entropy

MDPI

Article

Information Theoretic Security for Shannon Cipher System under Side-Channel Attacks †

Bagus Santoso *,‡ and Yasutada Oohama ‡

University of Electro-Communications, 1-5-1 Chofugaoka, Tokyo 182-8585, Japan; oohama@uec.ac.jp

* Correspondence: santoso.bagus@uec.ac.jp; Tel.: +81-42-443-5288

† This paper is an extended version of our paper published in Oohama, Y.; Santoso, B. Information theoretical analysis of side-channel attacks to the Shannon cipher system. In Proceedings of the 2018 IEEE International Symposium on Information Theory (ISIT), Vail, CO, USA, 17–22 June 2018; pp. 581–585.

‡ These authors contributed equally to this work.

Received: 11 March 2019; Accepted: 29 April 2019; Published: 5 May 2019

Abstract: In this paper, we propose a new theoretical security model for Shannon cipher systems under side-channel attacks, where the adversary is not only allowed to collect ciphertexts by eavesdropping the public communication channel but is also allowed to collect the physical information leaked by the devices where the cipher system is implemented on, such as running time, power consumption, electromagnetic radiation, etc. Our model is very robust as it does not depend on the kind of physical information leaked by the devices. We also prove that in the case of one-time pad encryption, we can strengthen the secrecy/security of the cipher system by using an appropriate affine encoder. More precisely, we prove that for any distribution of the secret keys and any measurement device used for collecting the physical information, we can derive an achievable rate region for reliability and security such that if we compress the ciphertext using an affine encoder with a rate within the achievable rate region, then: (1) anyone with a secret key will be able to decrypt and decode the ciphertext correctly, but (2) any adversary who obtains the ciphertext and also the side physical information will not be able to obtain any information about the hidden source as long as the leaked physical information is encoded with a rate within the rate region. We derive our result by adapting the framework of the one helper source coding problem posed and investigated by Ahlswede and Körner (1975) and Wyner (1975). For reliability and security, we obtain our result by combining the result of Csizár (1982) on universal coding for a single source using linear codes and the exponential strong converse theorem of Oohama (2015) for the one helper source coding problem.

Keywords: information theoretic security; side-channel attacks; Shannon cipher system; one helper source coding problem; strong converse theorem

1. Introduction

In most of theoretical security models for encryption schemes, the adversary only obtains information from the public communication channel. In such models, an adversary is often treated as an entity that tries to obtain information about the hidden source only from the ciphertexts that are sent through the public communication channel. However, in the real world, the encryption schemes are implemented on physical electronic devices, and it is widely known that any process executed in an electronic circuit will generate a certain kind of correlated physical phenomena as "side" effects, according to the type of process. For example, differences in inputs to a process in an electronic circuit can induce differences in the heat, power consumption, and electromagnetic radiation generated as byproducts by the devices. Therefore, we may consider that an adversary who has a certain degree of physical access to the devices may obtain some information on very sensitive hidden data, such as the keys used for the encryption, just by measuring the generated physical phenomena using

appropriate measurement devices. More precisely, an adversary may deduce the value of the bits of the key by measuring the differences in the timing of the process of encryption or the differences in the power consumption, electromagnetic radiation, and other physical phenomena. This information channel where the adversary obtains data in the form of physical phenomena is called the *side-channel*, and attacks using the side-channel are known as side-channel attacks.

In the literature, there have been many works showing that adversaries have succeeded in breaking the security of cryptographic systems by exploiting side-channel information such as running time, power consumption, and electromagnetic radiation in the real physical world [1–5].

1.1. Our Contributions

1.1.1. Security Model for Side-Channel Attacks

In this paper, we propose a security model where the adversary attempts to obtain information about the hidden source by collecting data from (1) the public communication channel in the form of ciphertexts, and (2) the side-channel in the form of some physical data related to the encryption keys. Our proposed security model is illustrated in Figure 1.

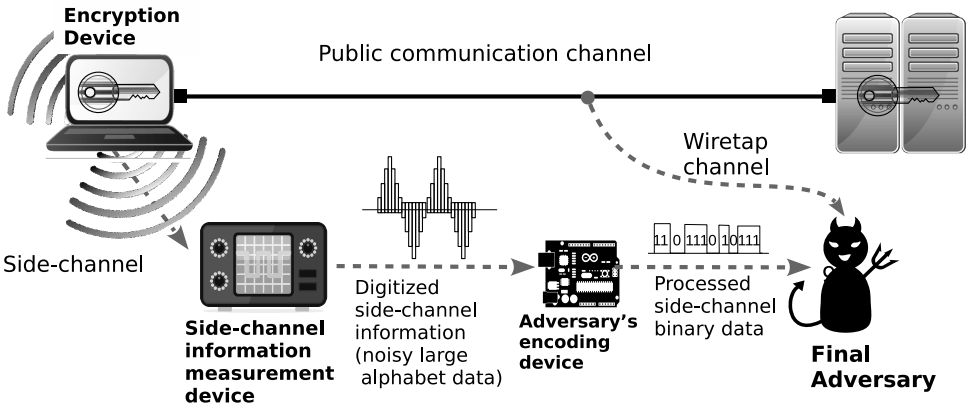

Figure 1. Illustration of side-channel attacks.

Based on the security model illustrated above, we formulate a security problem of strengthening the security of Shannon cipher system where the encryption is implemented on a physical encryption device and the adversary attempts to obtain some information on the hidden source by collecting ciphertexts and performing side-channel attacks.

We describe our security model in a more formal way as follows. The source X is encrypted using an encryption device with secret key K installed. The result of the encryption, i.e., ciphertext C, is sent through a public communication channel to a data center where C is decrypted back into the source X using the same key K. The adversary $\mathcal{A}$ is allowed to obtain C from the public communication channel and is also equipped with an encoding device $\varphi_{\mathcal{A}}$ that encodes and processes the noisy large alphabet data Z, i.e., the measurement result of the physical information obtained from the side-channel, into the appropriate binary data $M_{\mathcal{A}}$. It should be noted that in our model, we do not put any limitation on the kind of physical information measured by the adversary. Hence, any theoretical result based on this model automatically applies to any kind of side-channel attack, including timing analysis, power analysis, and electromagnetic (EM) analysis. In addition, the measurement device may just be a simple analog-to-digital converter that converts the analog data representing physical information leaked

from the device into "noisy" digital data Z. In our model, we represent the measurement process as a communication channel W.

1.1.2. Main Result

As the main theoretical result, we show that we can strengthen the secrecy/security of the Shannon cipher implemented on a physical device against an adversary who collects the ciphertexts and launches side-channel attacks by a simple method of compressing the ciphertext C from a Shannon cipher using an affine encoder φ into $\widetilde{C}$ before releasing it into the public communication channel.

We prove that in the case of one-time pad encryption, we can strengthen the secrecy/security of the cipher system by using an appropriate affine encoder. More precisely, we prove that for any distribution of the secret key K and any measurement device (used to convert the physical information from a side-channel into the noisy large alphabet data Z), we can derive an achievable rate region for $(R_{\mathcal{A}}, R)$ such that if we compress the ciphertext C into $\widetilde{C}$ using the affine encoder φ, which has an encoding rate R inside the achievable region, then we can achieve reliability and security in the following sense:

- anyone with secret key K can construct an appropriate decoder that decrypts and encodes $\widetilde{C}$ with exponentially decaying error probability, but
- the amount of information gained by any adversary $\mathcal{A}$ who obtains the compressed ciphertext $\widetilde{C}$ and encoded physical information $M_{\mathcal{A}}$ is exponentially decaying to zero as long as the encoding device $\varphi_{\mathcal{A}}$ encodes the side physical information into $M_{\mathcal{A}}$ with a rate $R_{\mathcal{A}}$ within the achievable rate region.

By utilizing the homomorphic property of one-time-pad and affine encoding, we are able to separate the theoretical analysis of reliability and security such that we can deal with each issue independently. For reliability, we mainly obtain our result by using the result of Csizár [6] on the universal coding for a single source using linear codes. For the security analysis, we derive our result by adapting the framework of the one helper source coding problem posed and investigated by Ahlswede, Körner [7] and Wyner [8]. Specifically, in order to derive the secrecy exponent, we utilize the exponential strong converse theorem of Oohama [9] for the one helper source coding problem. In [10], Watanabe and Oohama deal with a similar source coding problem, but their result is insufficient for deriving the lower bound of the secrecy exponent. We will explain the relation between our method and previous related works in more detail in Section 4.

1.2. Comparison to Existing Models of Side-Channel Attacks

The most important feature of our model is that we do not make any assumption about the type or characteristics of the physical information that is measured by the adversary. Several theoretical models analyzing the security of a cryptographic system against side-channel attacks have been proposed in the literature. However, most of the existing works are applicable only for specific characteristics of the leaked physical information. For example, Brier et al. [1] and Coron et al. [11] propose a statistical model for side-channel attacks using the information from power consumption and the running time, whereas Agrawal et al. [5] propose a statistical model for side-channel attacks using electromagnetic (EM) radiations. A more general model for side-channel attacks is proposed by Köpf et al. [12] and Backes et al. [13], but they are heavily dependent upon implementation on certain specific devices. Micali et al. [14] propose a very general security model to capture the side-channel attacks, but they fail to offer any hint of how to build a concrete countermeasure against the side-channel attacks. The closest existing model to ours is the general framework for analyzing side-channel attacks proposed by Standaert et al. [15]. The authors of [15] propose a countermeasure against side-channel attacks that is different from ours, i.e., noise insertion on implementation. It should be noted that the noise insertion countermeasure proposed by [15] is dependent on the characteristics of the leaked physical

information. On the other hand, our countermeasure, i.e., compression using an affine encoder, is independent of the characteristics of the leaked physical information.

1.3. Comparison to Encoding before Encryption

In this paper, our proposed solution is to perform additional encoding in the form of compression after the encryption process. Our aim is that by compressing the ciphertext, we compress the key "indirectly" and increase the "flatness" of the key used in the compressed ciphertext ($\widetilde{C}$) such that the adversary will not get much additional information from eavesdropping on the compressed ciphertext ($\widetilde{C}$). Instead of performing the encoding after encryption, one may consider performing the encoding before encryption, i.e., encoding the source and the key "directly" before performing the encryption. However, since we need to apply two separate encodings on the source and the key, we can expect that the implementation cost is more expensive than our proposed solution, i.e., approximately double the cost of applying our proposed solution. Moreover, it is not completely clear whether our security analysis still applies for this case. For example, if the adversary performs the side-channel attacks on the key after it is encoded (before encryption), we need a complete remodeling of the security problem.

1.4. Organization of this Paper

This paper is structured as follows. In Section 2, we show the basic notations and definitions that we use throughout this paper, and we also describe the formal formulations of our model and the security problem. In Section 3, we explain the idea and the formulation of our proposed solution. In Section 4, we explain the relation between our formulation and previous related works. Based on this, we explain the theoretical challenge which we have to overcome to prove that our proposed solution is sound. In Section 5, we state our main theorem on the reliability and security of our solution. In Section 6, we show the proof of our main theorem. We put the proofs of other related propositions, lemmas, and theorems in the appendix.

2. Problem Formulation

In this section, we will introduce the general notations used throughout this paper and provide a description of the basic problem we are focusing on, i.e., side-channel attacks on Shannon cipher systems. We also explain the basic framework of the solution that we consider to solve the problem. Finally, we state the formulation of the reliability and security problem that we consider and aim to solve in this paper.

2.1. Preliminaries

In this subsection, we show the basic notations and related consensus used in this paper.

Random Source of Information and Key: Let X be a random variable from a finite set $\mathcal{X}$. Let $\{X_t\}_{t=1}^{\infty}$ be a stationary discrete memoryless source (DMS) such that for each $t = 1, 2, \ldots$, X_t takes values in the finite set $\mathcal{X}$ and obeys the same distribution as that of X denoted by $p_X = \{p_X(x)\}_{x\in\mathcal{X}}$. The stationary DMS $\{X_t\}_{t=1}^{\infty}$ is specified with p_X. In addition, let K be a random variable taken from the same finite set $\mathcal{X}$ and representing the key used for encryption. Similarly, let $\{K_t\}_{t=1}^{\infty}$ be a stationary discrete memoryless source such that for each $t = 1, 2, \ldots$, K_t takes values in the finite set $\mathcal{X}$ and obeys the same distribution as that of K denoted by $p_K = \{p_K(k)\}_{k\in\mathcal{X}}$. The stationary DMS $\{K_t\}_{t=1}^{\infty}$ is specified with p_K. In this paper, we assume that p_K is the uniform distribution over $\mathcal{X}$.

Random Variables and Sequences: We write the sequence of random variables with length n from the information source as follows: $X^n := X_1 X_2 \cdots X_n$. Similarly, strings with length n of $\mathcal{X}^n$ are written as

$x^n := x_1 x_2 \cdots x_n \in \mathcal{X}^n$. For $x^n \in \mathcal{X}^n$, $p_{X^n}(x^n)$ stands for the probability of the occurrence of x^n. When the information source is memoryless, specified with p_X, the following equation holds:

$$p_{X^n}(x^n) = \prod_{t=1}^{n} p_X(x_t).$$

In this case, we write $p_{X^n}(x^n)$ as $p_X^n(x^n)$. Similar notations are used for other random variables and sequences.

Consensus and Notations: Without loss of generality, throughout this paper, we assume that $\mathcal{X}$ is a finite field. The notation $\oplus$ is used to denote the field addition operation, while the notation $\ominus$ is used to denote the field subtraction operation, i.e., $a \ominus b = a \oplus (-b)$, for any elements $a, b \in \mathcal{X}$. Throughout this paper, all logarithms are taken to the natural basis.

2.2. Basic System Description

In this subsection, we explain the basic system setting and the basic adversarial model we consider in this paper. First, let the information source and the key be generated independently by different parties $\mathcal{S}_{\mathsf{gen}}$ and $\mathcal{K}_{\mathsf{gen}}$, respectively. In our setting, we assume the following:

- The random key K^n is generated by $\mathcal{K}_{\mathsf{gen}}$ from a uniform distribution.
- The source is generated by $\mathcal{S}_{\mathsf{gen}}$ and is independent of the key.

Next, let the random source X^n from $\mathcal{S}_{\mathsf{gen}}$ be sent to the node L, and let the random key K^n from $\mathcal{K}_{\mathsf{gen}}$ also be sent to L. Further settings of our system are described as follows and are also shown in Figure 2.

1. *Source Processing:* At the node L, X^n is encrypted with the key K^n using the encryption function Enc. The ciphertext C^n of X^n is given by
$$C^n := \mathsf{Enc}(X^n) = X^n \oplus K^n.$$
2. *Transmission:* Next, the ciphertext C^n is sent to the information processing center D through a public communication channel. Meanwhile, the key K^n is sent to D through a private communication channel.
3. *Sink Node Processing:* In D, we decrypt the ciphertext C^n using the key K^n through the corresponding decryption procedure Dec defined by $\mathsf{Dec}(C^n) = C^n \ominus K^n$. It is obvious that we can correctly reproduce the source output X^n from C^n and K^n with the decryption function Dec.

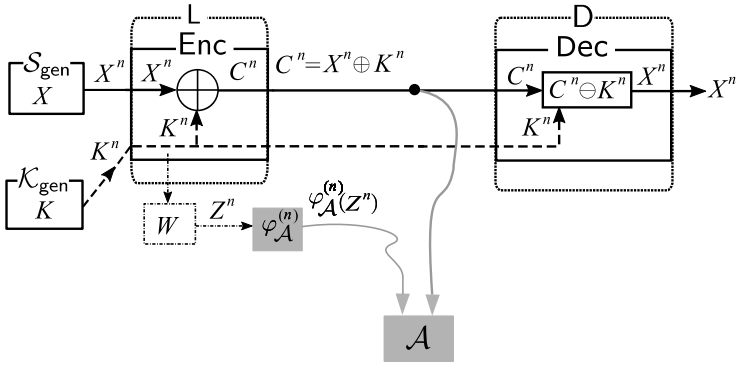

Figure 2. Main problem: side-channel attacks on a Shannon cipher system.

Side-Channel Attacks by Eavesdropper Adversary: An (eavesdropper) adversary $\mathcal{A}$ eavesdrops on the public communication channel in the system. The adversary $\mathcal{A}$ also uses side information obtained

by side-channel attacks. In this paper, we introduce a new theoretical model of side-channel attacks that is described as follows. Let $\mathcal{Z}$ be a finite set and let $W : \mathcal{X} \to \mathcal{Z}$ be a noisy channel. Let Z be a channel output from W for the random input variable K. We consider the discrete memoryless channel specified with W. Let $Z^n \in \mathcal{Z}^n$ be a random variable obtained as the channel output by connecting $K^n \in \mathcal{X}^n$ to the input channel. We write a conditional distribution on Z^n given K^n as

$$W^n = \{W^n(z^n|k^n)\}_{(k^n,z^n)\in\mathcal{K}^n\times\mathcal{Z}^n}.$$

Since the channel is memoryless, we have

$$W^n(z^n|k^n) = \prod_{t=1}^{n} W(z_t|k_t). \tag{1}$$

On the above output Z^n of W^n for the input K^n, we assume the following:

- The three random variables X, K, and Z satisfy $X \perp (K, Z)$, which implies that $X^n \perp (K^n, Z^n)$.
- W is given in the system and the adversary $\mathcal{A}$ cannot control W.
- Through side-channel attacks, the adversary $\mathcal{A}$ can access Z^n.

We next formulate the side information the adversary $\mathcal{A}$ obtains by side-channel attacks. For each $n = 1, 2, \cdots$, let $\varphi_{\mathcal{A}}^{(n)} : \mathcal{Z}^n \to \mathcal{M}_{\mathcal{A}}^{(n)}$ be an encoder function. Set $\varphi_{\mathcal{A}} := \{\varphi_{\mathcal{A}}^{(n)}\}_{n=1,2,\ldots}$. Let

$$R_{\mathcal{A}}^{(n)} := \frac{1}{n}\log||\varphi_{\mathcal{A}}|| = \frac{1}{n}\log|\mathcal{M}_{\mathcal{A}}^{(n)}|$$

be a rate of the encoder function $\varphi_{\mathcal{A}}^{(n)}$. For $R_{\mathcal{A}} > 0$, we set

$$\mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}}) := \{\varphi_{\mathcal{A}}^{(n)} : R_{\mathcal{A}}^{(n)} \le R_{\mathcal{A}}\}.$$

For the encoded side information the adversary $\mathcal{A}$ obtains, we assume the following.

