^{\infty}$ asymptotically realizes the $(2, 2)$–threshold scheme. In addition, by the same argument with (48) and (59), $\{(\varphi_{n,\gamma}^*, \psi_{n,\gamma}^*)\}_{n=1}^{\infty}$ satisfies

$$\frac{1}{n} \log |\mathcal{X}_n| = \frac{1}{n} \log |\mathcal{Y}_n| = \frac{1}{n} \log |\mathcal{U}_n| \leq H + \ell + \gamma + \frac{1}{n} \tag{63}$$

and

$$\begin{aligned} \frac{1}{n} \log \lfloor 2^{n\ell} \rfloor &\leq \frac{1}{n} I(X_n; Y_n) \\ &\leq \frac{1}{n} \log \lfloor 2^{n\ell} \rfloor + \delta_{n,\gamma} H + (2 - \delta_{n,\gamma})\gamma \\ &\quad + \frac{1}{n}(\delta_{n,\gamma} \log \delta_{n,\gamma} + 1) \end{aligned} \tag{64}$$

where $\delta_{n,\gamma} \overset{\text{def}}{=} \Pr\{S^n \notin \mathcal{T}_{n,\gamma}\} \to 0$ as $n \to \infty$. Note that (64) implies that

$$\left| \frac{1}{n} I(X_n; Y_n) - \ell \right| \leq 3\gamma \quad \text{for all } n \geq N_0(\gamma). \tag{65}$$

We now fix a sequence $\{\gamma_m\}_{m=1}^{\infty}$ satisfying $\gamma_0 > \gamma_1 > \cdots > \gamma_m > \cdots > 0$ arbitrarily and define $N_0 = 1$ and N_m, $m = 1, 2, \ldots$, as the minimum integer N satisfying $|\, I(X_n; Y_n)/n - \ell \,| \leq 3\gamma_m$ for all $n \geq N$. Obviously,

$\{N_m\}_{m=1}^{\infty}$ is monotone nondecreasing. We define (φ_n^*, ψ_n^*) as $(\varphi_{n,\gamma_0}^*, \psi_{n,\gamma_0}^*)$ for each $1 \le n < N_1$ and $(\varphi_{n,\gamma_m}^*, \psi_{n,\gamma_m}^*)$ for each $N_m \le n < N_{m+1}$, $m = 1, 2, \ldots$. Then, in view of (63), (65) and $\gamma_m \downarrow 0$ as $m \to \infty$, we can conclude that $\{(\varphi_n^*, \psi_n^*)\}_{n=1}^{\infty}$ satisfies

$$\limsup_{n\to\infty} \frac{1}{n} \log |\mathcal{X}_n| = \limsup_{n\to\infty} \frac{1}{n} \log |\mathcal{Y}_n| = \limsup_{n\to\infty} \frac{1}{n} \log |\mathcal{U}_n| \le H + \ell \tag{66}$$

and

$$\lim_{n\to\infty} \frac{1}{n} I(X_n; Y_n) = \ell. \tag{67}$$

V. Another Optimal Scheme Using Symbolwise Encoding

In Section III, we have shown by using blockwise coding that the sequence $\{(\varphi_n^*, \psi_n^*)\}_{n=1}^{\infty}$ of an encoder and a decoder realizes the asymptotically optimal $(2,2)$–threshold scheme with correlation level ℓ. In addition, $\{(\varphi_n^*, \psi_n^*)\}_{n=1}^{\infty}$ also attains the maximum exponent in the success probabilities of impersonation attack which is given by ℓ. In this section, by using a symbolwise encoding, we give a simple construction of $\{(\varphi_n^*, \psi_n^*)\}_{n=1}^{\infty}$ that realizes the asymptotically optimal $(2,2)$–threshold scheme with correlation level ℓ and the exponent in the success probability of impersonation attacks equals to ℓ. In this construction, we use a pair (f, g) of an encoder f and a decoder g for a $(2,2)$–threshold scheme for a single source output S. In addition, a one-sided test is used to detect the impersonation attacks.

