entropy

MDPI

Article

Information Theoretic Security for Broadcasting of Two Encrypted Sources under Side-Channel Attacks †

Bagus Santoso *,‡ **and Yasutada Oohama** ‡

Department of Computer and Network Engineering, University of Electro-Communications, Tokyo 182-8585, Japan

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

† This paper is an extended version of our paper published in 2019 IEEE International Symposium on Information Theory (ISIT) *B. Santoso and Y. Oohama: "Secure Broadcasting of Two Encrypted Sources under Side-Channel Attacks", ISIT 2019.*

‡ Current address: 1-5-1 Chofugaoka, Tokyo 182-8585, Japan.

Received: 8 June 2019; Accepted: 6 August 2019; Published: 9 August 2019

Abstract: In this paper, we propose a theoretical framework to analyze the secure communication problem for broadcasting two encrypted sources in the presence of an adversary which launches side-channel attacks. The adversary is not only allowed to eavesdrop the ciphertexts in the public communication channel, but is also allowed to gather additional information on the secret keys via the side-channels, physical phenomenon leaked by the encryption devices during the encryption process, such as the fluctuations of power consumption, heat, or electromagnetic radiation generated by the encryption devices. Based on our framework, we propose a countermeasure against such adversary by using the post-encryption-compression (PEC) paradigm, in the case of one-time-pad encryption. We implement the PEC paradigm using affine encoders constructed from linear encoders and derive the explicit the sufficient conditions to attain the exponential decay of the information leakage as the block lengths of encrypted sources become large. One interesting feature of the proposed countermeasure is that its performance is independent from the type of side information leaked by the encryption devices.

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

1. Introduction

In recent years, it has become very common that one person holds multiple wireless communication devices and broadcasts the messages through multiple devices. In order to ensure secrecy, it is a standard practice to encrypt the data before broadcasting them into the public communication channel. The usual security problem that is considered in such system of broadcasting encrypted sources is the secrecy against an adversary which eavesdrops the ciphertexts sent via the public communication channel. However, Kocher et al. [1,2] have shown that an adversary may also learn "side" information about the secret keys from "side-channel", i.e., the measurements of physical phenomenon that occur in the physical devices where the encryption procedures are implemented. Such adversary is called as side-channel adversary. Examples of the physical phenomenon exploited by the side-channel adversaries are the fluctuations of time cost [1], the fluctuations of power consumption [2], and the electromagnetic (EM) radiation [3]. In this paper, we are focusing on a specific scenario where an adversary is not only eavesdropping on the public communication channel but is also launching side-channel attacks on multiple communication devices owned by a sender. We consider that this kind of side-channel attack is feasible in the real world when multiple devices owned

by the sender relocated in the same area such that the adversary can catch the side information from the devices directly.

1.1. Modelling Side-Channel Attacks

The adversarial/security model we use in this paper and its relation to a real-world example are shown in Figure 1. Basically, we adapt the approach in [4] on modeling the side-channel, where the side-channel is modelled as a rate constraint noiseless channel.

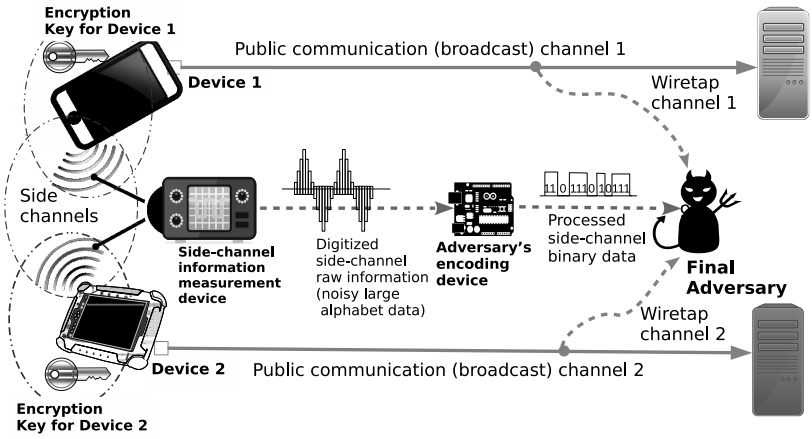

Figure 1. Side-channel attacks in a broadcasting system.

We describe our model in a more formal way as follows. Let us consider two sources X_1 and X_2, where each is encrypted in two different encryption devices using secret keys K_1 and K_2, respectively, resulting in ciphertexts C_1 and C_2, respectively. The ciphertexts C_1 and C_2 are sent by the sender to multiple receivers through multiple public communication channels. The adversary $\mathcal{A}$ is allowed to obtain: (1) ciphertexts C_1 and C_2 from the public communication channels, and also (2) "noisy" digital data Z generated by the probe or the measurement device from the physical phenomenon leaked by all encryption devices of the sender. The measurement device may just be a simple analog-to-digital converter that converts the analog data representing physical information leaked by the devices into "noisy" digital data Z. In our model, we represent the measurement process as a communication channel W.The adversary $\mathcal{A}$ is equipped with a side-channel encoding device $\varphi_{\mathcal{A}}$ which encodes and processes Z into the binary data $M_{\mathcal{A}}$. Finally, combining C_1, C_2, and $M_{\mathcal{A}}$, $\mathcal{A}$ will attempt to derive information on the sources X_1 and X_2.

1.2. Our Results and Methodology in Brief

We show that we can strengthen the secrecy/security of the Shannon ciphers which are implemented on multiple physical devices of a sender in a broadcasting system against an adversary who collects ciphertexts and launches side-channel attacks by a simple method of reencoding the ciphertexts before releasing them into the public communication channels. This method is based on post-encryption-compression (PEC) paradigm. We prove that, in the case that all encryption devices implement one time pad encryption, we can strengthen the secrecy/security using appropriate affine encoders φ_1 and φ_2 which transform the original ciphertexts C_1 and C_2 into reencoded ciphertexts $\widetilde{C}_1$ and $\widetilde{C}_2$.