- The adversary $\mathcal{A}$, having accessed Z^n, obtains the encoded additional information $\varphi_{\mathcal{A}}^{(n)}(Z^n)$. For each $n = 1, 2, \cdots$, the adversary $\mathcal{A}$ can design $\varphi_{\mathcal{A}}^{(n)}$.
- The sequence $\{R_{\mathcal{A}}^{(n)}\}_{n=1}^{\infty}$ must be upper-bounded by a prescribed value. In other words, the adversary $\mathcal{A}$ must use $\varphi_{\mathcal{A}}^{(n)}$ such that for some $R_{\mathcal{A}}$ and for any sufficiently large n, $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$.

On the Scope of Our Theoretical Model: When the $|\mathcal{Z}|$ is not so large, the adversary $\mathcal{A}$ may directly access Z^n. In contrast, in a real situation of side-channel attacks, often the noisy version Z^n of K^n can be regarded as very close to an analog random signal. In this case, $|\mathcal{Z}|$ is sufficiently large and the adversary $\mathcal{A}$ cannot obtain Z^n in a lossless form. Our theoretical model can address such situations of side-channel attacks.

2.3. Solution Framework

As the basic solution framework, we consider applying a post-encryption-compression coding system. The application of this system is illustrated in Figure 3.

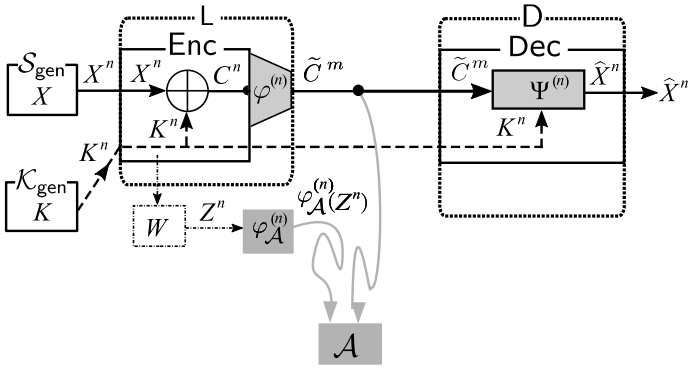

Figure 3. Basic solution framework: post-encryption-compression coding system.

1. *Encoding at Source node* L*:* We first use $\varphi^{(n)}$ to encode the ciphertext $C^n = X^n \oplus K^n$. The formal definition of $\varphi^{(n)}$ is $\varphi_i^{(n)} : \mathcal{X}^n \to \mathcal{X}^m$. Let $\widetilde{C}^m = \varphi^{(n)}(C^n)$. Instead of sending C^n, we send $\tilde{C}^m$ to the public communication channel.
2. *Decoding at Sink Nodes* D*:* D receives $\widetilde{C}^m$ from the public communication channel. Using the common key K^n and the decoder function $\Psi^{(n)} : \mathcal{X}^m \times \mathcal{X}^n \to \mathcal{X}^n$, D outputs an estimation $\hat{X}^n = \Psi^{(n)}(\tilde{C}^m, K^n)$ of X^n.

On Reliability and Security: From the description of our system in the previous section, the decoding process in our system above is successful if $\widehat{X}^n = X^n$ holds. Combining this and (6), it is clear that the decoding error probabilities p_{e} are as follows:

$$p_{\text{e}} = p_{\text{e}}(\varphi^{(n)}, \Psi^{(n)} | p_X^n) := \Pr[\Psi^{(n)}(\varphi^{(n)}(X^n)) \neq X^n].$$

Set $M_{\mathcal{A}}^{(n)} = \varphi_{\mathcal{A}}^{(n)}(Z^n)$. The information leakage $\Delta^{(n)}$ on X^n from $(\widetilde{C}^m, M_{\mathcal{A}}^{(n)})$ is measured by the mutual information between X^n and $(\widetilde{C}^m, M_{\mathcal{A}}^{(n)})$. This quantity is formally defined by

$$\Delta^{(n)} = \Delta^{(n)}(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)} | p_X^n, p_K^n, W^n) := I(X^n; \widetilde{C}^m, M_{\mathcal{A}}^{(n)}).$$

Reliable and Secure Framework:

Definition 1. *A quantity R is achievable under $R_{\mathcal{A}} > 0$ for the system* Sys *if there exists a sequence $\{(\varphi^{(n)}, \Psi^{(n)})\}_{n\geq 1}$ such that $\forall \epsilon > 0$, $\exists n_0 = n_0(\epsilon) \in \mathbb{N}_0$, $\forall n \geq n_0$, we have*

$$\frac{1}{n} \log |\mathcal{X}^m| = \frac{m}{n} \log |\mathcal{X}| \leq R, p_{\text{e}}(\varphi^{(n)}, \Psi^{(n)} | p_X^n) \leq \epsilon,$$

and for any eavesdropper $\mathcal{A}$ with $\varphi_{\mathcal{A}}$ satisfying $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$,

$$\Delta^{(n)}(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)} | p_X^n, p_K^n, W^n) \leq \epsilon.$$

Definition 2. *[Reliable and Secure Rate Region] Let $\mathcal{R}_{\text{Sys}}(p_X, p_K, W)$ denote the set of all $(R_{\mathcal{A}}, R)$ such that R is achievable under $R_{\mathcal{A}}$. We call $\mathcal{R}_{\text{Sys}}(p_X, p_K, W)$ the reliable and secure rate region.*

Definition 3. *A triple (R, E, F) is achievable under $R_{\mathcal{A}} > 0$ for the system* Sys *if there exists a sequence $\{(\varphi^{(n)}, \psi^{(n)})\}_{n\geq 1}$ such that $\forall \epsilon > 0$, $\exists n_0 = n_0(\epsilon) \in \mathbb{N}_0$, $\forall n \geq n_0$, we have*

$$\frac{1}{n} \log |\mathcal{X}^m| = \frac{m}{n} \log |\mathcal{X}| \leq R, p_{\text{e}}(\phi^{(n)}, \psi^{(n)} | p_X^n) \leq \text{e}^{-n(E-\epsilon)},$$

and for any eavesdropper $\mathcal{A}$ with $\varphi_{\mathcal{A}}$ satisfying $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$, we have

$$\Delta^{(n)}(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)} | p_X^n, p_K^n, W^n) \leq \mathrm{e}^{-n(F-\epsilon)}.$$

Definition 4 (Rate, Reliability, and Security Region)**.** *Let $\mathcal{D}_{\mathsf{Sys}}(p_X, p_K, W)$ denote the set of all $(R_{\mathcal{A}}, R, E, F)$ such that (R, E, F) is achievable under $R_{\mathcal{A}}$. We call $\mathcal{D}_{\mathsf{Sys}}(p_X, p_K, W)$ the rate, reliability and security region.*

Our aim in this paper is to find the explicit inner bounds of $\mathcal{R}_{\mathsf{Sys}}(p_X, p_K, W)$ and $\mathcal{D}_{\mathsf{Sys}}(p_X, p_K, W)$.

3. Proposed Idea: Affine Encoder as a Privacy Amplifier

In order to instantiate the basic solution framework mentioned in previous section, we propose the use of an affine encoder as the compression function $\varphi^{(n)}$. We show in this section that we can easily construct an affine encoder that is suitable for our solution framework based on a linear encoder. The instantiation of the solution framework with an affine encoder is illustrated in Figure 4.

Construction of the Affine Encoder: For each $n = 1, 2, \cdots$, let $\phi^{(n)} : \mathcal{X}^n \to \mathcal{X}^m$ be a linear mapping. We define the mapping $\phi^{(n)}$ by

$$\phi^{(n)}(x^n) = x^n A \text{ for } x^n \in \mathcal{X}^n, \tag{2}$$

where A is a matrix with n rows and m columns. Entries of A are from $\mathcal{X}$. We fix $b^m \in \mathcal{X}^m$. Define the mapping $\varphi^{(n)} : \mathcal{X}^n \to \mathcal{X}^m$ by

$$\varphi^{(n)}(k^n) := \phi^{(n)}(k^n) \oplus b^m = k^n A \oplus b^m, \text{ for } k^n \in \mathcal{X}^n. \tag{3}$$

The mapping $\varphi^{(n)}$ is called the affine mapping induced by the linear mapping $\phi^{(n)}$ and constant vector $b^m \in \mathcal{X}^m$. By the definition of $\varphi^{(n)}$ shown in (3), the following *affine structure* holds:

$$\varphi^{(n)}(x^n \oplus k^n) = (x^n \oplus k^n)A \oplus b^m = x^n A \oplus (k^n A \oplus b^m) = \phi^{(n)}(x^n) \oplus \varphi^{(n)}(k^n), \text{ for } x^n, k^n \in \mathcal{X}^n. \tag{4}$$

Next, let $\psi^{(n)}$ be the corresponding decoder for $\phi^{(n)}$ such that $\psi^{(n)} : \mathcal{X}^m \to \mathcal{X}^n$. Note that $\psi^{(n)}$ does not have a linear structure in general.

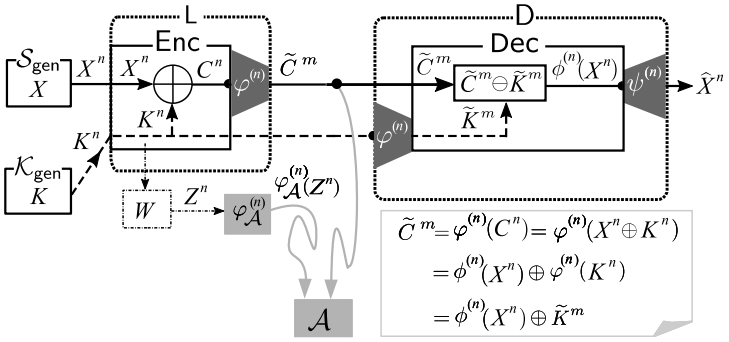

Figure 4. Our proposed solution: affine encoders as privacy amplifiers.

Description of Proposed Procedure: We describe the procedure of our privacy amplified system as follows.

1. *Encoding of Ciphertext:* First, we use $\varphi^{(n)}$ to encode the ciphertext $C^n = X^n \oplus K^n$. Let $\widetilde{C}^m = \varphi^{(n)}(C^n)$. Then, instead of sending C^n, we send $\widetilde{C}^m$ to the public communication channel. By the affine structure of the encoder $\varphi^{(n)}$ (shown in (4)) we have

$$\widetilde{C}^m = \varphi^{(n)}(X^n \oplus K^n) = \phi^{(n)}(X^n) \oplus \varphi^{(n)}(K^n) = \widetilde{X}^m \oplus \widetilde{K}^m, \tag{5}$$

where we set $\widetilde{X}^m := \phi^{(n)}(X^n), \widetilde{K}^m := \varphi^{(n)}(K^n)$.

2. *Decoding at Sink Node* D: First, using the linear encoder $\varphi^{(n)}$, D encodes the key K^n received through a private channel into $\widetilde{K}^m = (\varphi^{(n)}(K^n)$. Receiving $\widetilde{C}^m$ from the public communication channel, D computes $\widetilde{X}^m$ in the following way. From (5), we have that the decoder D can obtain $\widetilde{X}^m = \phi^{(n)}(X^n)$ by subtracting $\widetilde{K}^m = \varphi^{(n)}(K^n)$ from $\widetilde{C}^m$. Finally, D outputs $\widehat{X}^n$ by applying the decoder $\psi^{(n)}$ to $\widetilde{X}^m$ as follows:

$$\widehat{X}^n = \psi^{(n)}(\widetilde{X}^m) = \psi^{(n)}(\phi^{(n)}(X^n)). \tag{6}$$

Our concrete privacy-amplified system described above is illustrated in Figure 4.

Splitting of Reliability and Security

By the affine structure of the encoder function $\varphi^{(n)}$, the proposed privacy amplified system can be split into two coding problems. One is a source coding problem using a linear encoder $\phi^{(n)}$. We hereafter call this Problem 0. The other is a privacy amplification problem using the affine encoder $\varphi^{(n)}$. We call this Problem 1. These two problems are shown in Figure 5.

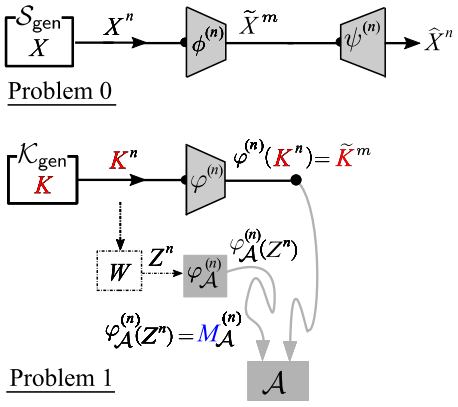

Figure 5. Two split problems: Problem 0 (Reliability) and Problem 1 (Security).

On Reliability (Problem 0): From the description of our system in the previous section, the decoding process in our system above is successful if $\widehat{X}^n = X^n$ holds. Combining this and (6), it is clear that the decoding error probability p_e is as follows:

$$p_e = p_e(\varphi^{(n)}, \psi^{(n)} | p_X^n) = \Pr[\psi^{(n)}(\phi^{(n)}(X^n)) \neq X^n].$$

In Problem 0, we discuss the minimum rate R such that $\exists \{(\phi^{(n)}, \psi^{(n)})\}_{n \geq 1}$ such that $\forall \epsilon > 0$, $\exists n_0 = n_0(\epsilon) \in \mathbb{N}_0$, $\forall n \geq n_0$, we have

$$\frac{1}{n} \log |\mathcal{X}^m| = \frac{m}{n} \log |\mathcal{X}| \leq R + \varepsilon, p_e(\phi^{(n)}, \psi^{(n)} | p_X^n) \leq \epsilon.$$

It is well known that this minimum is equal to $H(X)$ when $\{\phi^{(n)}\}_{n \geq}$ is a sequence of general (nonlinear) encoders. Csiszár [6] proved the existence of a sequence of linear encoders and nonlinear decoders $\{(\phi^{(n)}, \psi^{(n)})\}_{n \geq 1}$ such that for any p_X satisfying $R > H(X)$, the error probability $p_e(\phi^{(n)}, \psi^{(n)} | p_X^n)$ decays exponentially as $n \to \infty$. His result is stated in the next section.

On Security (Problem 1): We assume that the adversary $\mathcal{A}$ knows (A, b^n) defining the affine encoder $\varphi^{(n)}$. When $\varphi^{(n)}$ has the affine structure shown in (4), the information leakage $\Delta^{(n)}$ measured by the mutual information between X^n and $(\widetilde{C}^m, M_{\mathcal{A}}^{(n)})$ has the following form:

$$\begin{aligned}\Delta^{(n)} &= \Delta^{(n)}(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)} | p_X^n, p_K^n, W^n) = I(X^n; \widetilde{C}^m, M_{\mathcal{A}}^{(n)}) = I(X^n; \varphi^{(n)}(X^n \oplus K^n), M_{\mathcal{A}}^{(n)}),\\ &\overset{(a)}{=} I(X^n; \varphi^{(n)}(X^n) \oplus \phi^{(n)}(K^n), M_{\mathcal{A}}^{(n)}) = I(X^n; \widetilde{X}^m \oplus \widetilde{K}^m | M_{\mathcal{A}}^{(n)}). \end{aligned} \tag{7}$$

Step (a) follows from $X_1^n \perp M_{\mathcal{A}}^{(n)}$. Using (7), we upper bound $\Delta^{(n)} = I(X^n; \widetilde{C}^m, M_{\mathcal{A}}^{(n)})$ to obtain the following lemma.

Lemma 1.

$$\Delta^{(n)} = I(X^n; \widetilde{C}^m, M_{\mathcal{A}}^{(n)}) \leq D\left(p_{\widetilde{K}^m | M_{\mathcal{A}}^{(n)}} \middle|\middle| p_{V^m} \middle| p_{M_{\mathcal{A}}^{(n)}}\right), \tag{8}$$

where p_{V^m} represents the uniform distribution over $\mathcal{X}^m$.

Proof. We have the following chain of inequalities:

$$\begin{aligned}\Delta^{(n)} &= I(X^n; \widetilde{C}^m, M_{\mathcal{A}}^{(n)}) \overset{(a)}{=} I(X_1^n; \widetilde{X}^m + \widetilde{K}^m | M_{\mathcal{A}}^{(n)}) \leq \log|\mathcal{X}^m| - H(\widetilde{X}^m + \widetilde{K}^m | X^n, M_{\mathcal{A}}^{(n)})\\ &\overset{(b)}{=} \log|\mathcal{X}^m| - H(\widetilde{K}^m | X^n, M_{\mathcal{A}}^{(n)}) \overset{(c)}{=} \log|\mathcal{X}^m| - H(\widetilde{K}^m | M_{\mathcal{A}}^{(n)}) = D\left(p_{\widetilde{K}^m | M_{\mathcal{A}}^{(n)}} \middle|\middle| p_{V^m} \middle| p_{M_{\mathcal{A}}^{(n)}}\right).\end{aligned}$$

Step (a) follows from (7). Step (b) follows from $\widetilde{X}^m = \phi^{(n)}(X^n)$. Step (c) follows from $(\widetilde{K}^m, M_{\mathcal{A}}^{(n)}) \perp X_1^n$. □

We set

$$\xi_D^{(n)} = \xi_D^{(n)}(\varphi^{(n)}, R_{\mathcal{A}} | p_K^n, W^n) := \max_{\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}^{(n)}(R_{\mathcal{A}})} D\left(p_{\widetilde{K}^m | M_{\mathcal{A}}^{(n)}} \middle|\middle| p_{V^m} \middle| p_{M_{\mathcal{A}}^{(n)}}\right).$$

Then we have the following lemma.