Let S, U, X and Y be random variables of a secret, a random number, and two shares taking values in finite sets $\mathcal{S}, \mathcal{U}, \mathcal{X}$ and $\mathcal{Y}$ respectively. For a non-negative number ℓ, we first define a pair (f, g) of an encoder f and a decoder g for a $(2,2)$–threshold scheme with correlation level ℓ. That is, the encoder $f : \mathcal{S} \times \mathcal{U} \to \mathcal{X} \times \mathcal{Y}$ is defined to be a deterministic map satisfying

$$H(S|X) = H(S|Y) = H(S) \tag{68}$$

$$H(S|XY) = 0 \tag{69}$$

in addition to

$$I(X; Y) = \ell \tag{70}$$

where shares X and Y are determined by $(X, Y) = f(S, U)$. Note that (68) and (69) are the ordinary requirements for $(2,2)$–threshold schemes, i.e., (68) guarantees that any information of S does not leak from either one of the shares, and (69) implies that the secret S can be decoded from X and Y without error. Hence, let $g : \mathcal{X} \times \mathcal{Y} \to \mathcal{S} \cup \{\lambda\}$ be a decoder corresponding to f and satisfying $g(x, y) = \lambda$ for every $(x, y) \in \mathcal{X} \times \mathcal{Y}$ that does not belong to the range of f. Furthermore, (70) means that the correlation level of X and Y generated by the encoder f is equal to ℓ. We say that a pair (f, g) of an encoder f and a decoder g realizes a $(2,2)$–threshold scheme with correlation level ℓ in the non-asymptotic sense if (f, g) satisfies (68)–(70). In addition, it is shown in [26] that

$$\min\{\, |\mathcal{X}|, |\mathcal{Y}|, |\mathcal{U}| \,\} \ge |\mathcal{S}| \tag{71}$$

must be satisfied for any encoder of $(2,2)$–threshold schemes satisfying (68) and (69). Hence, we also impose (71) on f in addition to (68)–(70).

In this setting, we define an encoder $\varphi_n^* : \mathcal{S}^n \times \mathcal{U}^n \to \mathcal{X}^n \times \mathcal{Y}^n$ as the repeated application of $f : \mathcal{S} \times \mathcal{U} \to \mathcal{X} \times \mathcal{Y}$ to (S_i, U_i), $i = 1, 2, \ldots, n$, which can be written as

$$\varphi_n^*(s^n, u^n) \stackrel{\text{def}}{=} f(s_1, u_1) f(s_2, u_2) \cdots f(s_n, u_n) \tag{72}$$

where $s^n \stackrel{\text{def}}{=} s_1 s_2 \cdots s_n \in \mathcal{S}^n$ and $u^n \stackrel{\text{def}}{=} u_1 u_2 \cdots u_n \in \mathcal{U}^n$ are n secrets and n random numbers, respectively. Hence, the two shares $X^n = X_1 X_2 \cdots X_n \in \mathcal{X}^n$ and $Y^n = Y_1 Y_2 \cdots Y_n \in \mathcal{Y}^n$ are i.i.d. copies of X and Y, respectively, where $(X_i, Y_i) = f(S_i, U_i)$.

Furthermore, we define

$$\mathcal{A}_n^* = \left\{ (x^n, y^n) \in \mathcal{X}^n \times \mathcal{Y}^n : \frac{1}{n} \log \frac{P_{XY}(x^n, y^n)}{P_{X^n}(x^n) P_{Y^n}(y^n)} > I(X; Y) - \gamma_n \right\} \tag{73}$$

where γ_n is an arbitrary sequence of positive integers $\{\gamma_n\}_{n=1}^{\infty}$ satisfying $\lim_{n\to\infty} \gamma_n = 0$ and $\lim_{n\to\infty} \sqrt{n}\gamma_n = \infty$. Then, legitimate shares belong to $\mathcal{A}_n^*$ with high probability if n is sufficiently large since

$$\lim_{n\to\infty} \Pr\{(X^n, Y^n) \in \mathcal{A}_n^*\} = 1 \tag{74}$$

holds from the law of large numbers. Hence, we regard the received shares as legitimate if they belong to $\mathcal{A}_n^*$, and decode them by the decoder g_n corresponding to the encoder φ_n^* in (72), where g_n can be written as

$$g_n(x^n, y^n) \stackrel{\text{def}}{=} g(x_1, y_1) g(x_2, y_2) \cdots g(x_n, y_n). \tag{75}$$

In addition, the decoder $\psi_n^* : \mathcal{X}^n \times \mathcal{Y}^n \to \mathcal{S}^n \cup \{\perp\}$ is defined by

$$\psi_n^*(x^n, y^n) = \begin{cases} g_n(x^n, y^n), & \text{if } (x^n, y^n) \in \mathcal{A}_n^* \\ \perp, & \text{otherwise} \end{cases} \tag{76}$$

where $\perp$ means that the impersonation attack, i.e., (a1) or (a2) in Section II, is detected.