More formally, we prove that, for any distribution of the secret keys (K_1, K_2) 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 $(R_1, R_2, R_{\mathcal{A}})$, where R_1 and R_2 are the encoding rates of φ_1 and φ_2, respectively, $R_{\mathcal{A}}$ is the encoding rate of adversary's encoding device $\varphi_{\mathcal{A}}$. More precisely, if we reencode C_1 and C_2 into $\widetilde{C}_1$ and $\widetilde{C}_2$ using φ_1 and φ_2 with encoding rates R_1 and R_2, respectively, such that R_1 and R_2 are inside the achievable region, then we can attain reliability and security in the following sense:

- anyone with secret keys K_1 and K_2 can construct appropriate decoders that decrypt and encode the reencoded ciphertexts $\widetilde{C}_1$ and $\widetilde{C}_2$ into original sources X_1 and X_2 with exponentially decaying error probability, and
- the amount of information on the sources X_1 and X_2 gained by any adversary $\mathcal{A}$ which collects the reencoded ciphertexts C_1, C_2 the encoded side-channel information $M_{\mathcal{A}}$ is exponentially decaying to zero as long as the side-channel encoding device $\varphi_{\mathcal{A}}$ encodes Z into $M_{\mathcal{A}}$ with the rate $R_{\mathcal{A}}$ which is inside the achievable rate region.

Taking the advantage of the homomorphic property of one-time-pad and affine encoding, we separate the theoretical analysis of reliability and security such that we can deal with each issue independently. For reliability analysis, similar to the analysis in [4–7], we mainly obtain our result by adapting the result of Csizár [8] on the universal coding using linear codes. Our main theorem on security is based on the technique developed in [4] which is actually a combination of two other techniques. One is a technique developed by Oohama in [9] for deriving approximation error exponents for the intrinsic randomness problem in some framework of distributed random number extraction. (This technique is is also used in the security analysis in Santoso and Oohama [6,10].) Another one is a technique proposed by Oohama [11] to establish exponential strong converse theorem for the one helper source coding problem. (This technique is used in the security analysis for the side channel attacks to the Shannon cipher system.)

In addition, since we model the side-channel as a rate constraint noiseless channel, all theoretical results in this paper are independent from the type of side-channel information the adversary collects from the encryption devices. This means that the countermeasure we propose in this paper can be applied against any type of side-channel attacks launched by the adversary, e.g., timing attacks, electromagnetic radiation or power analysis, and so on.

1.3. Related Works

The use of PEC for communication system can be traced back to the work by Johnson et al., in [12]. However, their main focus is the issue of reliability and they only provide weak secrecy for security, whereas, in this paper, we provide security based on the strong secrecy [13,14].

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. [15] and Coron et al. [16] propose a statistical model for side-channel attacks using the information from power consumption and the running time, whereas Agrawal et al. [3] 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. [17] and Backes et al. [18], but they are heavily dependent upon implementation on certain specific devices. Micali et al. [19] 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. One of the closest existing models to ours is the general framework for analyzing side-channel attacks proposed by Standaert et al. [20]. However, the authors of [20] 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 [20] depends on the characteristics of the leaked physical information. Another model that is similar to ours in the sense that it is independent from the type of leaked physical information is proposed by Chérisey et al. [21,22]. However, the main aim of [21,22] is only establishing the mathematical link between success probability of side-channel adversary and mutual information and no countermeasure is proposed.

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 state our main theorem on the reliability and security of our solution. In Section 5, we show the proof of our main theorem. In Section 6, we discuss an alternative formulation of our model and problem. In Section 7, we show the comparison between our current results in this paper and our previous works. We put our conclusions in Section 9. We put the proofs of other related propositions, lemmas, and theorems in the appendix.

2. Problem Formulation

2.1. Preliminaries

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

Random Source of Information and Key: For each $i = 1, 2$, let X_i be a random variable from a finite set $\mathcal{X}_i$. For each $i = 1, 2$, let $\{X_{i,t}\}_{t=1}^{\infty}$ be two stationary discrete memoryless sources (DMS) such that, for each $t = 1, 2, \ldots$, $X_{i,t}$ take values in finite set $\mathcal{X}_i$ and has the same distribution as that of X_i denoted by $p_{X_i} = \{p_{X_i}(x_i)\}_{x_i \in \mathcal{X}_i}$. The stationary DMS $\{X_{i,t}\}_{t=1}^{\infty}$, are specified with p_{X_i}.

We next define the two keys used in the two common cryptosystems. For each $i = 1, 2$, let (K_1, K_2) be a pair of two correlated random variables taken from the same finite set $\mathcal{X}_1 \times \mathcal{X}_2$. Let $\{(K_{1,t}, K_{2,t})\}_{t=1}^{\infty}$ be a stationary discrete memoryless source such that, for each $t = 1, 2, \ldots$, $(K_{1,t}, K_{2,t})$ takes values in $\mathcal{X}_1 \times \mathcal{X}_2$ and has the same distribution as that of (K_1, K_2) denoted by

$$p_{K_1K_2} = \{p_{K_1K_2}(k_1, k_2)\}_{(k_1,k_2) \in \mathcal{X}_1 \times \mathcal{X}_2}.$$

The stationary DMS $\{(K_{1,t}, K_{2,t}\}_{t=1}^{\infty}$ is specified with $p_{K_1K_2}$.

Random Variables and Sequences: We write the sequence of random variables with length n from the information sources as follows: $X_i^n := X_{i,1}X_{i,2} \cdots X_{i,n}, i = 1, 2$. Similarly, the strings with length n of $\mathcal{X}_i^n$ are written as $x_i^n := x_{i,1}x_{i,2} \cdots x_{i,n} \in \mathcal{X}_i^n$. For $(x_1^n, x_2^n) \in \mathcal{X}_1^n \times \mathcal{X}_2^n$, $p_{X_1^nX_2^n}(x_1^n, x_2^n)$ stands for the probability of the occurrence of (x_1^n, x_2^n). When the information source is memoryless specified with $p_{X_1X_2}$, we have the following equation holds:

$$p_{X_1^nX_2^n}(x_1^n, x_2^n) = \prod_{t=1}^{n} p_{X_1X_2}(x_{1,t}, x_{2,t}).$$

In this case, we write $p_{X_1^nX_2^n}(x_1^n, x_2^n)$ as $p_{X_1X_2}^n(x_1^n, x_2^n)$. Similar notations are used for other random variables and sequences.