Lemma 2. *For any affine encoder $\varphi^{(n)} : \mathcal{X}^n \to \mathcal{X}^m$, we have*

$$\Delta^{(n)}(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)} | p_X^n, p_K^n, W^n) \leq \xi_D^{(n)}(\varphi^{(n)}, R_{\mathcal{A}} | p_K^n, W^n).$$

The quantity $\xi_D^{(n)}(\varphi^{(n)}, R_{\mathcal{A}} | p_K^n, W^n)$ will play an important role in deriving an explicit upper bound of $\Delta^{(n)}(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)} | p_X^n, p_K^n, W^n)$. In Problem 1, we consider the privacy amplification problem using the quantity $\xi_D^{(n)}(\varphi^{(n)}, R_{\mathcal{A}} | p_K^n, W^n)$ as a security criterion. In this problem, we study an explicit characterization of the region denoted by $\mathcal{R}_{\mathrm{P1}}(p_K, W)$, which consists of all pairs $(R, R_{\mathcal{A}})$ such that $\exists \{\varphi^{(n)}\}_{n \geq 1}$ such that $\forall \varepsilon > 0, \exists n_0 = n_0(\varepsilon) \in \mathbb{N}_0, \forall n \geq n_0$,

$$\frac{1}{n} \log ||\varphi^{(n)}|| = \frac{m}{n} \log|\mathcal{X}| \geq R - \varepsilon \text{ and } \xi_D^{(n)}(\varphi^{(n)}, R_{\mathcal{A}} | p_K^n, W^n) \leq \varepsilon.$$

In the next section, we discuss two previous works related to Problem 1.

4. Previous Related Works

In this section, we introduce approaches from previous existing work related to Problem 0 (reliability) and Problem 1 (security). Our goal is that by showing these previous approaches, it will be easier to understand our approach to analyzing reliability and security. In particular, for Problem

1 (security), we explain approaches used in similar problems in previous works and highlight their differences from Problem 1.

We first state a previous result related to Problem 0. Let $\varphi^{(n)}$ be an affine encoder and $\phi^{(n)}$ be a linear encoder induced by $\varphi^{(n)}$. We define a function related to an exponential upper bound of $p_{\mathrm{e}}(\phi^{(n)}, \psi^{(n)}|p_X^n)$. Let $\overline{X}$ be an arbitrary random variable over $\mathcal{X}$ that has a probability distribution $p_{\overline{X}}$. Let $\mathcal{P}(\mathcal{X})$ denote the set of all probability distributions on $\mathcal{X}$. For $R \geq 0$ and $p_X \in \mathcal{P}(\mathcal{X})$, we define the following function:

$$E(R|p_X) := \min_{p_{\overline{X}} \in \mathcal{P}(\mathcal{X})} \{[R - H(\overline{X})]^+ + D(p_{\overline{X}}||p_X)\}.$$

By simple computation, we can prove that $E(R|p_X)$ takes positive values if and only if $R > H(X)$. We have the following result.

Theorem 1 (Csiszár [6]). *There exists a sequence $\{(\phi^{(n)}, \psi^{(n)}\}_{n\geq 1}$ such that for any p_X, we have*

$$\frac{1}{n}\log|\mathcal{X}^m| = \frac{m}{n}\log|\mathcal{X}| \leq R, p_{\mathrm{e}}(\phi^{(n)}, \psi^{(n)}|p_X^n) \leq \mathrm{e}^{-n[E(R|p_X)-\delta_n]}, \tag{9}$$

where δ_n is defined by

$$\delta_n := \frac{1}{n}\log\left[\mathrm{e}(n+1)^{3|\mathcal{X}|}\right].$$

Note that $\delta_n \to 0$ as $n \to \infty$.

It follows from Theorem 1 that if $R > H(X)$, then the error probability of decoding $p_{\mathrm{e}}(\phi^{(n)}, \psi^{(n)}|p_X^n)$ decays exponentially, and its exponent is lower bounded by the quantity $E(R|p_X)$. Furthermore, the code $\{(\phi^{(n)}, \psi^{(n)})\}_{n\geq 1}$ is a universal code that depends only on the rate R and not on the value of $p_X \in \mathcal{P}(\mathcal{X})$.

We next state two coding problems related to Problem 1. One is a problem on the privacy amplification for the bounded storage eavesdropper posed and investigated by Watanabe and Oohama [10]. The other is the one helper source coding problem posed and investigated by Ashlswede and Körner [7] and Wyner [16]. We hereafter call the former and latter problems, respectively, Problem 2 and Problem 3. Problems 1–3 are shown in Figure 6. As we can see from this figure, these three problems are based on the same communication scheme. The classes of encoder functions and the security criteria on $\mathcal{A}$ are different between these three problems. In Problem 1, the sequence of encoding functions $\{\varphi^{(n)}\}_{n\geq 1}$ is restricted to the class of affine encoders to satisfy the homomorphic property. On the other hand, in Problems 2 and 3, we have no such restriction on the class of encoder functions. In descriptions of Problems 2 and 3, we state the difference in security criteria between Problems 1, 2, and 3. A comparison of three problems in terms of $\{\varphi^{(n)}\}_{n\geq 1}$ and security criteria is summarized in Table 1.

In Problem 2, Alice and Bob share a random variable K^n of block length n, and an eavesdropper adversary $\mathcal{A}$ has a random variable Z^n that is correlated to K^n. In such a situation, Alice and Bob try to distill a secret key as long as possible. In [10], they considered a situation such that the adversary's random variable Z^n is stored in a storage that is obtained as a function value of Z^n, and the rate of the storage size is bounded. This situation makes sense when the alphabet size of the adversary's observation Z^n is too huge to be stored directly in a storage. In such a situation, Watanabe and Oohama [10] obtained an explicit characterization of the region $\mathcal{R}_{\mathrm{WO}}(p_K, W)$ indicating the trade-off between the key rate $R = (m/n)\log|\mathcal{X}|$ and the rate $R_{\mathcal{A}} = (1/n)\log|\mathcal{M}_{\mathcal{A}}^{(n)}$ of the storage size.

In Problem 2, the variational distance $d(p_{V^m} \times p_{M_{\mathcal{A}}^{(n)}}, p_{\widetilde{K}^m M_{\mathcal{A}}^{(n)}})$ between $p_{V^m} \times p_{M_{\mathcal{A}}^{(n)}}$ and $p_{\widetilde{K}^m M_{\mathcal{A}}^{(n)}})$ is used as a security criterion instead of $D(p_{\widetilde{K}^m|M_{\mathcal{A}}^{(n)}}||p_{V^m}|p_{M_{\mathcal{A}}^{(n)}})$ in Problem 1. Define

$$\xi_d^{(n)} = \xi_d^{(n)}(\varphi^{(n)}, R_{\mathcal{A}}|p_K^n, W^n) := \max_{\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}^{(n)}(R_{\mathcal{A}})} d(p_{V^m} \times p_{M_{\mathcal{A}}^{(n)}}, p_{\widetilde{K}^m M_{\mathcal{A}}^{(n)}}).$$

Then the formal definition of the region $\mathcal{R}_{\mathrm{WO}}(p_K, W)$ is given by the following:

$$\begin{aligned}\mathcal{R}_{\mathrm{WO}}(p_K, W) := \{(R_{\mathcal{A}}, R) : \exists\{\varphi^{(n)}\}_{n\geq 1} \text{ such that } \forall \varepsilon > 0, \exists n_0 = n_0(\varepsilon) \in \mathbb{N}_0, \forall n \geq n_0,\\ (m/n)\log|\mathcal{X}| \geq R - \varepsilon \text{ and } \xi_d^{(n)}(\varphi^{(n)}, R_{\mathcal{A}}|p_K^n, W^n) \leq \varepsilon\}.\end{aligned}$$

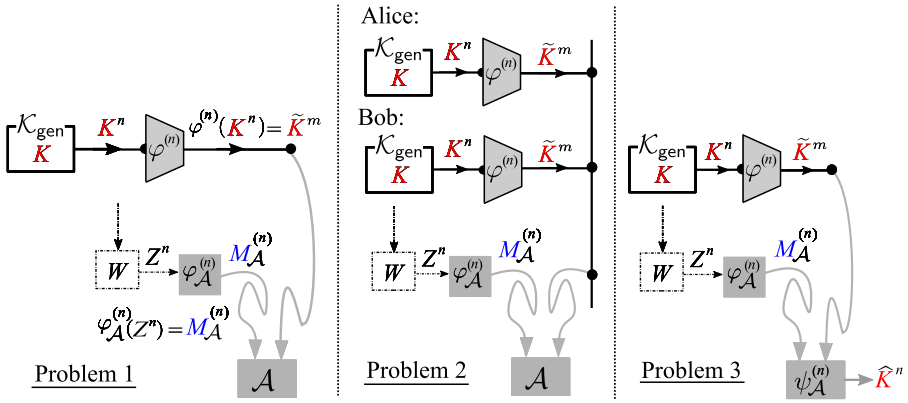

Figure 6. Three related coding problems.

Table 1. Differences between Problems 1, 2, and 3 in terms of $\{\varphi^{(n)}\}_{n\geq 1}$ and security criteria.

	Problem 1	**Problem 2**	**Problem 3**
$\varphi^{(n)}$	affine encoders	general	general
Security Criteria	$D(p_{\widetilde{K}^m\|M_{\mathcal{A}}^{(n)}}\|\|p_{V^m}\|p_{M_{\mathcal{A}}^{(n)}})$	$d(p_{V^m} \times p_{M_{\mathcal{A}}^{(n)}}, p_{\widetilde{K}^m M_{\mathcal{A}}^{(n)}})$	$p_{\mathrm{c},\mathcal{A}}^{(n)}\left(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)}, \psi_{\mathcal{A}}^{(n)} \middle\| p_K^n, W^n\right)$

In Problem 3, the adversary outputs an estimation $\hat{K}^n$ of K^n from $\widetilde{K}^m = \varphi^{(n)}(K^n)$ and $M_{\mathcal{A}}^{(n)} = \varphi_{\mathcal{A}}^{(n)}(Z^n)$. Let $\psi_{\mathcal{A}}^{(n)} : \mathcal{M}^{(n)} \times \mathcal{X}^m$ be a decoder function of the adversary. Then $\widehat{K}^n$ is given by $\widehat{K}^n = \psi_{\mathcal{A}}^{(n)}(\varphi_{\mathcal{A}}^{(n)}(Z^n), \tilde{K}^m = \varphi^{(n)}(K^n)$. Let

$$p_{\mathrm{e},\mathcal{A}}^{(n)} = p_{\mathrm{e},\mathcal{A}}^{(n)}\left(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)}\psi_{\mathcal{A}}^{(n)} \middle| p_K^n, W^n\right) := \Pr\left\{K^n \neq \psi_{\mathcal{A}}^{(n)}(\varphi_{\mathcal{A}}^{(n)}(Z^n), \varphi^{(n)}(K^n))\right\}$$

be the error probability of decoding for Problem 3. The quantity $M_{\mathcal{A}}^{(n)}$ serves as a helper for the decoding of K^n from $\widetilde{K}^m$. In Problem 3, Ahlswede and Körner [7] and Wyner [16] investigated an explicit characterization of the rate region $\mathcal{R}_{\mathrm{AKW}}(p_K, W)$ indicating the trade-off between $R_{\mathcal{A}}$ and R under the condition that $p_{\mathrm{e},\mathcal{A}}^{(n)} = \Pr\{K^n \neq \widehat{K}_n\}$ vanishes asymptotically. The region $\mathcal{R}_{\mathrm{AKW}}(p_K, W)$ is formally defined by

$$\begin{aligned}\mathcal{R}_{\mathrm{AKW}}(p_K, W) := \Big\{&(R_{\mathcal{A}}, R) : \exists\{(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)}, \psi_{\mathcal{A}}^{(n)}\}_{n\geq 1} \text{ such that}\\ &\forall \varepsilon > 0, \exists n_0 = n_0(\varepsilon) \in \mathbb{N}_0, \forall n \geq n_0,\\ &(m/n)\log|\mathcal{X}| \leq R + \varepsilon, \varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}(R + \varepsilon),\\ &\text{and } p_{\mathrm{e},\mathcal{A}}^{(n)}\left(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)}, \psi_{\mathcal{A}}^{(n)} \middle| p_K^n, W^n\right) \leq \varepsilon\Big\}.\end{aligned}$$

The region $\mathcal{R}_{\mathrm{AKW}}(p_K, W)$ was determined by Ashlswede and Körner [7] and Wyner [16]. To state their result, we define several quantities. Let U be an auxiliary random variable taking values in a finite set $\mathcal{U}$. We assume that the joint distribution of (U, Z, K) is

$$p_{UZK}(u,z,k) = p_U(u)p_{Z|U}(z|u)p_{K|Z}(k|z).$$

The above condition is equivalent to $U \leftrightarrow Z \leftrightarrow K$. Define the set of probability distribution $p = p_{UZK}$ by

$$\mathcal{P}(p_K, W) := \{p_{UZK} : |\mathcal{U}| \leq |\mathcal{Z}| + 1, U \leftrightarrow Z \leftrightarrow K\}.$$

Set

$$\begin{aligned} \mathcal{R}(p) &:= \{(R_{\mathcal{A}}, R) : R_{\mathcal{A}}, R \geq 0, R_{\mathcal{A}} \geq I(Z;U), R \geq H(K|U)\}, \\ \mathcal{R}(p_K, W) &:= \bigcup_{p \in \mathcal{P}(p_K, W)} \mathcal{R}(p). \end{aligned}$$

We can show that the region $\mathcal{R}(p_K, W)$ satisfies the following property.

Property 1.

(a) *The region $\mathcal{R}(p_K, W)$ is a closed convex subset of $\mathbb{R}^2_+ := \{R_{\mathcal{A}} \geq 0, R \geq 0\}$.*

(b) *For any (p_K, W), we have*

$$\min_{(R_{\mathcal{A}}, R) \in \mathcal{R}(p_K, W)} (R_{\mathcal{A}} + R) = H(K). \tag{10}$$

The minimum is attained by $(R_{\mathcal{A}}, R) = (0, H(K))$. This result implies that

$$\mathcal{R}(p_K, W) \subseteq \{(R_{\mathcal{A}}, R) : R_{\mathcal{A}} + R \geq H(K)\} \cap \mathbb{R}^2_+.$$

Furthermore, the point $(0, H(K))$ always belongs to $\mathcal{R}(p_K, W)$.

Property 1 part (a) is a well-known property. Proof of Property 1 part (b) is easy. Proofs of Property 1 parts (a) and (b) are omitted. Typical shape of the region $\mathcal{R}(p_K, W)$ is shown in Figure 7.

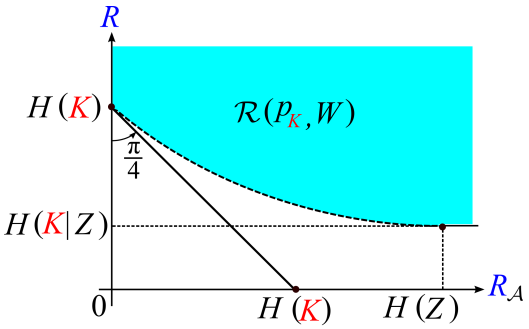

Figure 7. Shape of the region $\mathcal{R}(p_K, W)$.

The rate region $\mathcal{R}_{\mathrm{AKW}}(p_K, W)$ was determined by Ahlswede and Körner [7] and Wyner [16]. Their result is the following.

Theorem 2 (Ahlswede, Körner [7] and Wyner [16])**.**

$$\mathcal{R}_{\mathrm{AKW}}(p_K, W) = \mathcal{R}(p_K, W).$$

Watanabe and Oohama [10] investigated an explicit form of $\mathcal{R}_{\mathrm{WO}}(p_K, W)$ to show that it is equal to $\mathcal{R}^{\mathrm{c}}(p_K, W)$, that is, we have the following result.

Theorem 3 (Watanabe and Oohama [10])**.**

$$\mathcal{R}_{\mathrm{WO}}(p_K, W) = \mathcal{R}^{\mathrm{c}}_{\mathrm{AKW}}(p_K, W) = \mathcal{R}^{\mathrm{c}}(p_K, W).$$

In the remaining part of this section, we investigate a relationship between Problems 2 and 3 to give an outline of the proof of this theorem. Let

$$p^{(n)}_{\mathrm{c},\mathcal{A}} = p^{(n)}_{\mathrm{c},\mathcal{A}}\left(\varphi^{(n)}, \varphi^{(n)}_{\mathcal{A}}, \psi^{(n)}_{\mathcal{A}} \middle| p^n_K, W^n\right) := \Pr\left\{K^n = \psi^{(n)}_{\mathcal{A}}(\varphi^{(n)}_{\mathcal{A}}(Z^n), \varphi^{(n)}(K^n))\right\}$$

be the correct probability of decoding for Problem 3. The following lemma provides an important inequality to examine a relationship between these two problems.

Lemma 3. *For any* $(\varphi^{(n)}, \varphi^{(n)}_{\mathcal{A}}, \psi^{(n)}_{\mathcal{A}})$*, we have the following:*

$$p^{(n)}_{\mathrm{c},\mathcal{A}}\left(\varphi^{(n)}, \varphi^{(n)}_{\mathcal{A}}, \psi^{(n)}_{\mathcal{A}} \middle| p^n_K, W^n\right) \le \frac{1}{|\mathcal{X}|^m} + d\left(p_{V^m} \times p_{M^{(n)}_{\mathcal{A}}}, p_{\widetilde{K}^m M^{(n)}_{\mathcal{A}}}\right).$$

Proof of this lemma is given in Appendix A. Using Lemma 3, we can easily prove the inclusion $\mathcal{R}_{\mathrm{WO}}(p_K, W) \subseteq \mathcal{R}_{\mathrm{AKW}}(p_K, W)$, which corresponds to the converse part of Theorem 3.