According to (74), every $(x^n, y^n) \in \mathcal{A}_n^*$ satisfies $P_{X^n Y^n}(x^n, y^n) > 0$, which is equivalent to $P_{XY}(x_i, y_i) > 0$, i.e., $g(x_i, y_i) \ne \lambda$, for all $i = 1, 2, \ldots, n$. Hence, for every $(x^n, y^n) \in \mathcal{A}_n^*$, there uniquely exists $s^n \in \mathcal{S}^n$ that satisfies $g_n(x^n, y^n) = s^n$ whether the received shares x^n and y^n are legitimate or not. Furthermore, if the pair of shares $(x^n, y^n) \in \mathcal{A}_n^*$ is legitimate, the secret is reproduced without error due to the definitions of f and φ_n^*. More precisely, $\psi_n^*(x^n, y^n) = g_n(x^n, y^n) = s^n$ holds for every $u^n \in \mathcal{U}^n$, $s^n \in \mathcal{S}^n$, $x^n \in \mathcal{X}^n$ and $y^n \in \mathcal{Y}^n$ satisfying $\varphi_n^*(s^n, u^n) = (x^n, y^n) \in \mathcal{A}_n^*$.

The above sequence $\{(\varphi_n^*, \psi_n^*)\}_{n=1}^{\infty}$ defined by (72) and (76) realizes an asymptotic $(2,2)$–threshold scheme with correlation level ℓ.

Theorem 3: Let (f,g) be any pair of an encoder and a decoder that realizes a $(2,2)$–threshold scheme with correlation level ℓ in the non-asymptotic sense. Then, the sequence $\{(\varphi_n^*,\psi_n^*)\}_{n=1}^{\infty}$ defined by (72) and (76) satisfies for all $n\geq 1$ that

$$P_n^e = \Pr\{(X^n,Y^n)\notin\mathcal{A}_n^*\} \tag{77}$$
$$H(S^n|X^n) = H(S^n|Y^n) = H(S^n) \tag{78}$$
$$I(X^n;Y^n) = n\ell \tag{79}$$

which obviously realizes an asymptotic $(2,2)$–threshold scheme with correlation level ℓ. In addition, this $\{(\varphi_n^*,\psi_n^*)\}_{n=1}^{\infty}$ satisfies (20).

Proof of Theorem 3: First, we prove (77). If there is a one-to-one correspondence between (s^n,u^n) and (x^n,y^n), (77) is obvious. We show that (77) holds for any pair of f and g satisfying (68) and (69) which does not guarantee the existence of such a one-to-one correspondence.

Define

$$\mathcal{D}_n^*(x^n,y^n) = \{(s^n,u^n) : \varphi_n^*(s^n,u^n) = (x^n,y^n) \text{ and } \psi_n^*(x^n,y^n) = s^n\}. \tag{80}$$

Recalling that $\psi_n^*(x^n,y^n) = g_n(x^n,y^n) = s^n$ for every $u^n\in\mathcal{U}^n$, $s^n\in\mathcal{S}^n$, $x^n\in\mathcal{X}^n$ and $y^n\in\mathcal{Y}^n$ satisfying $\varphi_n^*(s^n,u^n) = (x^n,y^n)\in\mathcal{A}_n^*$, it holds for all $(x^n,y^n)\in\mathcal{A}_n^*$ that

$$\begin{aligned}\mathcal{D}_n(x^n,y^n) &= \{(s^n,u^n) : \varphi_n^*(s^n,u^n) = (x^n,y^n) \text{ and } g_n(x^n,y^n) = s^n\}\\ &= \{(s^n,u^n) : \varphi_n^*(s^n,u^n) = (x^n,y^n)\}\\ &\stackrel{\text{def}}{=} {\varphi_n^*}^{-1}(x^n,y^n)\end{aligned} \tag{81}$$

where ${\varphi_n^*}^{-1}(x^n,y^n)$ means the inverse image of (x^n,y^n).