Consensus and Notations: Without loss of generality, throughout this paper, we assume that X_1 and X_2 are finite fields. 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 from the same finite field. All discussions and theorems in this paper still hold although X_1 and X_2 are different finite fields. However, for the sake of simplicity, we use the same notation for field addition and subtraction for both X_1 and X_2. 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 basic adversarial model we consider in this paper. First, let the information source and the key be generated independently by three different parties $\mathcal{S}_{\mathsf{gen},1}$, $\mathcal{S}_{\mathsf{gen},2}$ and $\mathcal{K}_{\mathsf{gen}}$, respectively. In our setting, we assume the following:

- The random keys K_1^n and K_2^n are generated by $\mathcal{K}_{\mathsf{gen}}$ from uniform distribution. We may have a correlation between K_1^n and K_2^n.
- The sources X_1^n and X_2^n, respectively, are generated by $\mathcal{S}_{\mathsf{gen},1}$ and $\mathcal{S}_{\mathsf{gen},2}$. Those are independent from the keys.

Next, let the two random sources X_1^n and X_2^n, respectively, from $\mathcal{S}_{\mathsf{gen},1}$ and $\mathcal{S}_{\mathsf{gen},2}$ be sent to two separated nodes L_1 and L_2. In addition, let two random key (sources) K_1^n and K_2^n from $\mathcal{K}_{\mathsf{gen}}$ be also sent separately to L_1 and L_2. Further settings of our system are described as follows. Those are also shown in Figure 2.

1. *Separate Sources Processing:* For each $i = 1, 2$, at the node L_i, X_i^n is encrypted with the key K_i^n using the encryption function Enc_i. The ciphertext C_i^n of X_i^n is given by $C_i^n := \mathsf{Enc}_i(X_i^n) = X_i^n \oplus K_i^n$.
2. *Transmission:* The ciphertexts C_1^n and C_2^n, respectively, are sent to the information processing center D_1 and D_2 through two *public* communication channels. Meanwhile, the keys K_1^n and K_2^n, respectively are sent to D_1 and D_2 through two *private* communication channels.
3. *Sink Nodes Processing:* For each $i = 1, 2$, in D_i, we decrypt the ciphertext C_i^n using the key K_i^n through the corresponding decryption procedure Dec_i defined by $\mathsf{Dec}_i(C_i^n) = C_i^n \ominus K_i^n$. It is obvious that we can correctly reproduce the source output X^n from C_i^n and K_i^n by the decryption function Dec_i.

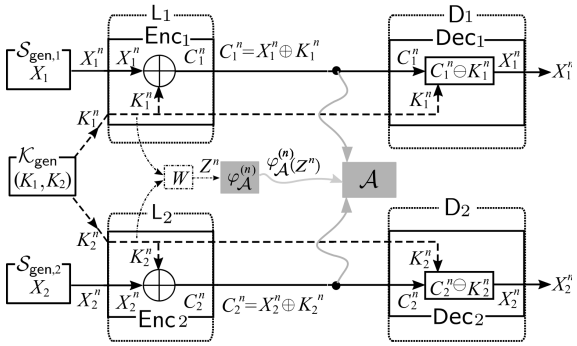

Figure 2. Side-channel attacks to the two Shannon cipher systems.

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 a side information obtained by side-channel attacks. Let $\mathcal{Z}$ be a finite set and let $W : \mathcal{X}_1 \times \mathcal{X}_2 \to \mathcal{Z}$ be a noisy channel. Let Z be a channel output from W for the input random 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 $(K_1^n, K_2^n) \in \mathcal{X}_1^n \times \mathcal{X}_2^n$ to the input of channel. We write a conditional distribution on Z^n given (K_1^n, K_2^n) as

$$W^n = \{W^n(z^n|k_1^n, k_2^n)\}_{(k_1^n, k_2^n, z^n) \in \mathcal{X}_1^n \times \mathcal{X}_2^n \times \mathcal{Z}^n}.$$

Since the channel is memoryless, we have

$$W^n(z^n|k_1^n, k_2^n) = \prod_{t=1}^{n} W(z_t|k_{1,t}, k_{2,t}). \tag{1}$$

On the above output Z^n of W^n for the input (K_1^n, K_2^n), we assume the following:

- The two random pairs (X_1, X_2), (K_1, K_2) and the random variable Z, satisfy $(X_1, X_2) \perp (K_1, K_2, Z)$, which implies that $(X_1^n, X_2^n) \perp (K_1^n, K_2^n, Z^n)$.
- By side-channel attacks, the adversary $\mathcal{A}$ can access Z^n.

We next formulate 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 $\varphi_{\mathcal{A}} := \{\varphi_{\mathcal{A}}^{(n)}\}_{n=1,2,\cdots}$. 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

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

On 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, $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$.

As a solution to the side channel attacks, we consider a system of broadcast encryption with post-encryption coding. We call this system as Sys. The illustration of Sys is shown in Figure 3.

1. *Encoding at Source node* $\mathsf{L}_i, i = 1, 2$*:* For each $i = 1, 2$, we first use $\varphi_i^{(n)}$ to encode the ciphertext $C_i^n = X_i^n \oplus K_i^n$. A formal definition of $\varphi_i^{(n)}$ is $\varphi_i^{(n)} : \mathcal{X}_i^n \to \mathcal{X}_i^{m_i}$. Let $\widetilde{C}_i^{m_i} = \varphi_i^{(n)}(C_i^n)$. Instead of sending C_i^n, we send $\widetilde{C}_i^{m_i}$ to the public communication channel.
2. *Decoding at Sink Nodes* $\mathsf{D}_i, i = 1, 2$*:* For each $i = 1, 2$, D_i receives $\widetilde{C}_i^{m_i}$ from a public communication channel. Using common key K_i^n and the decoder function $\Psi_i^{(n)} : \mathcal{X}_i^m \times \mathcal{X}_i^n \to \mathcal{X}_i^n$, D_i outputs an estimation $\hat{X}_i^n = \Psi_i^{(n)}(\tilde{C}_i^{m_i}, K_i^n)$ of X_i^n.