Proof of $\mathcal{R}_{\mathrm{WO}}(p_K, W) \subseteq \mathcal{R}^{\mathrm{c}}_{\mathrm{AKW}}(p_K, W)$**:** We assume that $(R_{\mathcal{A}}, R) \in \mathcal{R}_{\mathrm{AKW}}(p_K, W)$. Then there exists $\{(\varphi^{(n)}, \varphi^{(n)}_{\mathcal{A}}, \psi^{(n)}_{\mathcal{A}})\}_{n\ge 1}$ such that $\forall \varepsilon > 0$, $\exists n_0 = n_0(\varepsilon) \in \mathbb{N}_0$, $\forall n \ge n_0$,

$$\frac{m}{n}\log|\mathcal{X}| \le R + \varepsilon, \varphi^{(n)}_{\mathcal{A}} \in \mathcal{F}^{(n)}_{\mathcal{A}}(R+\varepsilon), \tag{11}$$

$$\text{and } p^{(n)}_{\mathrm{e},\mathcal{A}}\left(\varphi^{(n)}, \varphi^{(n)}_{\mathcal{A}}, \psi^{(n)}_{\mathcal{A}} \middle| p^n_K, W^n\right) \le \varepsilon. \tag{12}$$

From the above sequence $\{(\varphi^{(n)}, \varphi^{(n)}_{\mathcal{A}}, \psi^{(n)}_{\mathcal{A}})\}_{n\ge 1}$, we can construct the sequence $\{(\hat{\varphi}^{(n)}, \varphi^{(n)}_{\mathcal{A}}, \psi^{(n)}_{\mathcal{A}}\}_{n\ge 1}$ such that

$$R + \varepsilon \ge \frac{1}{n}\log||\hat{\varphi}^{(n)}|| = \frac{\hat{m}}{n}\log|\mathcal{X}| \ge \max\left\{R-\varepsilon, \frac{m}{n}\log|\mathcal{X}|\right\}, \varphi^{(n)}_{\mathcal{A}} \in \mathcal{F}^{(n)}_{\mathcal{A}}(R+\varepsilon), \tag{13}$$

$$p^{(n)}_{\mathrm{e},\mathcal{A}}\left(\hat{\varphi}^{(n)}, \varphi^{(n)}_{\mathcal{A}}, \psi^{(n)}_{\mathcal{A}} \middle| p^n_K, W^n\right) \le p^{(n)}_{\mathrm{e},\mathcal{A}}\left(\varphi^{(n)}, \varphi^{(n)}_{\mathcal{A}}, \psi^{(n)}_{\mathcal{A}} \middle| p^n_K, W^n\right) \le \varepsilon. \tag{14}$$

Set $\widetilde{K}^{\hat{m}} := \hat{\varphi}^{(n)}(K^n)$. Then from (14) and Lemma 3, we have

$$d\left(p_{V^{\hat{m}}} \times p_{M^{(n)}_{\mathcal{A}}}, p_{\widetilde{K}^{\hat{m}} M^{(n)}_{\mathcal{A}}}\right) \ge 1 - \varepsilon - \frac{1}{|\mathcal{X}|^{\hat{m}}},$$

from which we have

$$d\left(p_{V^{\hat{m}}} \times p_{M^{(n)}_{\mathcal{A}}}, p_{\widetilde{K}^{\hat{m}} M^{(n)}_{\mathcal{A}}}\right) \ge 1 - 2\varepsilon, \tag{15}$$

for sufficiently large n. From (13), (15), and the definition of $\mathcal{R}_{\mathrm{WO}}(p_K, W)$, we can see that $(R_{\mathcal{A}} + \varepsilon, R) \notin \mathcal{R}_{\mathrm{WO}}(p_K, W)$, or equivalent to

$$(R_{\mathcal{A}} + \varepsilon, R) \in \mathcal{R}^{c}_{\mathrm{WO}}(p_K, W) \Leftrightarrow (R_{\mathcal{A}}, R) \in \mathcal{R}^{c}_{\mathrm{WO}}(p_K, W) - \varepsilon(1, 0), \tag{16}$$

where we set $\mathcal{R} - (a,b) := \{(u,v) : (u+a, v+b) \in \mathcal{R}\}$. Since $(R_{\mathcal{A}}, R) \in \mathcal{R}_{\mathrm{AKW}}(p_K, W)$ is arbitrary, we have that

$$\begin{aligned}&\mathcal{R}_{\mathrm{AKW}}(p_K,W) \subseteq \mathcal{R}^c_{\mathrm{WO}}(p_K,W) - \varepsilon(1,0) \Leftrightarrow \mathcal{R}_{\mathrm{AKW}}(p_K,W) + \varepsilon(1,0) \subseteq \mathcal{R}^c_{\mathrm{WO}}(p_K,W)\\ &\Leftrightarrow \mathcal{R}_{\mathrm{WO}}(p_K,W) \subseteq \mathcal{R}^{\mathrm{c}}_{\mathrm{AKW}}(p_K,W) + \varepsilon(1,0) \Leftrightarrow \mathcal{R}_{\mathrm{WO}}(p_K,W) \subseteq \mathcal{R}^{\mathrm{c}}(p_K,W) + \varepsilon(1,0). \end{aligned} \tag{17}$$

By letting $\varepsilon \to 0$ in (17) and considering that $\mathcal{R}^{\mathrm{c}}(p_K, W)$ is an open set, we have that $\mathcal{R}_{\mathrm{WO}}(p_K, W) \subseteq \mathcal{R}^{\mathrm{c}}(p_K, W)$. □

To prove $\mathcal{R}_{\mathrm{WO}}(p_K, W) \supseteq \mathcal{R}^{\mathrm{c}}_{\mathrm{AKW}}$, we examine an upper bound of $\xi_d^{(n)}(\varphi^{(n)}, R_{\mathcal{A}} | p_K^n, W^n)$. For $\eta > 0$, we define

$$\begin{aligned}\wp_\eta^{(n)} = \wp_\eta^{(n)}(R|p_K^n, W^n) &:= p_{M_{\mathcal{A}}^{(n)} Z^n K^n}\left\{ R \geq \frac{1}{n}\log \frac{1}{p_{K^n|M_{\mathcal{A}}^{(n)}}(K^n|M_{\mathcal{A}}^{(n)})} - \eta \right\},\\ \Phi_{d,\eta}^{(n)}(R_{\mathcal{A}}, R|p_K^n W^n) &:= \max_{\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}^{(n)}(\mathcal{R}_{\mathcal{A}})} \left\{ \wp_\eta^{(n)}(R|p_K^n, W^n) + \sqrt{\mathrm{e}^{-n\eta}} \right\}.\end{aligned}$$

According to Watanabe and Oohama [10], we have the following two propositions.

Proposition 1 (Watanabe and Oohama [10]). *Fix any positive $\eta > 0$. $\exists \varphi^{(n)} : \mathcal{X}^n \to \mathcal{X}^m$ satisfying $(m/n)\log|\mathcal{X}| \geq R - 2\eta$, we have*

$$\xi_d^{(n)}(\varphi^{(n)}, R_{\mathcal{A}}|p_K^n, W^n) \leq \Phi_{d,\eta}^{(n)}(R_{\mathcal{A}}, R|p_K^n W^n).$$

Proposition 2 (Watanabe and Oohama [10]). *If $(R_{\mathcal{A}}, R) \notin \mathcal{R}(p_K, W)$, then for any $\eta > 0$ and any $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$, we have*

$$\lim_{n\to\infty} \wp_\eta^{(n)}(R|p_K^n, W) = 0,$$

which implies that

$$\lim_{n\to\infty} \Phi_{d,\eta}^{(n)}(R_{\mathcal{A}}, R|p_K^n W^n) = 0.$$

The inclusion $\mathcal{R}_{\mathrm{WO}}(p_K, W) \supseteq \mathcal{R}^{\mathrm{c}}_{\mathrm{AKW}}$ immediately follows from Propositions 1 and 2.

5. Reliability and Security Analysis

In this section, we state our main results. We use the affine encoder $\varphi^{(n)}$ defined in the previous section. We upper bound $p_{\mathrm{e}} = p_{\mathrm{e}}(\varphi^{(n)}, \psi^{(n)}|p_X^n)$ and $\Delta^{(n)} = \Delta^{(n)}(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)}|p_X^n, p_K^n, W^n)$ to obtain inner bounds of $\mathcal{R}_{\mathsf{Sys}}(p_X, p_K, W)$ and $\mathcal{D}_{\mathsf{Sys}}(p_X, p_K, W)$.

Let

$$\begin{aligned}\Phi_{D,\eta}^{(n)}(R_{\mathcal{A}}, R|p_K^n W^n) &:= \max_{\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}^{(n)}(\mathcal{R}_{\mathcal{A}})} \left\{ nR\wp_\eta^{(n)}(R|p_K^n, W^n) + \mathrm{e}^{-n\eta} \right\},\\ \Phi_D^{(n)}(R_{\mathcal{A}}, R|p_K^n W^n) &:= \inf_{\eta>0} \Phi_{D,\eta}(R_{\mathcal{A}}, R|p_K^n W^n).\end{aligned}$$

Then we have the following proposition.

Proposition 3. *For any $R_{\mathcal{A}}, R > 0$ and any (p_K, W), there exists a sequence of mappings $\{(\varphi^{(n)}, \psi^{(n)})\}_{n=1}^{\infty}$ such that for any $p_X \in \mathcal{P}(\mathcal{X})$, we have*

$$\begin{aligned} &R - \frac{1}{n} \le \frac{1}{n} \log |\mathcal{X}^m| = \frac{m}{n} \log |\mathcal{X}| \le R, \\ &p_{\mathrm{e}}(\phi^{(n)}, \psi^{(n)} | p_X^n) \le \mathrm{e}(n+1)^{2|\mathcal{X}|} \{(n+1)^{|\mathcal{X}|} + 1\} \mathrm{e}^{-nE(R|p_X)}, \end{aligned} \tag{18}$$

and for any eavesdropper $\mathcal{A}$ with $\varphi_{\mathcal{A}}$ satisfying $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$, we have

$$\Delta^{(n)}(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)} | p_X^n, p_K^n, W^n) \le \{(n+1)^{|\mathcal{X}|} + 1\} \Phi_D^{(n)}(R_{\mathcal{A}}, R | p_K^n W^n). \tag{19}$$

This proposition can be proved by several tools developed by previous works. The detail of the proof is given in the next section. As we stated in Proposition 2, Watanabe and Oohama [10] proved that if $(R_{\mathcal{A}}, R) \notin \mathcal{R}(p_K, W)$, then the quantity for any $\eta > 0$ and any $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$, the quantity $\wp_{\eta}^{(n)}(R | p_K^n, W)$. Their method can not be applied to the analysis of $\Phi_D^{(n)}(R_{\mathcal{A}}, R | p_K^n W^n)$ since the quantity nR is multiplied with the quantity $\wp_{\eta}^{(n)}(R | p_K^n, W)$ in the definition of $\Phi_D^{(n)}(R_{\mathcal{A}}, R | p_K^n W^n)$. In this paper, we derive an upper bound of $\Phi_D^{(n)}(R_{\mathcal{A}}, R | p_K^n W^n)$ that decays exponentially as $n \to \infty$ if $(R_{\mathcal{A}}, R) \notin \mathcal{R}(p_K, W)$. To derive the upper bound, we use a new method that is developed by Oohama to prove strong converse theorems in multi-terminal source or channel networks [9,17–20].

We define several functions and sets to describe the upper bound of $\Phi_D^{(n)}(R_{\mathcal{A}}, R | p_K^n W^n)$. Set

$$\mathcal{Q}(p_{K|Z}) := \{q = q_{UZK} : |\mathcal{U}| \le |\mathcal{Z}|, U \leftrightarrow Z \leftrightarrow K, p_{K|Z} = q_{K|Z}\}.$$

For $(\mu, \alpha) \in [0,1]^2$ and for $q = q_{UZK} \in \mathcal{Q}(p_{K|Z})$, define

$$\begin{aligned} &\omega_{q|p_Z}^{(\mu,\alpha)}(z,k|u) := \bar{\alpha} \log \frac{q_Z(z)}{p_Z(z)} + \alpha \left[\mu \log \frac{q_{Z|U}(z|u)}{p_Z(z)} + \bar{\mu} \log \frac{1}{q_{K|U}(k|u)} \right], \\ &\Omega^{(\mu,\alpha)}(q|p_Z) := -\log \mathrm{E}_q \left[\exp \left\{ -\omega_{q|p_Z}^{(\mu,\alpha)}(Z,K|U) \right\} \right], \Omega^{(\mu,\alpha)}(p_K, W) := \min_{q \in \mathcal{Q}(p_{K|Z})} \Omega^{(\mu,\alpha)}(q|p_Z), \\ &F^{(\mu,\alpha)}(\mu R_{\mathcal{A}} + \bar{\mu} R | p_K, W) := \frac{\Omega^{(\mu,\alpha)}(p_K, W) - \alpha(\mu R_{\mathcal{A}} + \bar{\mu} R)}{2 + \alpha\bar{\mu}}, \\ &F(R_{\mathcal{A}}, R | p_K, W) := \sup_{(\mu,\alpha) \in [0,1]^2} F^{(\mu,\alpha)}(\mu R_{\mathcal{A}} + \bar{\mu} R | p_K, W). \end{aligned}$$

We next define a function serving as a lower bound of $F(R_{\mathcal{A}}, R | p_K, W)$. For each $p_{UZK} \in \mathcal{P}_{\mathrm{sh}}(p_K, W)$, define

$$\begin{aligned} &\tilde{\omega}_p^{(\mu)}(z,k|u) := \mu \log \frac{p_{Z|U}(z|u)}{p_Z(z)} + \bar{\mu} \log \frac{1}{p_{K|U}(K|U)}, \\ &\tilde{\Omega}^{(\mu,\lambda)}(p) := -\log \mathrm{E}_p \left[\exp \left\{ -\lambda \tilde{\omega}_p^{(\mu)}(Z,K|U) \right\} \right], \tilde{\Omega}^{(\mu,\lambda)}(p_K, W) := \min_{p \in \mathcal{P}_{\mathrm{sh}}(p_K, W)} \tilde{\Omega}^{(\mu,\lambda)}(p). \end{aligned}$$

Furthermore, set

$$\begin{aligned} &\tilde{F}^{(\mu,\lambda)}(\mu R_{\mathcal{A}} + \bar{\mu} R | p_K, W) := \frac{\tilde{\Omega}^{(\mu,\lambda)}(p_K, W) - \lambda(\mu R_{\mathcal{A}} + R)}{2 + \lambda(5 - \mu)}, \\ &\tilde{F}(R_{\mathcal{A}}, R | p_K, W) := \sup_{\substack{\lambda \ge 0, \\ \mu \in [0,1]}} \tilde{F}^{(\mu,\lambda)}(\mu R_{\mathcal{A}} + \bar{\mu} R | p_K, W). \end{aligned}$$

We can show that the above functions satisfy the following property.

Property 2.

(a) *The cardinality bound $|\mathcal{U}| \leq |\mathcal{Z}|$ in $\mathcal{Q}(p_{K|Z})$ is sufficient to describe the quantity $\Omega^{(\mu,\beta,\alpha)}(p_K, W)$. Furthermore, the cardinality bound $|\mathcal{U}| \leq |\mathcal{Z}|$ in $\mathcal{P}_{\mathrm{sh}}(p_K, W)$ is sufficient to describe the quantity $\tilde{\Omega}^{(\mu,\lambda)}(p_K, W)$.*

(b) *For any $R_{\mathcal{A}}, R \geq 0$, we have*

$$F(R_{\mathcal{A}}, R|p_K, W) \geq \tilde{F}(R_{\mathcal{A}}, R|p_K, W).$$

(c) *For any $p = p_{UZK} \in \mathcal{P}_{\mathrm{sh}}(p_Z, W)$ and any $(\mu, \lambda) \in [0,1]^2$, we have*

$$0 \leq \tilde{\Omega}^{(\mu,\lambda)}(p) \leq \mu \log |\mathcal{Z}| + \bar{\mu} \log |\mathcal{K}|. \tag{20}$$

(d) *Fix any $p = p_{UZK} \in \mathcal{P}_{\mathrm{sh}}(p_K, W)$ and $\mu \in [0,1]$. For $\lambda \in [0,1]$, we define a probability distribution $p^{(\lambda)} = p^{(\lambda)}_{UZK}$ by*

$$p^{(\lambda)}(u,z,k) := \frac{p(u,z,k) \exp\left\{-\lambda \tilde{\omega}^{(\mu)}_p(z,k|u)\right\}}{\mathrm{E}_p\left[\exp\left\{-\lambda \tilde{\omega}^{(\mu)}_p(Z,K|U)\right\}\right]}.$$

Then for $\lambda \in [0, 1/2]$, $\tilde{\Omega}^{(\mu,\lambda)}(p)$ is twice differentiable. Furthermore, for $\lambda \in [0, 1/2]$, we have

$$\frac{\mathrm{d}}{\mathrm{d}\lambda}\tilde{\Omega}^{(\mu,\lambda)}(p) = \mathrm{E}_{p^{(\lambda)}}\left[\tilde{\omega}^{(\mu)}_p(Z,K|U)\right], \ \frac{\mathrm{d}^2}{\mathrm{d}\lambda^2}\tilde{\Omega}^{(\mu,\lambda)}(p) = -\mathrm{Var}_{p^{(\lambda)}}\left[\tilde{\omega}^{(\mu)}_p(Z,K|U)\right].$$

The second equality implies that $\tilde{\Omega}^{(\mu,\lambda)}(p|p_K, W)$ is a concave function of $\lambda \geq 0$.