Next, we define

$$\mathcal{D}_n = \{(s^n,u^n) : \psi_n^*(\varphi_n^*(s^n,u^n)) = s^n\}. \tag{82}$$

Then, since $\psi_n^*(x^n,y^n) = \perp$ for all $(x^n,y^n)\notin\mathcal{A}_n^*$ and s^n is reproduced without error from every $(x^n,y^n)\in\mathcal{A}_n^*$, we have

$$\begin{aligned}\mathcal{D}_n &= \bigcup_{(x^n,y^n)\in\mathcal{A}_n^*}\mathcal{D}_n(x^n,y^n)\\ &= \bigcup_{(x^n,y^n)\in\mathcal{A}_n^*}{\varphi_n^*}^{-1}(x^n,y^n)\end{aligned} \tag{83}$$

where the second equality follows from (81). Furthermore, since φ_n^* is deterministic, it is easy to see that

$${\varphi_n^*}^{-1}(x^n,y^n)\cap{\varphi_n^*}^{-1}(\tilde{x}^n,\tilde{y}^n) = \emptyset \quad \text{for all } (x^n,y^n)\neq(\tilde{x}^n,\tilde{y}^n). \tag{84}$$

From (83) and (84), it is shown that $\{{\varphi_n^*}^{-1}(x^n,y^n)\}_{(x^n,y^n)\in\mathcal{A}_n^*}$ is a partition of $\mathcal{D}_n$. Therefore, we have

$$\begin{aligned}1-P_n^e &= \sum_{(s^n,u^n)\in\mathcal{D}_n}P_{S^nU^n}(s^n,u^n).\\ &= \sum_{(x^n,y^n)\in\mathcal{A}_n^*}\ \sum_{(s^n,u^n)\in{\varphi_n^*}^{-1}(x^n,y^n)}P_{S^nU^n}(s^n,u^n)\\ &= \sum_{(x^n,y^n)\in\mathcal{A}_n^*}P_{X^nY^n}(x^n,y^n)\\ &= \Pr\{(X^n,Y^n)\in\mathcal{A}_n^*\}\end{aligned} \tag{85}$$

where the first equality comes from the definition of the decoding error probability and the third equality is due to the definition of $P_{X^nY^n}(\cdot,\cdot)$, i.e., $P_{X^nY^n}(x^n,y^n) = \sum_{(s^n,u^n)\in\mathcal{S}^n\times\mathcal{U}^n:\varphi_n^*(s^n,u^n)=(x^n,y^n)}P_{S^nE^n}(s^n,u^n)$. Hence, we obtain (77). It is easy to see from (74) that P_n^e satisfies (7) i.e., the decoding error probability of ψ_n^* in (76) vanishes as n goes to infinity.

In order to establish Theorem 3, it remains to show that $\{(\varphi_n^*,\psi_n^*)\}_{n=1}^{\infty}$ satisfies (20). Note that (78) and (79) clearly hold from (68) and (70), respectively. To this end, we evaluate the success probability of the impersonation attack as follows:

$$\begin{aligned}P_n^X &= \max_{P_{\overline{X}^n}}\Pr\left\{(\overline{X}^n,Y^n)\in\mathcal{A}_n^*\right\}\\ &= \max_{P_{\overline{X}^n}}\sum_{(x^n,y^n)\in\mathcal{A}_n^*}P_{\overline{X}^n}(x^n)P_{Y^n}(y^n)\\ &\leq \max_{P_{\overline{X}^n}}\sum_{(x^n,y^n)\in\mathcal{A}_n^*}P_{\overline{X}^n}(x^n)\frac{P_{X^nY^n}(x^n,y^n)}{P_{X^n}(x^n)}2^{-n(\ell-\gamma_n)}\\ &\leq \max_{P_{\overline{X}^n}}\sum_{\substack{(x^n,y^n)\\ \in\mathcal{X}^n\times\mathcal{Y}^n}}P_{\overline{X}^n}(x^n)\frac{P_{X^nY^n}(x^n,y^n)}{P_{X^n}(x^n)}2^{-n(\ell-\gamma_n)}\\ &= 2^{-n(\ell-\gamma_n)}\end{aligned} \tag{86}$$