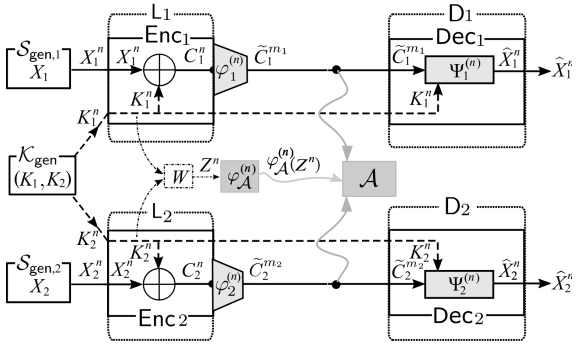

Figure 3. Sys: a system of broadcast encryption with post-encryption coding.

On Reliability and Security: From the description of our system in the previous section, the decoding process in our system above is successful if $\widehat{X}_i^n = X_i^n$ holds. Combining this and Equation (5), it is clear that the decoding error probabilities $p_{\mathrm{e},i}, i = 1, 2$, are as follows:

$$p_{\mathrm{e},i} = p_{\mathrm{e}}(\varphi_i^{(n)}, \Psi_i^{(n)} | p_{X_i}^n) := \Pr[\Psi_i^{(n)}(\varphi_i^{(n)}(X_i^n)) \neq X_i^n].$$

Set $M_{\mathcal{A}}^{(n)} = \varphi_{\mathcal{A}}^{(n)}(Z^n)$. The information leakage $\Delta^{(n)}$ on (X_1^n, X_2^n) from $(\widetilde{C}_1^{m_1}, \widetilde{C}_2^{m_2}, M_{\mathcal{A}}^{(n)})$ is measured by the mutual information between (X_1^n, X_2^n) and $(\widetilde{C}_1^{m_1}, \widetilde{C}_2^{m_2}, M_{\mathcal{A}}^{(n)})$. This quantity is formally defined by

$$\Delta^{(n)} = \Delta^{(n)}(\varphi_1^{(n)}, \varphi_2^{(n)}, \varphi_{\mathcal{A}}^{(n)} | p_{X_1X_2}^n, p_{ZK_1K_2}^n) := I(X_1^n X_2^n; \widetilde{C}_1^{m_2}, \widetilde{C}_2^{m_2}, M_{\mathcal{A}}^{(n)}).$$

Reliable and Secure Framework:

Definition 1. *A pair* (R_1, R_2) *is achievable under* $R_{\mathcal{A}} > 0$ *for the system* Sys *if there exists two sequences* $\{(\varphi_i^{(n)}, \Psi_i^{(n)})\}_{n \geq 1}, i = 1, 2$*, such that* $\forall \epsilon > 0$, $\exists n_0 = n_0(\epsilon) \in \mathbb{N}_0$, $\forall n \geq n_0$*, we have for* $i = 1, 2$*,*

$$\frac{1}{n} \log |\mathcal{X}_i^{m_i}| = \frac{m_i}{n} \log |\mathcal{X}_i| \leq R_i, p_{\mathrm{e}}(\varphi_i^{(n)}, \Psi_i^{(n)} | p_{X_i}^n) \leq \epsilon,$$

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

$$\Delta^{(n)}(\varphi_1^{(n)}, \varphi_2^{(n)}, \varphi_{\mathcal{A}}^{(n)} | p_{X_1X_2}^n, p_{ZK_1K_2}^n) \leq \epsilon.$$

Definition 2 (Reliable and Secure Rate Region). *Let $\mathcal{R}_{\mathsf{Sys}}(p_{X_1X_2}, p_{ZK_1K_2})$ denote the set of all $(R_{\mathcal{A}}, R)$ such that R is achievable under $R_{\mathcal{A}}$. We call $\mathcal{R}_{\mathsf{Sys}}(p_{X_1X_2}, p_{ZK_1K_2})$ the* **reliable and secure rate** *region.*

Definition 3. *A five tuple (R_1, R_2, E_1, E_2, F) is achievable under $R_{\mathcal{A}} > 0$ for the system* Sys *if there exists a sequence $\{(\varphi_i^{(n)}, \Psi_i^{(n)})\}_{n\geq 1}$, $i = 1, 2$, such that $\forall \epsilon > 0$, $\exists n_0 = n_0(\epsilon) \in \mathbb{N}_0$, $\forall n \geq n_0$, we have for $i = 1, 2$,*

$$\frac{1}{n} \log |\mathcal{X}_i^{m_i}| = \frac{m_i}{n} \log |\mathcal{X}_i| \leq R_i, p_{\mathrm{e}}(\varphi_i^{(n)}, \Psi_i^{(n)} | p_{X_i}^n) \leq \mathrm{e}^{-n(E_i - \epsilon)},$$

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

$$\Delta^{(n)}(\varphi_1^{(n)}, \varphi_2^{(n)}, \varphi_{\mathcal{A}}^{(n)} | p_{X_1X_2}^n, p_{ZK_1K_2}^n) \leq \mathrm{e}^{-n(F - \epsilon)}.$$

Definition 4 (Rate, Reliability, and Security Region). *Let $\mathcal{D}_{\mathsf{Sys}}(p_{X_1X_2}, p_{K_1K_2}, W)$ denote the set of all $(R_{\mathcal{A}}, R, E, F)$ such that (R_1, R_2, E_1, E_2, F) is achievable under $R_{\mathcal{A}}$. We call $\mathcal{D}_{\mathsf{Sys}}(p_{X_1X_2}, p_{K_1K_2}, W)$ the* **rate, reliability, and security** *region.*