(e) *For $(\mu, \lambda) \in [0,1] \times [0, 1/2]$, define*

$$\rho^{(\mu,\lambda)}(p_K, W) := \max_{\substack{(\nu,p) \in [0,\lambda] \times \mathcal{P}_{\mathrm{sh}}(p_K,W): \\ \tilde{\Omega}^{(\mu,\lambda)}(p) = \tilde{\Omega}^{(\mu,\lambda)}(p_K,W)}} \mathrm{Var}_{p^{(\nu)}}\left[\tilde{\omega}^{(\mu)}_p(Z,K|U)\right],$$

and set

$$\rho = \rho(p_K, W) := \max_{(\mu,\lambda) \in [0,1] \times [0,1/2]} \rho^{(\mu,\lambda)}(p_K, W).$$

Then we have $\rho(p_K, W) < \infty$. Furthermore, for any $(\mu, \lambda) \in [0,1] \times [0, 1/2]$, we have

$$\tilde{\Omega}^{(\mu,\lambda)}(p_K, W) \geq \lambda R^{(\mu)}(p_K, W) - \frac{\lambda^2}{2}\rho(p_K, W).$$

(f) *For every $\tau \in (0, (1/2)\rho(p_K, W))$, the condition $(R_{\mathcal{A}}, R + \tau) \notin \mathcal{R}(p_K, W)$ implies*

$$\tilde{F}(R_{\mathcal{A}}, R|p_K, W) > \tfrac{\rho(p_K,W)}{4} \cdot g^2\left(\tfrac{\tau}{\rho(p_K,W)}\right) > 0,$$

where g is the inverse function of $\vartheta(a) := a + (5/4)a^2, a \ \geq 0$.

Proof of this property is found in Oohama [9] (extended version). On the upper bound of $\Phi^{(n)}_D(R_{\mathcal{A}}, R|p^n_K W^n)$, we have the following:

Proposition 4. *For any $n \geq 1/R$, we have*

$$\Phi^{(n)}_D(R_{\mathcal{A}}, R|p^n_K W^n) \leq 5nR\mathrm{e}^{-nF(R_{\mathcal{A}},R|p_K,W)}. \tag{21}$$

Proof of this proposition is given in the next section. Proposition 4 has a close connection with the one helper source coding problem, which is explained as Problem 3 in the previous section. In fact, for the proof we use the result Oohama [9] obtained for an explicit lower bound of the optimal exponent on the exponential decay of $p_{\mathrm{c},\mathcal{A}}^{(n)}\left(\varphi^{(n)},\varphi_{\mathcal{A}}^{(n)},\psi_{\mathcal{A}}^{(n)}\middle|p_K^n,W^n\right)$ for $(R_{\mathcal{A}},R)\notin\mathcal{R}_{\mathrm{AKW}}(p_K,W)$. By Propositions 3 and 4, we obtain our main result shown below.

Theorem 4. For any $R_{\mathcal{A}},R>0$ and any (p_K,W), there exists a sequence of mappings $\{(\varphi^{(n)},\psi^{(n)})\}_{n=1}^{\infty}$ such that for any $p_X\in\mathcal{P}(\mathcal{X})$, we have

$$\begin{aligned}&\frac{1}{n}-R\le\frac{1}{n}\log|\mathcal{X}^m|=\frac{m}{n}\log|\mathcal{X}|\le R,\\&p_{\mathrm{e}}(\phi^{(n)},\psi^{(n)}|p_X^n)\le\mathrm{e}^{-n[E(R|p_X)-\delta_{1,n}]}\end{aligned}\tag{22}$$

and for any eavesdropper $\mathcal{A}$ with $\varphi_{\mathcal{A}}$ satisfying $\varphi_{\mathcal{A}}^{(n)}\in\mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$, we have

$$\Delta^{(n)}(\varphi^{(n)},\varphi_{\mathcal{A}}^{(n)}|p_X^n,p_K^n,W^n)\le\mathrm{e}^{-n[F(R_{\mathcal{A}},R|p_K,W)-\delta_{2,n}]},\tag{23}$$

where $\delta_{i,n},i=1,2$ are defined by

$$\begin{aligned}\delta_{1,n}&:=\frac{1}{n}\log\left[\mathrm{e}(n+1)^{2|\mathcal{X}|}\{(n+1)^{|\mathcal{X}|}+1\}\right],\\\delta_{2,n}&:=\frac{1}{n}\log\left[5nR\{(n+1)^{|\mathcal{X}|}+1\}\right].\end{aligned}$$

Note that for $i=1,2$, $\delta_{i,n}\to0$ as $n\to\infty$.

The functions $E(R|p_X)$ and $F(R_{\mathcal{A}},R|p_K,W)$ take positive values if and only if $(R_{\mathcal{A}},R)$ belongs to the set

$$\{R>H(X)\}\cap\mathcal{R}^{\mathrm{c}}(p_K,W):=\mathcal{R}_{\mathrm{Sys}}^{(\mathrm{in})}(p_X,p_K,W).$$

Thus, by Theorem 4, under $(R_{\mathcal{A}},R)\in\mathcal{R}_{\mathrm{Sys}}^{(\mathrm{in})}(p_X,p_K,W)$, we have the following::

- In terms of reliability, $p_{\mathrm{e}}(\phi^{(n)},\psi^{(n)}|p_X^n)$ goes to zero exponentially as n tends to infinity, and its exponent is lower bounded by the function $E(R|p_X)$.
- In terms of security, for any $\varphi_{\mathcal{A}}$ satisfying $\varphi_{\mathcal{A}}^{(n)}\in\mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$, the information leakage $\Delta^{(n)}(\varphi^{(n)},\varphi_{\mathcal{A}}^{(n)}|p_X^n,p_K^n,W^n)$ on X^n goes to zero exponentially as n tends to infinity, and its exponent is lower bounded by the function $F(R_{\mathcal{A}},R|p_K,W)$.
- The code that attains the exponent functions $E(R|p_X)$ is the universal code that depends only on R and not on the value of the distribution p_X.

Define

$$\mathcal{D}_{\mathrm{Sys}}^{(\mathrm{in})}(p_X,p_K,W):=\{(R_1,R_2,E(R|p_X),F(R_{\mathcal{A}},R|p_K)):(R_1,R_2)\in\mathcal{R}_{\mathrm{Sys}}^{(\mathrm{in})}(p_X,p_K,W)\}.$$

From Theorem 4, we immediately obtain the following corollary.

Corollary 1.

$$\mathcal{R}_{\mathrm{Sys}}^{(\mathrm{in})}(p_X,p_K,W)\subseteq\mathcal{R}_{\mathrm{Sys}}(p_X,p_K,W),\mathcal{D}_{\mathrm{Sys}}^{(\mathrm{in})}(p_X,p_K,W)\subseteq\mathcal{D}_{\mathrm{Sys}}(p_X,p_K,W).$$

A typical shape of $\{R>H(X)\}\cap\mathcal{R}^{\mathrm{c}}(p_K,W)$ is shown in Figure 8.

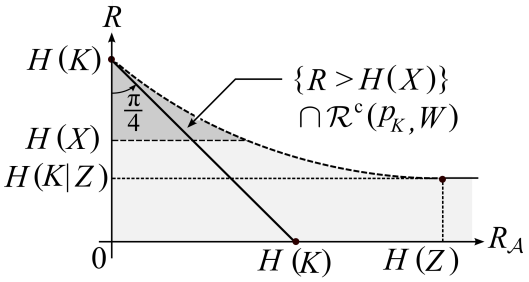

Figure 8. The inner bound $\mathcal{R}_{\mathrm{Sys}}^{(\mathrm{in})}(p_X, p_K, W)$ of the reliable and secure rate region $\mathcal{R}_{\mathrm{Sys}}(p_X, p_K\, W)$.

6. Proofs of the Results

In this section, we prove our main theorem, i.e., Theorem 4.

6.1. Types of Sequences and Their Properties

In this subsection, we present basic results on the types. These results are basic tools for our analysis of several bounds related to the error provability of decoding or security.

Definition 5. For any n-sequence $x^n = x_1 x_2 \cdots x_n \in \mathcal{X}^n$, $n(x|x^n)$ denotes the number of t such that $x_t = x$. The relative frequency $\{n(x|x^n)/n\}_{x\in\mathcal{X}}$ of the components of x^n is called the type of x^n denoted by P_{x^n}. The set that consists of all the types on $\mathcal{X}$ is denoted by $\mathcal{P}_n(\mathcal{X})$. Let $\overline{X}$ denote an arbitrary random variable whose distribution $P_{\overline{X}}$ belongs to $\mathcal{P}_n(\mathcal{X})$. For $p_{\overline{X}} \in \mathcal{P}_n(\mathcal{X})$, set $T^n_{\overline{X}} := \left\{x^n : P_{x^n} = p_{\overline{X}}\right\}$.

For sets of types and joint types, the following lemma holds. For details of the proof, see Csiszár and Körner [21].

Lemma 4.

(a) $|\mathcal{P}_n(\mathcal{X})| \le (n+1)^{|\mathcal{X}|}$.

(b) For $P_{\overline{X}} \in \mathcal{P}_n(\mathcal{X})$,

$$(n+1)^{-|\mathcal{X}|}\mathrm{e}^{nH(\overline{X})} \le |T^n_{\overline{X}}| \le \mathrm{e}^{nH(\overline{X})}.$$

(c) For $x^n \in T^n_{\overline{X}}$,

$$p^n_X(x^n) = \mathrm{e}^{-n[H(\overline{X})+D(p_{\overline{X}}||p_X)]}.$$

By Lemma 4 parts (b) and (c), we immediately obtain the following lemma:

Lemma 5. For $p_{\overline{X}} \in \mathcal{P}_n(\mathcal{X})$,

$$p^n_X(T^n_{\overline{X}}) \le \mathrm{e}^{-nD(p_{\overline{X}}||p_X)}.$$

6.2. Upper Bounds of $p_{\mathrm{e}}(\phi^{(n)}, \psi^{(n)}|p^n_X)$, and $\Delta_n(\varphi^{(n)}, \varphi^{(n)}_{\mathcal{A}}|p^n_X, p^n_K, W^n)$

In this subsection, we evaluate upper bounds of $p_{\mathrm{e}}(\phi^{(n)}, \psi^{(n)}|p^n_X)$ and $\Delta_n(\varphi^{(n)}, \varphi^{(n)}_{\mathcal{A}}|p^n_X, p^n_K, W^n)$. For $p_{\mathrm{e}}(\phi^{(n)}, \psi^{(n)}|p^n_X)$, we derive an upper bound that can be characterized with a quantity depending

on $(\phi^{(n)}, \psi^{(n)})$ and type P_{x^n} of sequences $x^n \in \mathcal{X}^n$. We first evaluate $p_{\mathrm{e}}(\phi^{(n)}, \psi^{(n)}|p_X^n)$. For $x^n \in \mathcal{X}^n$ and $p_{\overline{X}} \in \mathcal{P}_n(\mathcal{X})$, we define the following functions:

$$\Xi_{x^n}(\phi^{(n)}, \psi^{(n)}) := \begin{cases} 1 & \text{if} \quad \psi^{(n)}\big(\phi^{(n)}(x^n)\big) \neq x^n, \\ 0 & \text{otherwise,} \end{cases}$$

$$\Xi_{\overline{X}}(\phi^{(n)}, \psi^{(n)}) := \frac{1}{|T^n_{\overline{X}}|} \sum_{x^n \in T^n_{\overline{X}}} \Xi_{x^n}(\phi^{(n)}, \psi^{(n)}).$$

Then we have the following lemma.

Lemma 6. *In the proposed system, for any pair of* $(\phi^{(n)}, \psi^{(n)})$*, we have*

$$p_{\mathrm{e}}(\phi^{(n)}, \psi^{(n)}|p_X^n) \leq \sum_{p_{\overline{X}} \in \mathcal{P}_n(\mathcal{X})} \Xi_{\overline{X}}(\phi^{(n)}, \psi^{(n)}) \mathrm{e}^{-nD(p_{\overline{X}}||p_X)}. \tag{24}$$

Proof. We have the following chain of inequalities:

$$\begin{aligned} p_{\mathrm{e}}(\phi^{(n)}, \psi^{(n)}|p_X^n) &\overset{\text{(a)}}{=} \sum_{p_{\overline{X}} \in \mathcal{P}_n(\mathcal{X})} \sum_{x^n \in T^n_{\overline{X}}} \Xi_{x^n}(\phi^{(n)}, \psi^{(n)}) p_X^n(x^n) \\ &= \sum_{p_{\overline{X}} \in \mathcal{P}_n(\mathcal{X})} \frac{1}{|T^n_{\overline{X}}|} \sum_{x^n \in T^n_{\overline{X}}} \Xi_{x^n}(\phi^{(n)}, \psi^{(n)}) |T^n_{\overline{X}}| p_X^n(x^n) \\ &\overset{\text{(b)}}{=} \sum_{p_{\overline{X}} \in \mathcal{P}_n(\mathcal{X})} \frac{1}{|T^n_{\overline{X}}|} \sum_{x^n \in T^n_{\overline{X}}} \Xi_{x^n}(\phi^{(n)}, \psi^{(n)}) p_X^n(T^n_{\overline{X}}) \overset{\text{(c)}}{=} \sum_{p_{\overline{X}} \in \mathcal{P}_n(\mathcal{X})} \Xi_{\overline{X}}(\phi^{(n)}, \psi^{(n)}) p_X^n(T^n_{\overline{X}}) \\ &\overset{\text{(d)}}{\leq} \sum_{p_{\overline{X}} \in \mathcal{P}_n(\mathcal{X})} \Xi_{\overline{X}}(\phi^{(n)}, \psi^{(n)}) \mathrm{e}^{-nD(p_{\overline{X}}||p_X)}. \end{aligned}$$

Step (a) follows from the definition of $\Xi_{x^n}(\phi^{(n)}, \psi^{(n)})$. Step (b) follows from the probabilities $p_X^n(x^n)$ for $x^n \in T^n_{\overline{X}}$ taking an identical value. Step (c) follows from the definition of $\Xi_{\overline{X}}(\phi^{(n)}, \psi^{(n)})$. Step (d) follows from Lemma 5. □

6.3. Random Coding Arguments

We construct a pair of affine encoders $\varphi^{(n)} = (\varphi_1^{(n)}, \varphi_{\mathrm{e}}^{(n)})$ using the random coding method. For the joint decoder $\psi^{(n)}$, we propose the minimum entropy decoder used in Csiszár [6] and Oohama and Han [22].

Random Construction of Affine Encoders: We first choose m such that

$$m := \left\lfloor \frac{nR}{\log|\mathcal{X}|} \right\rfloor,$$

where $\lfloor a \rfloor$ stands for the integer part of a. It is obvious that

$$R - \frac{1}{n} \leq \frac{m}{n} \log|\mathcal{X}| \leq R.$$

By definition (2) of $\phi^{(n)}$, we have that for $x^n \in \mathcal{X}^n$,

$$\phi^{(n)}(x^n) = x^n A,$$

where A is a matrix with n rows and m columns. By definition (3) of $\varphi^{(n)}$, we have that for $k^n \in \mathcal{X}^n$,

$$\varphi^{(n)}(k^n) = k^n A + b^m,$$

where b^m is a vector with m columns. Entries of A and b^m are from the field of $\mathcal{X}$. These entries are selected at random, independently of each other, and with a uniform distribution. Randomly constructed linear encoder $\phi^{(n)}$ and affine encoder $\varphi^{(n)}$ have three properties shown in the following lemma.

Lemma 7 (Properties of Linear/Affine Encoders)**.**

(a) *For any $x^n, v^n \in \mathcal{X}^n$ with $x^n \neq v^n$, we have*

$$\Pr[\phi^{(n)}(x^n) = \phi^{(n)}(v^n)] = \Pr[(x^n \ominus v^n)A = 0^m] = |\mathcal{X}|^{-m}. \tag{25}$$

(b) *For any $s^n \in \mathcal{X}^n$ and for any $\widetilde{s}^m \in \mathcal{X}^m$, we have*

$$\Pr[\varphi^{(n)}(s^n) = \widetilde{s}^m] = \Pr[s^n A \oplus b^m = \widetilde{s}^m] = |\mathcal{X}|^{-m}. \tag{26}$$

(c) *For any $s^n, t^n \in \mathcal{X}^n$ with $s^n \neq t^n$, and for any $\widetilde{s}^m \in \mathcal{X}^m$, we have*

$$\Pr[\varphi^{(n)}(s^n) = \varphi^{(n)}(t^n) = \widetilde{s}^m] = \Pr[s^n A \oplus b^m = t^n A \oplus b^m = \widetilde{s}^m] = |\mathcal{X}|^{-2m}. \tag{27}$$

Proof of this lemma is given in Appendix B. We next define the decoder function $\psi^{(n)} : \mathcal{X}^m \to \mathcal{X}^n$. To this end, we define the following quantities.

Definition 6. For $x^n \in \mathcal{X}^n$, we denote the entropy calculated from the type P_{x^n} by $H(x^n)$. In other words, for a type $P_{\overline{X}} \in \mathcal{P}_n(\mathcal{X})$ such that $P_{\overline{X}} = P_{x^n}$, we define $H(x^n) = H(\overline{X})$.

Minimum Entropy Decoder: For $\phi^{(n)}(x^n) = \widetilde{x}^m$, we define the decoder function $\psi^{(n)} : \mathcal{X}^m \to \mathcal{X}^n$ as follows:

$$\psi^{(n)}(\widetilde{x}^m) := \begin{cases} \widehat{x}^n & \text{if } \phi^{(n)}(\widehat{x}^n) = \widetilde{x}^m, \\ & \text{and } H(\widehat{x}^n) < H(\check{x}^n) \\ & \text{for all } \check{x}^n \text{ such that} \\ & \phi^{(n)}(\check{x}^n) = \widetilde{x}^m, \\ & \text{and } \check{x}^n \neq \widehat{x}^n, \\ \text{arbitrary} & \text{if there is no such } \widehat{x}^n \in \mathcal{X}^n. \end{cases}$$

Error Probability Bound: In the following arguments, we let expectations based on the random choice of the affine encoder $\varphi^{(n)}$ be denoted by $\mathbf{E}[\cdot]$. Define

$$\Lambda_{\overline{X}}(R) := \mathrm{e}^{-n[R - H(\overline{X})]^+}.$$

Then we have the following lemma.