where the first inequality follows from (73) which implies

$$\begin{aligned}P_{Y^n}(y^n) &< \frac{P_{X^nY^n}(x^n,y^n)}{P_{X^n}(x^n)}2^{-n\{I(X;Y)-\gamma_n\}}\\ &= \frac{P_{X^nY^n}(x^n,y^n)}{P_{X^n}(x^n)}2^{-n(\ell-\gamma_n)}\end{aligned} \tag{87}$$

for any $(x^n,y^n)\in\mathcal{A}_n^*$. Similarly, we have $P_n^Y\leq 2^{-n(\ell-\gamma_n)}$. Hence, we obtain (20) since $\lim_{n\to\infty}\gamma_n = 0$. □

Since Theorem 3 has been proved, we are now interested in a relation between the share rates and the correlation level attained by a pair (f,g) of an encoder f and a decoder g, which is given by the following claim:

Claim 6: Let M and M_S be arbitrary positive integers satisfying $M\geq M_S$. Then, there exists a pair (f^*,g^*) of an encoder f^* and a decoder g^* for a $(2,2)$–threshold scheme with correlation level $\ell = \log M - H(S)$ in the non-asymptotic sense satisfying $|\mathcal{X}| = |\mathcal{Y}| = |\mathcal{U}| = M$ and $|\mathcal{S}| = M_S$.

Remark 5: According to Claim 6, the rates of shares and randomness are $\log|\mathcal{X}| = \log|\mathcal{Y}| = \log|\mathcal{U}| = \log M = H(S)-\ell$, which coincides with the lower bounds of the rates given by (17)–(19). Hence, the sequence $\{(\varphi_n^*,\psi_n^*)\}_{n=1}^{\infty}$ defined by (72) and (76) also achieves all the bounds in

Theorem 2. Observe that the sequence of encoders $\{\varphi_n^*\}_{n=1}^{\infty}$ in this section is simpler than the the sequence of encoders presented in Theorems 2. For instance, S^n cannot be encoded symbolwisely by the sequence of encoders in the proof of Theorem 2 since the correlation of two shares is generated by the random variable $U_n^{\mathcal{L}}$ in both shares contained in common. On the other hand, symbolwise encoding is possible by the sequence of encoders in this section since X_i and Y_i are correlated due to f for every $i = 1, 2, \ldots, n$. Furthermore, such symbolwise encoding also enables us that $I(S_i; X_i) = I(S_i; Y_i) = 0$ for every $i = 1, 2, \ldots, n$, which is stronger than the security condition given by (21) in Theorem 2.

However, we note that M, M_S and the correlation level ℓ cannot be set arbitrarily in Claim 6 although they can be taken arbitrarily in Theorem 2, which is compensation for the simplicity.

Remark 6: In the threshold scheme with detectability of substitution attacks in a non-asymptotic setup (e.g., [3]–[8]), it is shown that any ideal secret sharing scheme cannot detect any forgery of shares with probability 1. Furthermore, as is shown in [26], we note that the ideal secret sharing schemes can be realized if and only if $|\mathcal{X}| = |\mathcal{Y}| = |\mathcal{S}|$ and S is uniformly distributed.

Similarly, in the asymptotic setup discussed in this section, it is impossible for any (f, g) of an ideal $(2, 2)$–threshold scheme to achieve P_n^X and P_n^Y with exponential order of n because the correlation level $\log M - H(S) = 0$ is satisfied if and only if $M = |\mathcal{S}|$ and S is uniformly distributed. On the other hand, we note that ℓ is positive for arbitrary distribution of S if $\min\{\, |\mathcal{X}|, |\mathcal{Y}|, |\mathcal{U}| \,\} > |\mathcal{S}|$. □