3. Proposed Idea: Affine Encoder as Privacy Amplifier

For each $n = 1, 2, \cdots$, let $\phi_i^{(n)} : \mathcal{X}_i^n \to \mathcal{X}_i^{m_i}$ be a linear mapping. We define the mapping $\phi_i^{(n)}$ by

$$\phi_i^{(n)}(x_i^n) = x_i^n A_i \text{ for } x_i^n \in \mathcal{X}_i^n, \tag{2}$$

where A_i is a matrix with n rows and m_i columns. Entries of A_i are from $\mathcal{X}_i$. We fix $b_i^{m_i} \in \mathcal{X}_i^{m_i}$. Define the mapping $\varphi_i^{(n)} : \mathcal{X}_i^n \to \mathcal{X}_i^{m_i}$ by

$$\varphi_i^{(n)}(k_i^n) := \phi_i^{(n)}(k_i^n) \oplus b_i^{m_i} = k_i^n A_i \oplus b_i^{m_i}, \text{ for } k_i^n \in \mathcal{X}_i^n.$$

The mapping $\varphi_i^{(n)}$ is called the affine mapping induced by the linear mapping $\phi_i^{(n)}$ and constant vector $b_i^{m_i} \in \mathcal{X}_i^{m_i}$. By the definition of $\varphi_i^{(n)}$, the following affine structure holds:

$$\begin{aligned} \varphi_i^{(n)}(x_i^n \oplus k_i^n) &= (x_i^n \oplus k_i^n) A_i \oplus b_i^{m_i} = x_i^n A_i \oplus (k_i^n A_i \oplus b_i^{m_i}) \\ &= \phi_i^{(n)}(x_i^n) \oplus \varphi_i^{(n)}(k_i^n), \text{ for } x_i^n, k_i^n \in \mathcal{X}_i^n. \end{aligned} \tag{3}$$

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

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

1. *Encoding at Source node* $\mathsf{L}_i, i = 1, 2$*:* First, we use $\varphi_i^{(n)}$ to encode the ciphertext $C_i^n = X_i^n \oplus K_i^n$ Let $\widetilde{C}_i^{m_i} = \varphi_i^{(n)}(C_i^n)$. Then, instead of sending C^n, we send $\tilde{C}_i^{m_i}$ to the public communication channel. By the affine structure (3) of encoder, we have that

$$\widetilde{C}_i^{m_i} = \varphi_i^{(n)}(X_i^n \oplus K_i^n) = \phi_i^{(n)}(X_i^n) \oplus \varphi_i^{(n)}(K_i^n) = \widetilde{X}_i^{m_i} \oplus \widetilde{K}_i^{m_i}, \tag{4}$$

   where we set $\widetilde{X}_i^{m_i} := \phi_i^{(n)}(X_i^n), \widetilde{K}_i^{m_i} := \varphi_i^{(n)}(K_i^n)$.
2. *Decoding at Sink Node* $\mathsf{D}_i, i = 1, 2$*:* First, using the linear encoder $\varphi_i^{(n)}$, D_i encodes the key K_i^n received through private channel into $\widetilde{K}_i^{m_i} = \varphi_i^{(n)}(K_i^n)$. Receiving $\widetilde{C}_i^{m_i}$ from public communication

channel, D_i computes $\widetilde{X}_i^{m_i}$ in the following way. From (4), we have that the decoder D_i can obtain $\widetilde{X}_i^{m_i} = \phi_i^{(n)}(X_i^n)$ by subtracting $\widetilde{K}_i^{m_i} = \varphi_i^{(n)}(K_i^n)$ from $\widetilde{C}_i^{m_i}$. Finally, D_i outputs $\widehat{X}_i^n$ by applying the decoder $\psi_i^{(n)}$ to $\widetilde{X}_i^{m_i}$ as follows:

$$\widehat{X}_i^n = \psi_i^{(n)}(\widetilde{X}_i^{m_i}) = \psi_i^{(n)}(\phi_i^{(n)}(X_i^n)). \tag{5}$$

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

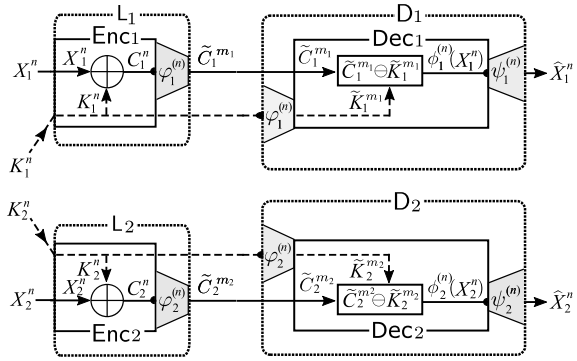

Figure 4. Our proposed countermeasure: affine encoders as privacy amplifiers.

4. Main Results

In this section, we state our main results. To describe our results, we define several functions and sets. 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_1, K_2) is

$$p_{UZK_1K_2}(u, z, k_1, k_2) = p_U(u)p_{Z|U}(z|u)p_{K_1K_2|Z}(k_1, k_2|z).$$

The above condition is equivalent to $U \leftrightarrow Z \leftrightarrow (K_1, K_2)$. In the following argument for convenience of descriptions of definitions, we use the following notations:

$$R_3 := R_1 + R_2, \mathcal{X}_3 := \mathcal{X}_1 \times \mathcal{X}_2, k_3 := (k_1, k_2), K_3 := (K_1, K_2).$$

For each $i = 1, 2, 3$, we simply write $p_i = p_{UZK_i}$. Specifically, for $i = 3$, we have $p_3 = p_{UZK_1K_2} = p$. Define the three sets of probability distribution with $i = 1, 2, 3$:

$$\mathcal{P}(p_{ZK_i}) := \{p_{UZK_i} : |\mathcal{U}| \leq |\mathcal{Z}| + 1, U \leftrightarrow Z \leftrightarrow K_i\}. \tag{6}$$

For $i = 1, 2, 3$, let us define as follows:

$$\mathcal{R}_i(p_i) := \{(R_\mathcal{A}, R_i) : R_\mathcal{A}, R_i \geq 0,\ R_\mathcal{A} \geq I(Z; U), R_i \geq H(K_i|U)\}, \tag{7}$$

$$\mathcal{R}_i(p_{ZK_i}) := \bigcup_{p_i \in \mathcal{P}(p_{ZK_i})} \mathcal{R}_i(p_i). \tag{8}$$

The two regions $\mathcal{R}_i(p_{ZK_i}), i = 1, 2$ have the same form as the region appearing as the admissible rate region in the one-helper source coding problem posed and investigated by Ahlswede and Körner [23]. We can show that the region $\mathcal{R}_i(p_{ZK_i}), i = 1, 2$, and $\mathcal{R}_3(p_{ZK_1K_2})$ satisfy the following property.