Lemma 8. *For any n and for any $P_{\overline{X}} \in \mathcal{P}_n(\mathcal{X})$,*

$$\mathbf{E}\left[\Xi_{\overline{X}}(\phi^{(n)}, \psi^{(n)})\right] \leq \mathrm{e}(n+1)^{|\mathcal{X}|}\Lambda_{\overline{X}}(R).$$

Proof of this lemma is given in Appendix C.

Estimation of Approximation Error: Define

$$\Theta(R, \varphi_{\mathcal{A}}^{(n)} | p_{K^n}, W^n) := \sum_{(a,k^n) \in \mathcal{M}_{\mathcal{A}}^{(n)} \times \mathcal{X}^n} p_{M_{\mathcal{A}}^{(n)} K^n}(a, k^n) \log \left[1 + (\mathrm{e}^{nR} - 1) p_{K^n | M_{\mathcal{A}}^{(n)}}(k^n | a) \right].$$

Then we have the following lemma.

Lemma 9. *For any n, m satisfying $(m/n) \log |\mathcal{X}| \leq R$, we have*

$$\mathbf{E}\left[D\left(p_{\tilde{K}^m | M_{\mathcal{A}}^{(n)}} \middle\| p_{V^m} \middle| p_{M_{\mathcal{A}}^{(n)}} \right) \right] \leq \Theta(R, \varphi_{\mathcal{A}}^{(n)} | p_{K^n}, W^n). \tag{28}$$

Proof of this lemma is given in Appendix D. From the bound (28) in Lemma (9), we know that the quantity $\Theta(R, \varphi_{\mathcal{A}}^{(n)} | p_{K^n}, W^n)$ serves as an upper bound of the ensemble average of the conditional divergence $D(p_{\tilde{K}^m | M_{\mathcal{A}}^{(n)}} || p_{V^m} | p_{M_{\mathcal{A}}^{(n)}})$. Hayashi [23] obtained the same upper bound of the ensemble average of the conditional divergence for an ensemble of universal$_2$ functions. In this paper, we prove the bound (28) for an ensemble of affine encoders. To derive this bound, we need to use Lemma 7 parts (b) and (c), the two important properties that a class of random affine encoders satisfies. From Lemmas 1 and 9, we have the following corollary.

Corollary 2.

$$\mathbf{E}\left[\Delta_n(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)} | p_X^n, p_K^n, W^n) \right] \leq \Theta(R, \varphi_{\mathcal{A}}^{(n)} | p_K^n, W^n).$$

Existence of Good Universal Code $(\varphi^{(n)}, \psi^{(n)})$:

From Lemma 8 and Corollary 2, we have the following lemma stating the existence of a good universal code $(\varphi^{(n)}, \psi^{(n)})$.

Lemma 10. *There exists at least one deterministic code $(\varphi^{(n)}, \psi^{(n)})$ satisfying $(m/n) \log |\mathcal{X}| \leq R$, such that for any $p_{\overline{X}} \in \mathcal{P}_n(\mathcal{X})$,*

$$\Xi_{\overline{X}}(\phi^{(n)}, \psi^{(n)}) \leq \mathrm{e}(n+1)^{|\mathcal{X}|} \{(n+1)^{|\mathcal{X}|} + 1\} \Lambda_{\overline{X}}(R).$$

Furthermore, for any $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$, we have

$$\Delta_n(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)} | p_X^n, p_K^n, W^n) \leq \{(n+1)^{|\mathcal{X}|} + 1\} \Theta(R, \varphi_{\mathcal{A}}^{(n)} | p_K^n, W^n).$$

Proof. We have the following chain of inequalities:

$$\begin{aligned}
&\mathbf{E}\left[\sum_{p_{\overline{X}} \in \mathcal{P}_n(\mathcal{X})} \frac{\Xi_{\overline{X}}(\phi^{(n)}, \psi^{(n)})}{\mathrm{e}(n+1)^{|\mathcal{X}|} \Lambda_{\overline{X}}(R)} + \frac{\Delta_n(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)} | p_X^n, p_K^n, W^n)}{\Theta(R, \varphi_{\mathcal{A}}^{(n)} | p_K^n, W^n)} \right] \\
&= \sum_{p_{\overline{X}} \in \mathcal{P}_n(\mathcal{X})} \frac{\mathbf{E}\left[\Xi_{\overline{X}}(\phi^{(n)}, \psi^{(n)}) \right]}{\mathrm{e}(n+1)^{|\mathcal{X}|} \Lambda_{\overline{X}}(R)} + \frac{\mathbf{E}\left[\Delta_n(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)} | p_X^n, p_K^n, W^n) \right]}{\Theta(R, \varphi_{\mathcal{A}}^{(n)} | p_K^n, W^n)} \\
&\overset{(a)}{\leq} \sum_{p_{\overline{X}} \in \mathcal{P}_n(\mathcal{X})} 1 + 1 = |\mathcal{P}_n(\mathcal{X})| + 1 \overset{(b)}{\leq} (n+1)^{|\mathcal{X}|} + 1.
\end{aligned}$$

Step (a) follows from Lemma 8 and Corollary 2. Step (b) follows from Lemma 4 part (a). Hence, there exists at least one deterministic code $(\varphi^{(n)}, \psi^{(n)})$ such that

$$\sum_{p_{\overline{X}} \in \mathcal{P}_n(\mathcal{X})} \frac{\Xi_{\overline{X}}(\phi^{(n)}, \psi^{(n)})}{\mathrm{e}(n+1)^{|\mathcal{X}|}\Lambda_{\overline{X}}(R)} + \frac{\Delta_n(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)}|p_X^n, p_K^n, W^n)}{\Theta(R, \varphi_{\mathcal{A}}^{(n)}|p_K^n, W^n)} \leq (n+1)^{|\mathcal{X}|} + 1,$$

from which we have that

$$\frac{\Xi_{\overline{X}}(\phi^{(n)}, \psi^{(n)})}{\mathrm{e}(n+1)^{|\mathcal{X}|}\Lambda_{\overline{X}}(R)} \leq (n+1)^{|\mathcal{X}|} + 1,$$

for any $p_{\overline{X}} \in \mathcal{P}_n(\mathcal{X})$. Furthermore, we have that for any $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$,

$$\frac{\Delta_n(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)}|p_X^n, p_K^n, W^n)}{\Theta(R, \varphi_{\mathcal{A}}^{(n)}|p_K^n, W^n)} \leq (n+1)^{|\mathcal{X}|} + 1,$$

completing the proof. □

Proposition 5. *For any $R_{\mathcal{A}}, R > 0$ and any (p_K, W), there exists a sequence of mappings $\{(\varphi^{(n)}, \psi^{(n)})\}_{n=1}^{\infty}$ such that for any $p_X \in \mathcal{P}(\mathcal{X})$, we have*

$$\begin{aligned} &R - \frac{1}{n} \leq \frac{1}{n}\log|\mathcal{X}^m| = \frac{m}{n}\log|\mathcal{X}| \leq R, \\ &p_{\mathrm{e}}(\phi^{(n)}, \psi^{(n)}|p_X^n) \leq \mathrm{e}(n+1)^{2|\mathcal{X}|}\{(n+1)^{|\mathcal{X}|}+1\}\mathrm{e}^{-n[E(R|p_X)]} \end{aligned} \tag{29}$$

and for any eavesdropper $\mathcal{A}$ with $\varphi_{\mathcal{A}}$ satisfying $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$, we have

$$\Delta^{(n)}(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)}|p_X^n, p_K^n, W^n) \leq \{(n+1)^{|\mathcal{X}|}+1\}\Theta(R, \varphi_{\mathcal{A}}^{(n)}|p_K^n, W^n). \tag{30}$$

Proof. By Lemma 10, there exists $(\varphi^{(n)}, \psi^{(n)})$ satisfying $(m/n)\log|\mathcal{X}| \leq R$ such that for any $p_{\overline{X}} \in \mathcal{P}_n(\mathcal{X})$,

$$\Xi_{\overline{X}}(\phi^{(n)}, \psi^{(n)}) \leq \mathrm{e}(n+1)^{|\mathcal{X}|}\{(n+1)^{|\mathcal{X}|}+1\}\Lambda_{\overline{X}}(R). \tag{31}$$

Furthermore, for any $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$,

$$\Delta_n(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)}|p_X^n, p_K^n, W^n) \leq \{(n+1)^{|\mathcal{X}|}+1\}\Theta(R, \varphi_{\mathcal{A}}^{(n)}|p_K^n, W^n). \tag{32}$$

The bound (30) in Proposition 5 has already been proven in (32). Hence, it suffices to prove the bound (29) in Proposition 5 to complete the proof. On an upper bound of $p_{\mathrm{e}}(\phi^{(n)}, \psi^{(n)}|p_X^n)$, we have the following chain of inequalities:

$$\begin{aligned} p_{\mathrm{e}}(\phi^{(n)}, \psi^{(n)}|p_X^n) &\overset{(a)}{\leq} \mathrm{e}(n+1)^{|\mathcal{X}|}\{(n+1)^{|\mathcal{X}|}+1\} \sum_{p_{\overline{X}} \in \mathcal{P}_n(\mathcal{X})} \Lambda_{\overline{X}}(R)\mathrm{e}^{-nD(p_{\overline{X}}||p_X)} \\ &\leq \mathrm{e}(n+1)^{|\mathcal{X}|}\{(n+1)^{|\mathcal{X}|}+1\}|\mathcal{P}_n(\mathcal{X})|\mathrm{e}^{-n[E(R|p_X)]} \overset{(c)}{\leq} \mathrm{e}(n+1)^{2|\mathcal{X}|}\{(n+1)^{|\mathcal{X}|}+1\}\mathrm{e}^{-nE(R|p_X)}. \end{aligned}$$

Step (a) follows from Lemma 6 and (31). Step (b) follows from Lemma 4 part (a). □

6.4. Explicit Upper Bound of $\Theta(R_1, R_2, \varphi_{\mathcal{A}}^{(n)} | p_{ZK_1K_2}^n)$

In this subsection, we derive an explicit upper bound of $\Theta(R, \varphi_{\mathcal{A}}^{(n)} | p_K^n, W^n)$ that holds for any eavesdropper $\mathcal{A}$ with $\varphi_{\mathcal{A}}$ satisfying $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$. Here we recall the following definitions:

$$\begin{aligned}
&\wp_\eta^{(n)} = \wp_\eta^{(n)}(R|p_K^n, W^n) := p_{M_{\mathcal{A}}^{(n)} Z^n K^n}\left\{ R \geq \frac{1}{n} \log \frac{1}{p_{K^n|M_{\mathcal{A}}^{(n)}}(K^n|M_{\mathcal{A}}^{(n)})} - \eta \right\}, \\
&\Phi_{D,\eta}^{(n)}(R_{\mathcal{A}}, R|p_K^n W^n) := \max_{\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}^{(n)}(\mathcal{R}_{\mathcal{A}})} \left\{ nR\wp_\eta^{(n)}(R|p_K^n, W^n) + \mathrm{e}^{-n\eta} \right\}, \\
&\Phi_D^{(n)}(R_{\mathcal{A}}, R|p_K^n W^n) := \inf_{\eta>0} \Phi_{D,\eta}^{(n)}(R_{\mathcal{A}}, R|p_K^n W^n).
\end{aligned}$$

Then we have the following lemma.

Lemma 11. *For any $\eta > 0$ and for any eavesdropper $\mathcal{A}$ with $\varphi_{\mathcal{A}}$ satisfying $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$, we have*

$$\Theta(R, \varphi_{\mathcal{A}}^{(n)} | p_K^n, W^n) \leq \Phi_{D,\eta}^{(n)}(R_{\mathcal{A}}, R|p_K^n W^n), \tag{33}$$

which implies that

$$\Theta(R, \varphi_{\mathcal{A}}^{(n)} | p_K^n, W^n) \leq \Phi_D^{(n)}(R_{\mathcal{A}}, R|p_K^n W^n). \tag{34}$$

Proof. We first observe that

$$\Theta(R, \varphi_{\mathcal{A}}^{(n)} | p_K^n, W^n) = \mathrm{E}\left[\log \left\{ 1 + (\mathrm{e}^{nR} - 1) p_{K^n|M_{\mathcal{A}}^{(n)}}(K^n|M_{\mathcal{A}}^{(n)}) \right\} \right]. \tag{35}$$

We further observe the following:

$$\begin{aligned}
&R < \frac{1}{n} \log \frac{1}{p_{K^n|M_{\mathcal{A}}^{(n)}}(K^n|M_{\mathcal{A}}^{(n)})} - \eta \Leftrightarrow \mathrm{e}^{nR} p_{K^n|M_{\mathcal{A}}^{(n)}}(K^n|M_{\mathcal{A}}^{(n)}) < \mathrm{e}^{-n\eta} \\
&\Rightarrow \log \left\{ 1 + \mathrm{e}^{nR} p_{K^n|M_{\mathcal{A}}^{(n)}}(K^n|M_{\mathcal{A}}^{(n)}) \right\} \leq \log\left(1 + \mathrm{e}^{-n\eta}\right) \\
&\overset{(a)}{\Rightarrow} \log \left\{ 1 + \mathrm{e}^{nR} p_{K^n|M_{\mathcal{A}}^{(n)}}(K^n|M_{\mathcal{A}}^{(n)}) \right\} \leq \mathrm{e}^{-n\eta} \\
&\Rightarrow \log \left\{ 1 + (\mathrm{e}^{nR} - 1) p_{K^n|M_{\mathcal{A}}^{(n)}}(K^n|M_{\mathcal{A}}^{(n)}) \right\} \leq \mathrm{e}^{-n\eta}.
\end{aligned} \tag{36}$$

Step (a) follows from $\log(1 + a) \leq a$. We also note that

$$\log \left\{ 1 + (\mathrm{e}^{nR} - 1) p_{K^n|M_{\mathcal{A}}^{(n)}}(K^n|M_{\mathcal{A}}^{(n)}) \right\} \leq \log[\mathrm{e}^{nR}] = nR. \tag{37}$$

From (35), (36), and (37) we have the bound (33) in Lemma 11. □

Proof of Proposition 3: This proposition immediately follows from Proposition 5 and Lemma 11. □

For the upper bound of $\wp_\eta^{(n)}$, we have the following lemma.

Lemma 12. *For any $\eta > 0$ and for any eavesdropper $\mathcal{A}$ with $\varphi_{\mathcal{A}}$ satisfying $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$, we have $\wp_{\eta}^{(n)} \leq \tilde{\wp}_{\eta}^{(n)} + 3\mathrm{e}^{-n\eta}$, where*

$$\tilde{\wp}_{\eta}^{(n)} := p_{M_{\mathcal{A}}^{(n)} Z^n K^n} \Bigg\{$$

$$0 \geq \frac{1}{n} \log \frac{\hat{q}_{M_{\mathcal{A}}^{(n)} Z^n K^n}(M_{\mathcal{A}}^{(n)}, Z^n, K^n)}{p_{M_{\mathcal{A}}^{(n)} Z^n K^n}(M_{\mathcal{A}}^{(n)}, Z^n, K^n)} - \eta, \tag{38}$$

$$0 \geq \frac{1}{n} \log \frac{q_{Z^n}(Z^n)}{p_{Z^n}(Z^n)} - \eta, \tag{39}$$

$$R_{\mathcal{A}} \geq \frac{1}{n} \log \frac{p_{Z^n|M_{\mathcal{A}}^{(n)}}(Z^n|M_{\mathcal{A}}^{(n)})}{p_{Z^n}(Z^n)} - \eta,$$

$$R \geq \frac{1}{n} \log \frac{1}{p_{K^n|M_{\mathcal{A}}^{(n)}}(K^n|M_{\mathcal{A}}^{(n)})} - \eta \Bigg\}. \tag{40}$$

The probability distributions appearing in the two inequalities (38) and (39) in the right members of (40) have a property that we can select them arbitrarily. In (38), we can choose any probability distribution $\hat{q}_{M_{\mathcal{A}}^{(n)} Z^n K^n}$ on $\mathcal{M}_{\mathcal{A}}^{(n)} \times \mathcal{Z}^n \times \mathcal{X}^n$. In (39), we can choose any distribution q_{Z^n} on $\mathcal{Z}^n$.

Proof of this lemma is given in Appendix E.

Proof of Proposition 4: The claim of Proposition 4 is that for $n \geq 1/R$,

$$\Phi_D^{(n)}(R_{\mathcal{A}}, R|p_K^n W^n) \leq 5nR\mathrm{e}^{-nF(R_{\mathcal{A}}, R|p_K, W)}. \tag{41}$$

By Lemma 12 and the definition of $\Phi_{D,\eta}^{(n)}(R_{\mathcal{A}}, R|p_K^n W^n)$, we have that for $n \geq 1/R$,

$$\Phi_{D,\eta}^{(n)}(R_{\mathcal{A}}, R|p_K^n W^n) \leq nR(\tilde{\wp}_{\eta}^{(n)} + 4\mathrm{e}^{-n\eta}). \tag{42}$$

The quantity $\tilde{\wp}_{\eta}^{(n)} + 4\mathrm{e}^{-n\eta}$ is the same as the upper bound on the correct probability of decoding for one helper source coding problem in Lemma 1 in Oohama [9] (extended version). In a manner similar to the derivation of the exponential upper bound of the correct probability of decoding for one helper source coding problem, we can prove that for any $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$ and for some $\eta^* = \eta^*(n, R_{\mathcal{A}}, R)$, we have

$$\tilde{\wp}_{\eta^*}^{(n)} + 4\mathrm{e}^{-n\eta^*} \leq 5\mathrm{e}^{-nF(R_{\mathcal{A}}, R|p_K, W)}. \tag{43}$$

From (42), (43), and the definition of $\Phi_D^{(n)}(R_{\mathcal{A}}, R|p_K^n W^n)$, we have (41). □

7. Conclusions

In this paper, we have proposed a novel security model for analyzing the security of Shannon cipher systems against an adversary that is not only eavesdropping the public communication channel to obtain ciphertexts but is also obtaining some physical information leaked by the device implementing the cipher system through side-channel attacks. We have also presented a countermeasure against such an adversary in the case of one-time pad encryption by using an affine encoder with certain properties. The main distinguishing feature of our countermeasure is that it is independent of the

characteristics or the types of physical information leaked from the devices on which the cipher system is implemented.