Proof of Claim 6: From (71), let us define

$$\mathcal{X} = \mathcal{Y} = \mathcal{U} = \{0, 1, \ldots, M-1\} \tag{88}$$

$$\mathcal{S} = \{0, 1, \ldots, M_S - 1\} \tag{89}$$

where $M \geq M_S$. Define the encoder $f^* : \mathcal{S} \times \mathcal{U} \to \mathcal{X} \times \mathcal{Y}$ for a secret $s \in \mathcal{S}$ and a random number $u \in \mathcal{U}$ as

$$f^*(s, u) = (s \ominus u, u) \tag{90}$$

where $\ominus$ denotes the subtraction of modulo M. Then, the corresponding decoder $g^* : \mathcal{X} \times \mathcal{Y} \to \mathcal{S} \cup \{\lambda\}$ can be written as

$$g^*(x, y) = \begin{cases} x \oplus y, & \text{if } x \oplus y \in \mathcal{S} \\ \lambda, & \text{otherwise} \end{cases} \tag{91}$$

where $\oplus$ represents the addition of modulo M. Note that the secret s can be decoded by g^* without error, and hence, (69) is satisfied. Furthermore, we can check that a pair of the shares (X, Y) is generated according to the conditional probability distribution

$$P_{XY|S}(x, y|s) = \begin{cases} 1/M, & \text{if } \ s = x \oplus y \in \mathcal{S} \\ 0, & \text{otherwise} \end{cases} \tag{92}$$

if we apply the encoder f^* defined in (90) to the secret S with an arbitrary probability distribution $P_S(\cdot)$. Hence, the following discussion holds for an arbitrary distribution on S. This idea is based on the secret sharing scheme for non-uniform secret distribution studied in [26].

We show that (68) is satisfied by X and Y generated by f^*. For every fixed $x \in \mathcal{X}$ and $s \in \mathcal{S}$, we can check that there exists a unique $y \in \mathcal{Y}$, satisfying $s = g^*(x, y)$. Hence, it holds from (92) that

$$\begin{aligned} P_{X|S}(x|s) &= \sum_{y \in \mathcal{Y}} P_{XY|S}(x, y|s) \\ &= \frac{1}{M} \end{aligned} \tag{93}$$

for every $(x, s) \in \mathcal{X} \times \mathcal{S}$. Then, we have

$$\begin{aligned} P_X(x) &= \sum_{s \in \mathcal{S}} P_{X|S}(x|s) P_S(s) \\ &= \sum_{s \in \mathcal{S}} \frac{1}{M} \cdot P_S(s) \\ &= \frac{1}{M}. \end{aligned} \tag{94}$$

From (93) and (94), it is shown that S and X are statistically independent. Similarly, it can be shown that S and Y are statistically independent, and hence, (68) is proved.

The correlation level of X and Y generated by f^* can be calculated as follows. We note that

$$\begin{aligned} H(XY) &\overset{\text{(e)}}{=} H(US) \\ &\overset{\text{(f)}}{=} H(U) + H(S) \\ &= \log M + H(S) \end{aligned} \tag{95}$$

where the marked equalities (e) and (f) hold since

(e) there exists a bijection between $\mathcal{U} \times \mathcal{S}$ and $\mathcal{X} \times \mathcal{Y}$.
(f) U and S are statistically independent.

Therefore, we obtain from (94) and (95) that

$$\begin{aligned} I(X; Y) &= H(X) + H(Y) - H(XY) \\ &= 2 \log M - \{\log M + H(S)\} \\ &= \log M - H(S). \end{aligned} \tag{96}$$

Hence, it is shown that the pair (f^*, g^*) of the encoder and the decoder actually realizes a $(2, 2)$–threshold scheme with correlation level $\log M - H(S)$. □

VI. Conclusion

This paper is concerned with coding theorems for a $(2, 2)$–threshold scheme in the presence of an opponent who impersonates one of the participants. We have considered an asymptotic setup of the $(2, 2)$–threshold scheme in which n secrets from a memoryless source are encoded to two shares by using a uniform random number, and the two shares are decoded to the n secrets with permitting negligible decoding error probability. We have investigated the minimum attainable rates of the two shares and the uniform random number, and the maximum exponents of the probabilities of the successful impersonation from a Shannon-theoretic viewpoint. We have presented coding theorems for two cases of encoding, i.e., blockwise and symbolwise encoding.