Property 1.

(a) *The region $\mathcal{R}_i(p_{ZK_i}), i = 1, 2$ is a closed convex subset of $\mathbb{R}_+^2$. The region $\mathcal{R}_3(p_{ZK_1K_2})$ is a closed convex subset of $\mathbb{R}_+^3$.*

(b) *The bound $|\mathcal{U}| \leq |\mathcal{Z}| + 1$ is sufficient to describe $\mathcal{R}_i(p_{ZK_i}), i = 1, 2, 3$.*

We define several quantities to state our main result. Let $i \in \{1,2\}$. We first define a function related to an exponential upper bound of $p_{\mathrm{e}}(\phi_i^{(n)}, \psi_i^{(n)} | p_{X_i}^n)$. Let $\overline{X}_i$ be an arbitrary random variable over $\mathcal{X}_i$ and has a probability distribution $p_{\overline{X}_i}$. Let $\mathcal{P}(\mathcal{X}_i)$ denote the set of all probability distributions on $\mathcal{X}_i$. For $R_i \geq 0$ and $p_{X_i} \in \mathcal{P}(\mathcal{X}_i)$, we define the following function:

$$E(R_i|p_{X_i}) := \min_{p_{\overline{X}_i} \in \mathcal{P}(\mathcal{X}_i)} \{[R_i - H(\overline{X}_i)]^+ + D(p_{\overline{X}_i}||p_{X_i})\}. \tag{9}$$

We next define a function related to an exponential upper bound of $\Delta^{(n)}(\varphi_1^{(n)}, \varphi_2^{(n)}, \varphi_{\mathcal{A}}^{(n)} | p_{X_1X_2}^n, p_{ZK_1K_2}^n)$. For each $i = 1,2,3$, we define three sets of probability distributions on $\mathcal{U} \times \mathcal{Z} \times \mathcal{X}_i$ by

$$\tilde{\mathcal{P}}(p_{ZK_i}) := \{p = p_{UZK_i} : |\mathcal{U}| \leq |\mathcal{Z}|, U \leftrightarrow Z \leftrightarrow K_i\}.$$

Furthermore, for each $i = 1,2,3$, we define three sets of probability distributions on $\mathcal{U} \times \mathcal{Z} \times \mathcal{X}_i$ by

$$\mathcal{Q}(p_{K_i|Z}) := \{q_i = q_{UZK_i} : q_{K_iZ|U} = p_{K_iZ|U} : \text{ for some } p_i \in \tilde{\mathcal{P}}(p_{ZK_i})\}.$$

For each $i = 1,2,3$, for $(\mu, \alpha) \in [0,1]^2$, and for $q_i = q_{UZK_i} \in \mathcal{Q}(p_{K_i|Z})$, define

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

In [11] (extended version), Oohama proved several properties on $F(R_{\mathcal{A}}, R_i|p_{ZK_i}), i = 1,2,3$. According to [11] (extended version), we have the following property.

Property 2. *For any $i = 1,2,3$ and for any $\tau \in (0, (1/2)\rho(p_{ZK_i}))$, the condition $(R_{\mathcal{A}}, R_i + \tau) \notin \mathcal{R}_i(p_{ZK_i})$ implies*

$$F(R_{\mathcal{A}}, R_i|p_{ZK_i}) > \frac{\rho(p_{ZK_i})}{4} \cdot g^2\left(\frac{\tau}{\rho(p_{ZK_i})}\right) > 0,$$

where $\rho(p_{ZK_i}), i = 1,2,3$, respectively, are some quantities depending on p_{ZK_i} and g is the inverse function of $\vartheta(a) := a + (5/4)a^2, a \geq 0$.

Let us define as follows:

$$F_{\min}(R_{\mathcal{A}}, R_1, R_2 | p_{ZK_1K_2}) := \min_{i=1,2,3} F(R_{\mathcal{A}}, R_i | p_{ZK_i}). \tag{10}$$

Our main result is as follows.

Theorem 1. *For any $R_{\mathcal{A}}, R_1, R_2 > 0$ and any $p_{ZK_1K_2}$, there exists two sequence of mappings $\{(\varphi_i^{(n)}, \psi_i^{(n)})\}_{n=1}^{\infty}, i = 1,2$ such that, for any $p_{X_i}, i = 1,2$, and any $n \geq (R_1 + R_2)^{-1}$, we have*

$$\begin{aligned}
\frac{1}{n} \log |\mathcal{X}_i^{m_i}| &= \frac{m_i}{n} \log |\mathcal{X}_i| \leq R_i, \\
p_{\mathrm{e}}(\phi_i^{(n)}, \psi_i^{(n)} | p_{X_i}^n) &\leq \mathrm{e}^{-n[E(R_i|p_{X_i}) - \delta_{i,n}]}, i = 1,2
\end{aligned} \tag{11}$$

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

$$\Delta^{(n)}(\varphi_1^{(n)}, \varphi_2^{(n)}, \varphi_{\mathcal{A}}^{(n)} | p_{X_1X_2}^n, p_{K_1K_2}^n, W^n) \le \mathrm{e}^{-n[F_{\min}(R_{\mathcal{A}}, R_1, R_2 | p_{ZK_1K_2}) - \delta_{3,n}]}, \tag{12}$$

where $\delta_{i,n}, i = 1, 2, 3$ are defined by

$$\delta_{i,n} := \frac{1}{n} \log \left[\mathrm{e}(n+1)^{2|\mathcal{X}_i|} \times \left\{ 1 + (n+1)^{|\mathcal{X}_1|} + (n+1)^{|\mathcal{X}_2|} \right\} \right], \text{ for } i = 1, 2,$$
$$\delta_{3,n} := \frac{1}{n} \log \left[15n(R_1 + R_2) \times \left\{ 1 + (n+1)^{|\mathcal{X}_1|} + (n+1)^{|\mathcal{X}_2|} \right\} \right].$$

Note that, for $i = 1, 2, 3$, $\delta_{i,n} \to 0$ as $n \to \infty$.