Author Contributions: Both the first and the second authors contributed for the writing of the original draft of this paper. Other contributions of the first author include (but are not limited to): the conceptualization of the research goals and aims, the validation of the results, the visualization/presentation of the works, the review and editing. Other contributions of the second author include (but are not limited to): the conceptualization of the ideas, research goals and aims, the formal analysis and the supervision.

Funding: This research was funded by Japan Society for the Promotion of Science (JSPS) Kiban (B) 18H01438 and Japan Society for the Promotion of Science (JSPS) Kiban (C) 18K11292.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

Appendix A. Correct Probability of Decoding and Variational Distance

In this appendix, we prove Lemma 3.

For $a \in \mathcal{M}_{\mathcal{A}}^{(n)}$, we set

$$\mathcal{D}(a) = \left\{ \tilde{k}^m : \tilde{k}^m = \varphi^{(n)}(k^n) \text{ and } \psi_{\mathcal{A}}^{(n)}(\tilde{k}^m, a) = k^n \text{ for some } k^n \in \mathcal{X}^n \right\}.$$

Then we have the following chain of inequalities:

$$\begin{aligned}
&d\left(p_{V^m} \times p_{M_{\mathcal{A}}^{(n)}}, p_{\tilde{K}^m M_{\mathcal{A}}^{(n)}}\right) = \sum_{a \in \mathcal{M}_{\mathcal{A}}^{(n)}} p_{M_{\mathcal{A}}^{(n)}}(a) \sum_{\tilde{k}^m \in \mathcal{X}^m} \left| p_{\tilde{K}^m | M_{\mathcal{A}}^{(n)}}(\tilde{k}^m | a) - \frac{1}{|\mathcal{X}|^m} \right| \\
&\geq \sum_{a \in \mathcal{M}_{\mathcal{A}}^{(n)}} p_{M_{\mathcal{A}}^{(n)}}(a) \left\{ p_{\tilde{K}^m | M_{\mathcal{A}}^{(n)}}(\mathcal{D}(a) | a) - \frac{|\mathcal{D}(a)|}{|\mathcal{X}|^m} \right\} = \sum_{a \in \mathcal{M}_{\mathcal{A}}^{(n)}} p_{M_{\mathcal{A}}^{(n)}}(a) \left\{ p_{\tilde{K}^m | M_{\mathcal{A}}^{(n)}}(\mathcal{D}(a) | a) - \frac{1}{|\mathcal{X}|^m} \right\} \\
&= p_{\mathrm{c},\mathcal{A}}^{(n)}\left(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)}, \psi_{\mathcal{A}}^{(n)} \middle| p_K^n, W^n\right) - \frac{1}{|\mathcal{X}|^m},
\end{aligned}$$

completing the proof. □

Appendix B. Proof of Lemma 7

Let a_l^m be the l-th low vector of the matrix A. For each $l = 1, 2, \cdots, n$, let $A_l^m \in \mathcal{X}^m$ be a random vector that represents the randomness of the choice of $a_l^m \in \mathcal{X}^m$. Let $B^m \in \mathcal{X}^m$ be a random vector that represents the randomness of the choice of $b^m \in \mathcal{X}^m$. We first prove part (a). Without loss of generality, we may assume $x_1 \neq v_1$. Under this assumption, we have the following:

$$(x^n \ominus v^n)A = 0^m \Leftrightarrow \sum_{l=1}^{n} (x_l \ominus v_l) a_l^m = 0^m \Leftrightarrow a_1^m = \sum_{l=2}^{n} \frac{v_l \ominus x_l}{x_1 \ominus v_1} a_l^m. \tag{A1}$$

Computing $\Pr[\phi(x^n) = \phi(v^n)]$, we have the following chain of equalities:

$$\begin{aligned}
&\Pr[\phi(x^n) = \phi(v^n)] = \Pr[(y^n \ominus w^n)A = 0^m] \overset{(a)}{=} \Pr\left[a_1^m = \sum_{l=2}^{n} \frac{w_l \ominus y_l}{x_1 \ominus v_1} a_l^m \right] \\
&\overset{(b)}{=} \sum_{\substack{\{a_l^m\}_{l=2}^n \\ \in \mathcal{X}^{(n-1)m}}} \prod_{l=2}^{n} P_{A_l^m}(a_l^m) P_{A_1^m}\left(\sum_{l=2}^{n} \frac{w_l \ominus x_l}{y_1 \ominus v_1} a_l^m \right) = |\mathcal{X}|^{-m} \sum_{\substack{\{a_l^m\}_{l=2}^n \\ \in \mathcal{X}^{(n-1)m}}} \prod_{l=2}^{n} P_{A_l^m}(a_l^m) = |\mathcal{X}|^{-m}.
\end{aligned}$$

Step (a) follows from (A1). Step (b) follows from that n random vectors $A_l^m, l = 1, 2, \cdots, n$ are independent. We next prove part b. We have the following:

$$s^n A \oplus b^m = \tilde{s}^m \Leftrightarrow b^m = \tilde{s}^m \ominus \left\{ \sum_{l=1}^{n} s_l a_l^m \right\}. \tag{A2}$$

Computing $\Pr[s^n A \oplus b^m = \tilde{s}^m]$, we have the following chain of equalities:

$$\begin{aligned}
\Pr[s^n A \oplus b^m = \tilde{s}^m] &\overset{(a)}{=} \Pr\left[b^m = \tilde{s}^m \ominus \left\{ \sum_{l=1}^{n} s_l a_l^m \right\} \right] \\
&\overset{(b)}{=} \sum_{\substack{\{a_l^m\}_{l=1}^n \\ \in \mathcal{X}^{nm}}} \prod_{l=1}^{n} P_{A_l^m}(a_l^m) P_{B^m}\left(\tilde{s}^m \ominus \left\{ \sum_{l=1}^{n} s_l a_l^m \right\} \right) \\
&\overset{(c)}{=} |\mathcal{X}|^{-m} \sum_{\substack{\{a_l^m\}_{l=1}^n \\ \in \mathcal{X}^{nm}}} \prod_{l=1}^{n} P_{A_l^m}(a_l^m) = |\mathcal{X}|^{-m}.
\end{aligned}$$

Step (a) follows from (A2). Step (b) follows from that n random vectors $A_l^m, l = 1, 2, \cdots, n$ and B^m are independent. We finally prove the part (c). We first observe that $s^n \neq t^n \Leftrightarrow$ is equivalent to $s_i \neq t_i$ for some $i \in \{1, 2, \cdots, n\}$. Without loss of generality, we may assume that $s_1 \neq t_1$. Under this assumption, we have the following:

$$\begin{aligned}
& s^n A \oplus b^m = t^n A \oplus b^m = \tilde{s}^m \\
\Leftrightarrow \quad & (s^n \ominus t^n) A = 0, b^m = \tilde{s}^m \ominus \left\{ \sum_{l=1}^{n} s_l a_l^m \right\} \\
\Leftrightarrow \quad & a_1^m = \sum_{l=2}^{n} \frac{t_l \ominus s_l}{s_1 \ominus t_1} a_l^m, b^m = \tilde{s}^m \ominus \left\{ \sum_{l=1}^{n} s_l a_l^m \right\} \\
\Leftrightarrow \quad & a_1^m = \sum_{l=2}^{n} \frac{t_l \ominus s_l}{s_1 \ominus t_1} a_l^m, b^m = \tilde{s}^m \oplus \sum_{l=2}^{n} \frac{t_1 s_l \ominus s_1 t_l}{s_1 \ominus t_1} a_l^m.
\end{aligned} \tag{A3}$$

Computing $\Pr[s^n A \oplus b^m = t^n A \oplus b^m = \tilde{s}^m]$, we have the following chain of equalities:

$$\begin{aligned}
& \Pr[s^n A \oplus b^m = t^n A \oplus b^m = \tilde{s}^m] \\
& \overset{(a)}{=} \Pr\left[a_1^m = \sum_{l=2}^{n} \frac{t_l \ominus s_l}{s_1 \ominus t_1} a_l^m \ \wedge b^m = \tilde{s}^m \oplus \sum_{l=2}^{n} \frac{t_1 s_l \ominus s_1 t_l}{s_1 \ominus t_1} a_l^m \right] \\
& \overset{(b)}{=} \sum_{\substack{\{a_l^m\}_{l=2}^n \\ \in \mathcal{X}^{(n-1)m}}} \left[\prod_{l=2}^{n} P_{A_l^m}(a_l^m) \right] P_{A_1^m}\left(\sum_{l=2}^{n} \frac{t_l \ominus s_l}{s_1 \ominus t_1} a_l^m \right) P_{B^m}\left(\tilde{s}^m \oplus \sum_{l=2}^{n} \frac{t_1 s_l \ominus s_1 t_l}{s_1 \ominus t_1} a_l^m \right) \\
& = |\mathcal{X}|^{-2m} \sum_{\substack{\{a_l^m\}_{l=2}^n \\ \in \mathcal{X}^{(n-1)m}}} \prod_{l=2}^{n} P_{A_l^m}(a_l^m) = |\mathcal{X}|^{-2m}.
\end{aligned}$$

Step (a) follows from (A3). Step (b) follows from the independent property on $A_l^m, l = 1, 2, \cdots, n$ and B^m. □

Appendix C. Proof of Lemma 8

In this appendix, we provide the proof of Lemma 8.

For simplicity of notation, we write $M = |\mathcal{X}|^m$. For $x^n \in \mathcal{X}^n$ we set

$$B(x^n) = \left\{ (\check{x}^n) : H(\check{x}^n) \le H(x^n),\ P_{\check{x}^n} = P_{x^n} \right\},$$

Using parts (a) and (b) of Lemma 4, we have following inequalities:

$$|B(x^n)| \le (n+1)^{|\mathcal{X}|} \mathrm{e}^{nH(x^n)}, \tag{A4}$$

On an upper bound of $\mathbf{E}[\Xi_{x^n}(\phi^{(n)}, \psi^{(n)})]$, we have the following chain of inequalities:

$$\begin{aligned}\mathbf{E}[\Xi_{x^n}(\phi^{(n)}, \psi^{(n)})] &\le \sum_{\substack{\check{x}^n \in B(x^n),\\ \check{x}^n \neq x^n}} \Pr\{\phi^{(n)}(\check{x}^n) = \phi^{(n)}(x^n)\} \\ &\overset{\text{(a)}}{\le} \sum_{\check{x}^n \in B(x^n)} \frac{1}{M} = \frac{|B(x^n)|}{M} \overset{\text{(b)}}{\le} \mathrm{e}(n+1)^{|\mathcal{X}|} \mathrm{e}^{-n[R-H(x^n)]}.\end{aligned}$$

Step (a) follows from Lemma 7 part (a) and independent random constructions of linear encoders $\phi_1^{(n)}$ and $\phi_{\mathrm{e}}^{(n)}$. Step (b) follows from (A4) and $M \ge \mathrm{e}^{nR-1}, i = 1, 2$. On the other hand we have the obvious bound $\mathbf{E}[\Xi_{x^n}(\phi^{(n)}, \psi^{(n)})] \le 1$. Hence we have

$$\mathbf{E}[\Xi_{x^n}(\phi^{(n)}, \psi^{(n)})] \le \mathrm{e}(n+1)^{|\mathcal{X}|} \left\{ \mathrm{e}^{-n[R-H(x^n)]^+} \right\}.$$

Hence we have

$$\begin{aligned}\mathbf{E}[\Xi_{\overline{X}_1\overline{X}_2}(\phi^{(n)}, \psi^{(n)})] = \mathbf{E}\left[\frac{1}{|T^n_{\overline{X}}|} \sum_{x^n \in T^n_{\overline{X}}} \Xi_{x^n}(\phi^{(n)}, \psi^{(n)}) \right] &= \frac{1}{|T^n_{\overline{X}}|} \sum_{x^n \in T^n_{\overline{X}}} \mathbf{E}[\Xi_{x^n}(\phi^{(n)}, \psi^{(n)})] \\ &\le \mathrm{e}(n+1)^{|\mathcal{X}|} \left\{ \mathrm{e}^{-n[R-H(\overline{X})]^+} \right\},\end{aligned}$$

completing the proof. □

Appendix D. Proof of Lemma 9

In this appendix, we prove Lemma 9. This lemma immediately follows from the following lemma:

Lemma A1. *For any n, m satisfying $(m/n)\log|\mathcal{X}| \le R$, we have*

$$\begin{aligned}&\mathbf{E}\left[D\left(p_{\tilde{K}^m|M_{\mathcal{A}}^{(n)}} \middle\| p_{V^m} \middle| p_{M_{\mathcal{A}}^{(n)}} \right) \right] \\ &\le \sum_{(a,k^n) \in \mathcal{M}_{\mathcal{A}}^{(n)} \times \mathcal{X}^n} p_{M_{\mathcal{A}}^{(n)} K^n}(a, k^n) \log\left[1 + (|\mathcal{X}^m| - 1) p_{K^n|M_{\mathcal{A}}^{(n)}}(k^n|a) \right].\end{aligned} \tag{A5}$$

In fact, from $|\mathcal{X}^m| \le \mathrm{e}^{nR}$ and (A5) in Lemma A1, we have the bound (28) in Lemma 9. Thus, we prove Lemma A1 instead of proving Lemma 9.

In the following arguments, we use the following simplified notations:

$$\begin{aligned}k^n, K^n \in \mathcal{X}^n &\Longrightarrow k, K \in \mathcal{K}, \\ \tilde{k}^m, \tilde{K}^m \in \mathcal{X}^m &\Longrightarrow l, L \in \mathcal{L}, \\ \varphi^{(n)} : \mathcal{X}^n \to \mathcal{X}^m &\Longrightarrow \varphi : \mathcal{K} \to \mathcal{L},\end{aligned}$$

$$\varphi^{(n)}(k^n) = k^n A + b^m \Longrightarrow \varphi(k) = kA + b,$$
$$V^m \in \mathcal{X}^m \Longrightarrow V \in \mathcal{L},$$
$$M_{\mathcal{A}}^{(n)} \in \mathcal{M}_{\mathcal{A}}^{(n)} \Longrightarrow M \in \mathcal{M}.$$

We define

$$\chi_{\varphi(k),l} = \begin{cases} 1, \text{ if } \varphi(k) = l, \\ 0, \text{ if } \varphi(k) \neq l. \end{cases}$$

Then, the conditional distribution of the random variable $L = L_\varphi$ for given $M = a \in \mathcal{M}$ is

$$p_{L|M}(l|a) = \sum_{k \in \mathcal{K}} p_{K|M}(k|a)\chi_{\varphi(k),l} \text{ for } l \in \mathcal{L}.$$

Define

$$\mathrm{Y}_{\varphi(k),l} := \chi_{\varphi(k),l} \log \left[|\mathcal{L}| \left\{ \sum_{k' \in \mathcal{K}} p_{K|M}(k'|a)\chi_{\varphi(k'),l} \right\} \right].$$

Then the conditional divergence between $p_{L|M}$ and p_V for given M is given by

$$D\left(p_{L|M} \middle|\middle| p_V \middle| p_M\right) = \sum_{(a,k) \in \mathcal{M} \times \mathcal{K}} \sum_{l \in \mathcal{L}} p_{MK}(a,k)\mathrm{Y}_{\varphi(k),l}. \tag{A6}$$

The quantity $\mathrm{Y}_{\varphi(k),l}$ has the following form:

$$\mathrm{Y}_{\varphi(k),l} = \chi_{\varphi(k),l} \log \left\{ |\mathcal{L}| \left(p_{K|M}(k|a)\chi_{\varphi(k),l} + \sum_{k' \in \{k\}^{\mathrm{c}}} p_{K|M}(k'|a)\chi_{\varphi(k'),l} \right) \right\}. \tag{A7}$$

The above form is useful for computing $\mathbf{E}[\mathrm{Y}_{\varphi(k),l}]$.