In the first case, we have considered the situation where the n secrets are encoded blockwisely to two shares. We

have defined the correlation level $\ell \geq 0$ of the shares as the limit of the normalized mutual information between the two shares. In the converse part it is shown that for any sequence $\{(\varphi_n, \psi_n)\}_{n=1}^{\infty}$ of pairs of an encoder φ_n and a decoder ψ_n that asymptotically realizes a $(2,2)$–threshold scheme with the correlation level ℓ, none of the rates can be less than $H(S)+\ell$, where $H(S)$ denotes the entropy of the source, and the exponent of the probability of the successful impersonation cannot be less than ℓ. In addition, we have shown the existence of a sequence $\{(\varphi_n^*, \psi_n^*)\}_{n=1}^{\infty}$ of pairs of an encoder φ_n^* and a decoder ψ_n^* that attains all the bounds given in the converse part. The obtained results can be easily extended to the case where the n secrets are generated from a stationary ergodic source.

In the second case, we have considered the situation where the n secrets are encoded symbolwisely to two shares of length n by repeatedly applying the encoder of an ordinary $(2,2)$–threshold scheme to the n secrets. While the above converse part is valid in this setup, we can give another interesting decoder in the direct part. That is, we have shown that the impersonation by an opponent can be verified with probability close to one by verifying the joint typicality of the two shares. It turns out that these encoder and decoder also attain all the bounds in the converse part.

ACKNOWLEDGMENT

The authors would like to thank Prof. H. Nagaoka in the University of Electro-Communications, for his helpful comments.

REFERENCES

[1] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[2] G. R. Blakley, "Safeguarding cryptographic keys," *AFIPS 1979 National Computer Conference*, vol. 48, pp. 313–317, 1979.

[3] R. J. McEliece and D. V. Sarwate, "On sharing secrets and Reed Solomon codes," *Communications of the ACM*, vol. 24, no. 9, pp. 583–584, 1981.

[4] E. D. Karnin, J. W. Greene, and M. E. Hellman, "On secret sharing systems," *IEEE Trans. Inform. Theory*, vol. 29, no. 1, pp. 35–41, 1983.

[5] M. Tompa and H. Woll, "How to share a secret with cheaters," *Journal of Cryptology*, vol. 1, no. 3, pp. 133–138, 1988. Preliminary version: *CRYPTO'86*, LNCS 263, pp.261–265.

[6] M. Carpentieri, A. D. Santis, and U. Vaccaro, "Size of shares and probability of cheating in threshold scheme," *Advances in Cryptology–EUROCRYPT'93,* LNCS 765, Springer-Verlag, pp. 118–125, 1994.

[7] K. Kurosawa, S. Obana, and W. Ogata, "t-cheater identifiable (k,n) secret sharing schemes," *Advances in Cryptology–CRYPTO'95,* LNCS 963, Springer-Verlag, pp. 410–423, 1995.

[8] W. Ogata, K. Kurosawa, and D. R. Stinson, "Optimum secret sharing scheme secure against cheating," *SIAM Journal of Discrete Mathematics*, vol. 20, no. 1, pp. 79–95, 2006. Preliminary version: *EUROCRYPT'96*, LNCS 1070, pp.200–211.

[9] S. Obana and T. Araki, "Secret sharing schemes secure against cheating for arbitrary secret distribution," *Advances in Cryptology–ASIACRYPT 2006,* LNCS 4284, Springer-Verlag, pp. 364–379, 2006.

[10] G. J. Simmons, "Authentication theory/coding theory," *Advances in Cryptology–CRYPTO'84,* LNCS 196, Springer-Verlag, pp. 411–431, 1985.

[11] H. Yamamoto, "On secret sharing communication systems with two or three channels," *IEEE Trans. Information Theory*, vol. 32, no. 3, pp. 387–393, 1986.

[12] H. Koga, "Coding theorems on the threshold secret sharing scheme for a general source," *IEEE Trans. Information Theory*, vol. 54, no. 6, pp. 2658–2677, 2006.

[13] D. R. Stinson and S. A. Vanstone, "A combinatorial approach to threshold schemes," *SIAM J. on Discrete Math.*, no. 1, pp. 230–237, 1988. Preliminary version: *CRYPTO'87*, pp.331–339.