Detail of the proof of Theorem 1 will be explained in Section 5.

The functions $E(R_i | p_{X_i})$ and $F(R_{\mathcal{A}}, R_1, R_2 | p_{ZK_1K_2})$ take positive values if $(R_{\mathcal{A}}, R_1, R_2)$ belongs to the set

$$\mathcal{R}_{\mathrm{Sys}}^{(\mathrm{in})}(p_{X_1X_2}, p_{ZK_1K_2}) := \{R_1 > H(X_1)\} \cap \{R_2 > H(X_2)\} \bigcap_{i=1,2,3} \mathcal{R}_i^{\mathrm{c}}(p_{ZK_i}).$$

Thus, by Theorem 1, under $(R_{\mathcal{A}}, R_1, R_2) \in \mathcal{R}_{\mathrm{Sys}}^{(\mathrm{in})}(p_{X_1X_2}, p_{ZK_1K_2})$, we have the following:

- On the reliability, for $i = 1, 2$, $p_{\mathrm{e}}(\phi_i^{(n)}, \psi_i^{(n)} | p_{X_i}^n)$ goes to zero exponentially as n tends to infinity, and its exponent is lower bounded by the function $E(R_i | p_{X_i})$.
- On the security, for any $\varphi_{\mathcal{A}}$ satisfying $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$, the information leakage $\Delta^{(n)}(\varphi_1^{(n)}, \varphi_2^{(n)}, \varphi_{\mathcal{A}}^{(n)} | p_{X_1X_2}^n, p_{ZK_1K_2}^n)$ on X_1^n, X_2^n goes to zero exponentially as n tends to infinity, and its exponent is lower bounded by the function $F_{\min}(R_{\mathcal{A}}, R_1, R_2 | p_{ZK_1K_2})$.
- For each $i = 1, 2$, any code $(\phi_i^{(n)}, \psi_i^{(n)})$ that attains the exponent function $E(R_i | p_{X_i})$ is a universal code that depends only on R_i not on the value of the distribution p_{X_i}.

Define

$$\mathcal{D}_{\mathrm{Sys}}^{(\mathrm{in})}(p_{X_1X_1}, p_{ZK_1K_2}) := \{(R_{\mathcal{A}}, R_1, R_2, E(R_1 | p_{X_1}), E(R_2 | p_{X_2}), F_{\min}(R_{\mathcal{A}}, R_1, R_2 | p_{K_1K_2})) : (R_1, R_2) \in \mathcal{R}_{\mathrm{Sys}}^{(\mathrm{in})}(p_{X_1X_2}, p_{ZK_1K_2})\}.$$

From Theorem 1, we obtain the following corollary:

Corollary 1.

$$\mathcal{R}_{\mathrm{Sys}}^{(\mathrm{in})}(p_{X_1X_1}, p_{ZK_1K_2}) \subseteq \mathcal{R}_{\mathrm{Sys}}(p_{X_1X_1}, p_{ZK_1K_2}),$$
$$\mathcal{D}_{\mathrm{Sys}}^{(\mathrm{in})}(p_{X_1X_1}, p_{ZK_1K_2}) \subseteq \mathcal{D}_{\mathrm{Sys}}(p_{X_1X_1}, p_{ZK_1K_2}).$$

Remark 1. *Note that, from the definitions of sets $\mathcal{P}(p_{ZK_i})$, $\mathcal{R}_i(p_{ZK_i})$, it is easy to see that the set $\mathcal{R}_{\mathrm{Sys}}^{(\mathrm{in})}(p_{X_1X_1}, p_{ZK_1K_2})$ is the intersection of the outer regions of all possible adversarial encoding of $\mathcal{A}$ (where each encoding is represented by one auxiliary variable U) within rate $R_{\mathcal{A}}$. Moreover, since we use the strong converse theorem developed in [11] instead of the weak converse, we can guarantee that in $\mathcal{R}_{\mathrm{Sys}}^{(\mathrm{in})}(p_{X_1X_1}, p_{ZK_1K_2})$, not only the adversarial decoding success probability, but also the information leakage decays to zero at an exponential rate.*

Remark 2. *Thanks to the separation between reliability and security analysis, the results related security in this paper will still hold even in the case where the sources are correlated. Moreover, our proposed countermeasure*

can strengthen the secrecy even in the case where the marginal distribution of each key K_i, i.e., p_{K_i}, $(i = 1, 2)$ is not uniform.

4.1. Examples of Extremal Cases

In the remaining part of this section, we give two simple examples of $\mathcal{R}_{\text{Sys}}^{(\text{in})}(p_{X_1X_1}, p_{ZK_1K_2})$. Those correspond to extremal cases on the correlation of (K_1, K_2, Z). In those two examples, we assume that $\mathcal{X}_1 = \mathcal{X}_2 = \{0, 1\}$ and $p_{X_1}(1) = s_1, p_{X_2}(1) = s_2$. We further assume that p_{K_1,K_2} has the binary symmetric distribution given by

$$p_{K_1K_2}(k_1, k_2) = (1/2)\left[\bar{\rho}k_1 \oplus k_2 + \rho\overline{k_1 \oplus k_2}\right] \text{ for } (k_1, k_2) \in \{0, 1\}^2,$$

where $\rho \in [0, 0.5]$ is a parameter indicating the correlation level of (K_1, K_2).