Proof of Lemma A1: Taking the expectation of both sides of (A7) with respect to the random choice of the entry of the matrix A and the vector b representing the affine encoder φ, we have

$$\mathbf{E}\left[D\left(p_{L|M} \middle|\middle| p_V \middle| p_M\right)\right] = \sum_{(a,k) \in \mathcal{M} \times \mathcal{K}} \sum_{l \in \mathcal{L}} p_{MK}(a,k)\mathbf{E}\left[\mathrm{Y}_{\varphi(k),l}\right]. \tag{A8}$$

To compute the expectation $\mathbf{E}\left[\mathrm{Y}_{\varphi(k),l}\right]$, we introduce an expectation operator useful for the computation. Let $\mathbf{E}_{\varphi(k)=l_k}[\cdot]$ be an expectation operator based on the conditional probability measures $\Pr(\cdot|\varphi(k) = l_k)$. Using this expectation operator, the quantity $\mathbf{E}\left[\mathrm{Y}_{\varphi(k),l}\right]$ can be written as

$$\mathbf{E}\left[\mathrm{Y}_{\varphi(k),l}\right] = \sum_{l_k \in \mathcal{L}} \Pr\left(\varphi(k) = l_k\right) \mathbf{E}_{\varphi(k)=l_k}\left[\mathrm{Y}_{l_k,l}\right]. \tag{A9}$$

Note that

$$\mathrm{Y}_{l_k,l} = \begin{cases} 1, \text{ if } l_k = l, \\ 0, \text{ otherwise.} \end{cases} \tag{A10}$$

From (A9) and (A10), we have

$$\mathbf{E}\left[\mathrm{Y}_{\varphi(k),l}\right] = \Pr\left(\varphi(k) = l\right) \mathbf{E}_{\varphi(k)=l}\left[\mathrm{Y}_{l,l}\right] = \frac{1}{|\mathcal{L}|}\mathbf{E}_{\varphi(k)=l}\left[\mathrm{Y}_{l,l}\right]. \tag{A11}$$

Using (A7), the expectation $\mathbf{E}_{\varphi(k)=l}\left[\mathrm{Y}_{l,l}\right]$ can be written as

$$\mathbf{E}_{\varphi(k)=l}\left[\mathrm{Y}_{l,l}\right]=\mathbf{E}_{\varphi(k)=l}\left[\log\left\{|\mathcal{L}|\left(p_{K|M}(k|a)\ +\sum_{k'\in\{k\}^{\mathrm{c}}}p_{K|M}(k'|a)\chi_{\varphi(k'),l}\right)\right\}\right]. \tag{A12}$$

Applying Jensen's inequality to the right member of (A12), we obtain the following upper bound of $\mathbf{E}_{\varphi(k)=l}\left[\mathrm{Y}_{l,l}\right]$:

$$\begin{aligned}\mathbf{E}_{\varphi(k)=l}\left[\mathrm{Y}_{l,l}\right]&\leq\log\left\{|\mathcal{L}|\left(p_{K|M}(k|a)\ +\sum_{k'\in\{k\}^{\mathrm{c}}}p_{K|M}(k'|a)\mathbf{E}_{\varphi(k)=l}\left[\chi_{\varphi(k'),l}\right]\right)\right\}\\&\overset{\text{(a)}}{=}\log\left\{|\mathcal{L}|\left(p_{K|M}(k|a)+\sum_{k'\in\{k\}^{\mathrm{c}}}p_{K|M}(k'|a)\frac{1}{|\mathcal{L}|}\right)\right\}=\log\left\{1+(|\mathcal{L}|-1)p_{K|M}(k|a)\right\}.\end{aligned} \tag{A13}$$

Step (a) follows from that by Lemma 7 parts (b) and (c),

$$\mathbf{E}_{\varphi(k)=l}\left[\chi_{\varphi(k'),l}\right]=\Pr(\varphi(k')=l|\varphi(k)=l)=\frac{1}{|\mathcal{L}|}.$$

From (A8), (A11), and (A13), we have the bound (A5) in Lemma A1. □

Appendix E. Proof of Lemma 12

To prove Lemma 12, we prepare a lemma. For simplicity of notation, set $|\mathcal{M}_{\mathcal{A}}^{(n)}|=M_{\mathcal{A}}$. Define

$$\mathcal{B}_n:=\left\{(a,z^n,k^n):\frac{1}{n}\log\frac{p_{M_{\mathcal{A}}^{(n)}Z^nK^n}(a,z^n,k^n)}{\hat{q}_{M_{\mathcal{A}}^{(n)}Z^nK^n}(a,z^n,k^n)}\geq-\eta\right\}.$$

Furthermore, define

$$\begin{aligned}&\tilde{\mathcal{C}}_n:=\left\{z^n:\frac{1}{n}\log\frac{p_{Z^n}(z^n)}{q_{Z^n}(z^n)}\geq-\eta\right\},\\&\mathcal{C}_n:=\tilde{\mathcal{C}}_n\times\mathcal{M}_{\mathcal{A}}^{(n)}\times\mathcal{X}^n,\mathcal{C}_n^{\mathrm{c}}:=\tilde{\mathcal{C}}_n^{\mathrm{c}}\times\mathcal{M}_{\mathcal{A}}^{(n)}\times\mathcal{X}^n,\\&\tilde{\mathcal{D}}_n:=\{(a,z^n):\ \ a=\varphi_{\mathcal{A}}^{(n)}(z^n),p_{Z^n|M_{\mathcal{A}}^{(n)}}(z^n|a)\leq M_{\mathcal{A}}\mathrm{e}^{n\eta}p_{Z^n}(z^n)\},\\&\mathcal{D}_n:=\tilde{\mathcal{D}}_n\times\mathcal{X}^n,\mathcal{D}_n^{\mathrm{c}}:=\tilde{\mathcal{D}}_n^{\mathrm{c}}\times\mathcal{X}^n,\\&\mathcal{E}_n:=\{(a,z^n,k^n):\ \ a=\varphi_{\mathcal{A}}^{(n)}(z^n),p_{K^n|M_{\mathcal{A}}^{(n)}}(k^n|a)\geq\mathrm{e}^{-n(R+\eta)}\}.\end{aligned}$$

Then we have the following lemma.

Lemma A2.

$$\begin{aligned}p_{M_{\mathcal{A}}^{(n)}Z^nK^n}(\mathcal{B}_n^{\mathrm{c}})&\leq\mathrm{e}^{-n\eta},\\p_{M_{\mathcal{A}}^{(n)}Z^nK^n}(\mathcal{C}_n^{\mathrm{c}})&\leq\mathrm{e}^{-n\eta},\\p_{M_{\mathcal{A}}^{(n)}Z^nK^n}(\mathcal{D}_n^{\mathrm{c}})&\leq\mathrm{e}^{-n\eta}.\end{aligned}$$

Proof. We first prove the first inequality.

$$\begin{aligned} p_{M_{\mathcal{A}}^{(n)}Z^nK^n}(\mathcal{B}_n^{\mathrm{c}}) &= \sum_{(a,z^n,k^n)\in\mathcal{B}_n^{\mathrm{c}}} p_{M_{\mathcal{A}}^{(n)}Z^nK^n}(a,z^n,k^n) \\ &\overset{\text{(a)}}{\leq} \sum_{(a,z^n,k^n)\in\mathcal{B}_n^{\mathrm{c}}} \mathrm{e}^{-n\eta}\hat{q}_{M_{\mathcal{A}}^{(n)}Z^nK^n}(a,z^n,k^n) \\ &= \mathrm{e}^{-n\eta}q_{M_{\mathcal{A}}^{(n)}Z^nK^n}(\mathcal{B}_n^{\mathrm{c}}) \leq \mathrm{e}^{-n\eta}. \end{aligned}$$

Step (a) follows from the definition of $\mathcal{B}_n$. For the second inequality we have

$$\begin{aligned} p_{M_{\mathcal{A}}^{(n)}Z^nK^n}(\mathcal{C}_n^{\mathrm{c}}) &= p_{Z^n}(\tilde{\mathcal{C}}_n^{\mathrm{c}}) = \sum_{x^n\in\tilde{\mathcal{C}}_n^{\mathrm{c}}} p_{Z_n}(z^n) \\ &\overset{\text{(a)}}{\leq} \sum_{x^n\in\tilde{\mathcal{C}}_n^{\mathrm{c}}} \mathrm{e}^{-n\eta}q_{Z^n}(z^n) = \mathrm{e}^{-n\eta}q_{Z^n}\left(\tilde{\mathcal{C}}_n^{\mathrm{c}}\right) \leq \mathrm{e}^{-n\eta}. \end{aligned}$$

Step (a) follows from the definition of $\mathcal{C}_n$. We finally prove the third inequality.

$$\begin{aligned} p_{M_{\mathcal{A}}^{(n)}Z^nK^n}(\mathcal{D}_n^{\mathrm{c}}) = p_{M_{\mathcal{A}}^{(n)}Z^n}(\tilde{\mathcal{D}}_n^{\mathrm{c}}) &= \sum_{a\in\mathcal{M}_{\mathcal{A}}^{(n)}} \sum_{\substack{z^n:\varphi_{\mathcal{A}}^{(n)}(z^n)=a \\ p_{Z^n}(z^n)\leq(\mathrm{e}^{-n\eta}/M_{\mathcal{A}}) \\ \times p_{Z^n|M_{\mathcal{A}}^{(n)}}(z^n|a)}} p_{Z^n}(z^n) \\ &\leq \frac{\mathrm{e}^{-n\eta}}{M_{\mathcal{A}}} \sum_{a\in\mathcal{M}_{\mathcal{A}}^{(n)}} \sum_{\substack{z^n:\varphi_{\mathcal{A}}^{(n)}(z^n)=a \\ p_{Z^n}(z^n)\leq(\mathrm{e}^{-n\eta}/M_{\mathcal{A}}) \\ \times p_{Z^n|M_{\mathcal{A}}^{(n)}}(z^n|a)}} p_{Z^n|M_{\mathcal{A}}^{(n)}}(z^n|a) \\ &\leq \frac{\mathrm{e}^{-n\eta}}{M_{\mathcal{A}}}|\mathcal{M}_{\mathcal{A}}^{(n)}| = \mathrm{e}^{-n\eta}. \end{aligned}$$

This completes the proof of Lemma A2. □

Proof of Lemma 12: By definition, we have

$$\begin{aligned} & p_{M_{\mathcal{A}}^{(n)}Z^nK^n}(\mathcal{B}_n\cap\mathcal{C}_n\cap\mathcal{D}_n\cap\mathcal{E}_n) \\ =& p_{M_{\mathcal{A}}^{(n)}Z^nK^n}\left\{\frac{1}{n}\log\frac{p_{M_{\mathcal{A}}^{(n)}Z^nK^n}(M_{\mathcal{A}}^{(n)},Z^n,K^n)}{\hat{q}_{M_{\mathcal{A}}^{(n)}Z^nK^n}(M_{\mathcal{A}}^{(n)},Z^n,K^n)} \geq -\eta,\right. \\ & 0 \geq \frac{1}{n}\log\frac{q_{Z^n}(Z^n)}{p_{Z^n}(Z^n)} - \eta, \\ & \frac{1}{n}\log M_{\mathcal{A}} \geq \frac{1}{n}\log\frac{p_{Z^n|M_{\mathcal{A}}^{(n)}}(Z^n|M_{\mathcal{A}}^{(n)})}{p_{Z^n}(Z^n)} - \eta, \\ & \left. R \geq \frac{1}{n}\log\frac{1}{p_{K^n|M_{\mathcal{A}}^{(n)}}(K^n|M_{\mathcal{A}}^{(n)})} - \eta\right\}. \end{aligned}$$

Then for any $\varphi_{\mathcal{A}}^{(n)}$ satisfying $(1/n)\log||\varphi_{\mathcal{A}}^{(n)}|| \leq R_{\mathcal{A}}$, we have

$$\begin{aligned}
&p_{M_{\mathcal{A}}^{(n)}Z^nK^n}\left(\mathcal{B}_n \cap \mathcal{C}_n \cap \mathcal{D}_n \cap \mathcal{E}_n\right) \\
\leq & p_{M_{\mathcal{A}}^{(n)}Z^nK^n}\left\{\frac{1}{n}\log\frac{p_{M_{\mathcal{A}}^{(n)}Z^nK^n}(M_{\mathcal{A}}^{(n)},Z^n,K^n)}{\hat{q}_{M_{\mathcal{A}}^{(n)}Z^nK^n}(M_{\mathcal{A}}^{(n)},Z^n,K^n)} \geq -\eta,\right. \\
&\qquad 0 \geq \frac{1}{n}\log\frac{q_{Z^n}(Z^n)}{p_{Z^n}(Z^n)} - \eta, \\
&\qquad R_{\mathcal{A}} \geq \frac{1}{n}\log\frac{p_{Z^n|M_{\mathcal{A}}^{(n)}}(Z^n|M_{\mathcal{A}}^{(n)})}{p_{Z^n}(Z^n)} - \eta, \\
&\qquad \left. R \geq \frac{1}{n}\log\frac{1}{p_{K^n|M_{\mathcal{A}}^{(n)}}(K^n|M_{\mathcal{A}}^{(n)})} - \eta\right\}.
\end{aligned}$$

Hence, it suffices to show

$$\wp_{\eta}^{(n)} \leq p_{M_{\mathcal{A}}^{(n)}Z^nK^n}\left(\mathcal{B}_n \cap \mathcal{C}_n \cap \mathcal{D}_n \cap \mathcal{E}_n\right) + 3\mathrm{e}^{-n\eta}$$

to prove Lemma 12. We have the following chain of inequalities:

$$\begin{aligned}
\wp &\overset{\text{(a)}}{=} p_{M_{\mathcal{A}}^{(n)}Z^nK^n}\left(\mathcal{E}_n\right) \\
&= p_{M_{\mathcal{A}}^{(n)}Z^nK^n}\left(\mathcal{B}_n \cap \mathcal{C}_n \cap \mathcal{D}_n \cap \mathcal{E}_n\right) + p_{M_{\mathcal{A}}^{(n)}Z^nK^n}\left([\mathcal{B}_n \cap \mathcal{C}_n \cap \mathcal{D}_n]^{\mathrm{c}} \cap \mathcal{E}_n\right) \\
&\leq p_{M_{\mathcal{A}}^{(n)}Z^nK^n}\left(\mathcal{B}_n \cap \mathcal{C}_n \cap \mathcal{D}_n \cap \mathcal{E}_n\right) + p_{M_{\mathcal{A}}^{(n)}Z^nK^n}\left(\mathcal{B}_n^{\mathrm{c}}\right) + p_{M_{\mathcal{A}}^{(n)}Z^nK^n}\left(\mathcal{C}_n^{\mathrm{c}}\right) + p_{M_{\mathcal{A}}^{(n)}Z^nK^n}\left(\mathcal{D}_n^{\mathrm{c}}\right) \\
&\overset{\text{(b)}}{\leq} p_{M_{\mathcal{A}}^{(n)}Z^nK^n}\left(\mathcal{B}_n \cap \mathcal{C}_n \cap \mathcal{D}_n \cap \mathcal{E}_n\right) + 3\mathrm{e}^{-n\eta} = \tilde{\wp}.
\end{aligned}$$

Step (a) follows from the defintion of $\wp$. Step (b) follows from Lemma A2. □

References

1. Brier, E.; Clavier, C.; Olivier, F. Correlation Power Analysis with a Leakage Model. In *International Workshop on Cryptographic Hardware and Embedded Systems*; Joye, M., Quisquater, J.J., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; pp. 16–29.
2. Quisquater, J.J.; Samyde, D. ElectroMagnetic Analysis (EMA): Measures and Counter-Measures for Smart Cards. In *International Conference on Research in Smart Cards*; Attali, I., Jensen, T., Eds.; Springer: London, UK, 2001; pp. 200–210.
3. Kocher, P.C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In *Annual International Cryptology Conference*; Springer: Berlin/Heidelberg, Germany, 1996; Volume 1109, pp. 104–113.
4. Kocher, P.C.; Jaffe, J.; Jun, B. Differential Power Analysis. In *Lecture Notes in Computer Science*; Springer: Berlin/Heidelberg, Germany, 1999; Volume 1666, pp. 388–397.
5. Agrawal, D.; Archambeault, B.; Rao, J.R.; Rohatgi, P. The EM Side—Channel(s). In *International Workshop on Cryptographic Hardware and Embedded Systems*; Kaliski, B.S., Koç, ç.K., Paar, C., Eds.; Springer: Berlin/Heidelberg, Germany, 2003; pp. 29–45.
6. Csiszár, I. Linear Codes for Sources and Source Networks: Error Exponents, Universal Coding. *IEEE Trans. Inform. Theory* **1982**, *28*, 585–592.
7. Ahlswede, R.; Körner, J. Source Coding with Side Information and A Converse for The Degraded Broadcast Channel. *IEEE Trans. Inform. Theory* **1975**, *21*, 629–637.
8. Wyner, A.D. The Common Information of Two Dependent Random Variables. *IEEE Trans. Inform. Theory* **1975**, *21*, 163–179.

9. Oohama, Y. Exponent function for one helper source coding problem at rates outside the rate region. In Proceedings of the 2015 IEEE International Symposium on Information Theory (ISIT), Hong Kong, 14–19 June 2015; pp. 1575–1579.
10. Watanabe, S.; Oohama, Y. Privacy amplification theorem for bounded storage eavesdropper. In Proceedings of the 2012 IEEE Information Theory Workshop (ITW), Bangalore, India, 20–25 October 2012; pp. 177–181.
11. Coron, J.; Naccache, D.; Kocher, P.C. Statistics and secret leakage. *ACM Trans. Embed. Comput. Syst.* **2004**, *3*, 492–508.
12. Köpf, B.; Basin, D.A. An information-theoretic model for adaptive side-channel attacks. In Proceedings of the 2007 ACM Conference on Computer and Communications Security, CCS 2007, Alexandria, VA, USA, 28–31 January 2007; pp. 286–296.
13. Backes, M.; Köpf, B. Formally Bounding the Side-Channel Leakage in Unknown-Message Attacks. In *European Symposium on Research in Computer Security*; Springer: Berlin/Heidelberg, Germany, 2008; Volume 5283, pp. 517–532.
14. Micali, S.; Reyzin, L. Physically Observable Cryptography (Extended Abstract). In *Theory of Cryptography Conference*; Springer: Berlin/Heidelberg, Germany, 2004; Volume 2951, pp. 278–296.
15. Standaert, F.; Malkin, T.; Yung, M. A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 2009; Volume 5479, pp. 443–461.
16. Wyner, A.D. On Source Coding with Side Information at The Decoder. *IEEE Trans. Inform. Theory* **1975**, *21*, 294–300.
17. Oohama, Y. Strong converse exponent for degraded broadcast channels at rates outside the capacity region. In Proceedings of the 2015 IEEE International Symposium on Information Theory (ISIT), Hong Kong, 14–19 June 2015; pp. 939–943.
18. Oohama, Y. Strong converse theorems for degraded broadcast channels with feedback. In Proceedings of the 2015 IEEE International Symposium on Information Theory (ISIT), Hong Kong, 14—19 June 2015; pp. 2510–2514.
19. Oohama, Y. New Strong Converse for Asymmetric Broadcast Channels. *arXiv* **2016**, arXiv:1604.02901.
20. Oohama, Y. Exponential Strong Converse for Source Coding with Side Information at the Decoder. *Entropy* **2018**, *20*, 352.
21. Csiszár, I.; Körner, J. *Information Theory, Coding Theorems for Discrete Memoryless Systems*, 2nd ed.; Cambridge University Press: Cambridge, UK, 2011.
22. Oohama, Y.; Han, T.S. Universal coding for the Slepian-Wolf data compression system and the strong converse theorem. *IEEE Trans. Inform. Theory* **1994**, *40*, 1908–1919.
23. Hayashi, M. Exponential Decreasing Rate of Leaked Information in Universal Random Privacy Amplification. *IEEE Trans. Inform. Theory* **2011**, *57*, 3989–4001.