[14] H. Koga and H. Yamamoto, "Coding theorems for secret-key authentication systems," *IEICE Trans. Fundamentals*, vol. E83–A, no. 8, pp. 1691–1703, 2000.

[15] H. Koga, "A generalization of the Simmons' bounds on secret-key authentication systems," *IEICE Trans. Fundamentals*, vol. E83–A, no. 10, pp. 1983–1985, 2000.

[16] U. M. Maurer, "Authentication theory and hypothesis testing," *IEEE Trans. on Information Theory*, vol. 46, no. 4, pp. 1350–1356, 2000. Preliminary version: *STACS'96*, LNCS 1046, pp.387–398, 1996.

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

[18] M. E. Hellman, "An extension of the Shannon theory approach to cryptography," *IEEE Trans. Information Theory*, vol. 23, no. 3, pp. 289–294, 1977.

[19] H. Yamamoto, "Coding theorems for Shannon's cipher system with correlated source outputs, and common information," *IEEE Trans. Information Theory*, vol. 40, no. 1, pp. 85–95, 1994.

[20] H. Yamamoto, "Information theory in cryptography," *IEICE Trans. Fundamentals*, vol. E–74, no. 9, pp. 2456–2464, 1991.

[21] U. M. Maurer, "Secret key agreement by public discussion based on common information," *IEEE Trans. Information Theory*, vol. 39, no. 3, pp. 733–743, 1993.

[22] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography– part I: secret sharing," *IEEE Trans. Information Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.

[23] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. Wiley and Interscience, second ed., 2006.

[24] R. E. Blahut, *Principles and Practice of Information Theory*. Addison Wesley, 1991.

[25] T. S. Han, *Information-Spectrum Methods in Information Theory*. Springer-Verlag, 2003.

[26] C. Blundo, A. D. Santis, and U. Vaccaro, "On secret sharing schemes," *Information Processing Letters*, no. 65, pp. 25–32, 1998.

Mitsugu Iwamoto (S'01-M'04) received the B.E., the M.E., and Ph.D. degrees from the University of Tokyo, Japan, in 1999, 2001, and 2004, respectively. In 2004, he joined University of Electro-Communications, where he is currently an Assistant Professor of the Center for Frontier Science and Engineering. His research interests include information theory and cryptography. He is a member of IACR and IEICE.

Hiroki Koga (S'93-M'94) received B.E., M.E. and Ph.D degrees from the University of Tokyo, in 1990, 1992 and 1995, respectively.

From 1995 to 1999, he was a Research Associate in Graduate school of Engineering, the University of Tokyo. Since 1999, he has been with the University of Tsukuba, where he is currently an Associate Professor of Graduate School of Systems and Information Engineering. His research interests are in Shannon theory and information security. He is a senior member of the IEICE.

Hirosuke Yamamoto (S'77-M'80-SM'03–F'11) received the B.E. degree from Shizuoka University, Shizuoka, Japan, in 1975 and the M.E. and Ph.D. degrees from the University of Tokyo, Tokyo, Japan, in 1977 and 1980, respectively, all in electrical engineering. In 1980, he joined Tokushima University. He was an Associate Professor at Tokushima University from 1983 to 1987, the University of Electro-Communications from 1987 to 1993, and the University of Tokyo from 1993 to 1999. Since 1999, he has been a Professor at the University of Tokyo and is currently with the Department of Complexity Science and Engineering at the university. In 1989–1990, he was a Visiting Scholar at the Information Systems Laboratory, Stanford University, Stanford, CA. His research interests are in Shannon theory, data compression algorithms and cryptology.

Dr. Yamamoto served as the Chair of IEEE Information Theory Society Japan Chapter in 2002–2003, the TPC Co-Chair of the ISITA2004, the TPC Chair of the ISITA2008, the president of the SITA (Society of Information Theory and its Applications) in 2008–2009, an Associate Editor for Shannon Theory, the IEEE Transactions on Information Theory in 2007–2010, Editor-in-Chief for the IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences in 2009-2011. He is a Fellow of the IEICE and he is currently the President of the Engineering Sciences Society, IEICE.