Example 1. *We consider the case where $W = p_{Z|K_1K_2}$ is given by*

$$W(z|k_1, k_2) = W(z|k_1) = \overline{\rho_{\mathcal{A}}}k_1 \oplus z + \rho_{\mathcal{A}}\overline{k_1 \oplus z} \quad \text{for } (k_1, k_2, z) \in \{0, 1\}^3.$$

In this case, we have $K_2 \leftrightarrow K_1 \leftrightarrow Z$. This corresponds to the case where the adversary $\mathcal{A}$ attacks only node L_1. Let $N_{\mathcal{A}}$ be a binary random variable with $p_{N_{\mathcal{A}}}(1) = \rho_{\mathcal{A}}$. We assume that $N_{\mathcal{A}}$ is independent from (X_1, X_2) and (K_1, K_2). Using $N_{\mathcal{A}}$, Z can be written as $Z = K_1 \oplus N_{\mathcal{A}}$. The inner bound for this example denoted by $\mathcal{R}_{\text{Sys,ex1}}^{(\text{in})}(p_{X_1X_2}, p_{ZK_1K_2})$ is the following:

$$\begin{aligned}\mathcal{R}_{\text{Sys,ex1}}^{(\text{in})}(p_{X_1X_2}, p_{ZK_1K_2}) = \{(R_{\mathcal{A}}, R_1, R_2) :& 0 \le R_{\mathcal{A}} \le \log 2 - h(\theta),\\ & h(s_1) < R_1 < h(\rho_{\mathcal{A}} * \theta),\\ & h(s_2) < R_2 < h\left((\rho * \rho_{\mathcal{A}}) * \theta\right),\\ & R_1 + R_2 < h(\rho) + h(\rho_{\mathcal{A}} * \theta) \text{ for some } \theta \in [0, 1]\},\end{aligned} \tag{13}$$

where $h(\cdot)$ denotes the binary entropy function and $a * b := a\bar{b} + \bar{a}b$.

One can easily compute $\mathcal{R}_{\text{Sys,ex1}}^{(\text{in})}(p_{X_1X_2}, p_{ZK_1K_2})$ based on the solution for the problem of lossless source coding with helper, which is explained in [24]. The computation of $\mathcal{R}_{\text{Sys,ex1}}^{(\text{in})}(p_{X_1X_2}, p_{ZK_1K_2})$ is given in Appendix A.

Example 2. *We consider the case of $\rho = 0.5$. In this case, K_1 and K_2 is independent. In this case, we have no information leakage if $R_{\mathcal{A}} = 0$. We assume that $W = p_{Z|K_1K_2}$ is given by*

$$W(z|k_1, k_2) = \overline{\rho_{\mathcal{A}}}k_1 \oplus k_2 \oplus z + \rho_{\mathcal{A}}\overline{k_1 \oplus k_2 \oplus z} \quad \text{for } (k_1, k_2, z) \in \{0, 1\}^3.$$

Let $N_{\mathcal{A}}$ be the same random variable as the previous example. Using $N_{\mathcal{A}}$, Z can be written as $Z = K_1 \oplus K_2 \oplus N_{\mathcal{A}}$. The inner bound in this example denoted by $\mathcal{R}_{\text{Sys,ex2}}^{(\text{in})}(p_{X_1X_2}, p_{ZK_1K_2})$ is the following:

$$\begin{aligned}\mathcal{R}_{\text{Sys,ex2}}^{(\text{in})}(p_{X_1X_2}, p_{ZK_1K_2}) = \{(R_{\mathcal{A}}, R_1, R_2) :& 0 \le R_{\mathcal{A}} \le \log 2 - h(\theta),\\ & h(s_i) < R_i < \log 2, i = 1, 2,\\ & R_1 + R_2 < \log 2 + h(\rho_{\mathcal{A}} * \theta) \text{ for some } \theta \in [0, 1]\}.\end{aligned} \tag{14}$$

Similar to Example 1, one can also easily compute $\mathcal{R}_{\text{Sys,ex2}}^{(\text{in})}(p_{X_1X_2}, p_{ZK_1K_2})$ based on the solution for the problem of lossless source coding with helper, which is explained in [24]. Computation of $\mathcal{R}_{\text{Sys,ex2}}^{(\text{in})}(p_{X_1X_2}, p_{ZK_1K_2})$ is given in Appendix B.

For the above two examples, we show the section of the regions $\mathcal{R}^{(\mathrm{in})}_{\mathrm{Sys,exi}}(p_{X_1X_2}, p_{ZK_1K_2})$ for $i = 1, 2$ by the plane $\{R_{\mathcal{A}} = \log 2 - h(\theta)\}$, which is shown in Figure 5.

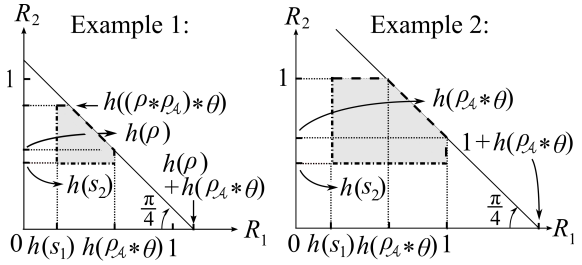

Figure 5. Shape of the regions $\mathcal{R}^{(\mathrm{in})}_{\mathrm{Sys,exi}}(p_{X_1X_2}, p_{ZK_1K_2}) \cap \{R_{\mathcal{A}} = 1 - h(\theta)\}$,$i =, 1, 2$.

5. Proofs of the Main Results

In this section, we prove Theorem 1.

5.1. Types of Sequences and Their Properties

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

Definition 5. *For each $i = 1, 2$ and for any n-sequence $x_i^n = x_{i,1}x_{i,2}\cdots x_{i,n} \in \mathcal{X}^n$, $n(x_i|x_i^n)$ denotes the number of t such that $x_{i,t} = x_i$. The relative frequency $\{n(x_i|x_i^n)/n\}_{x_i\in\mathcal{X}_i}$ of the components of x_i^n is called the type of x_1^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 $\overline{\mathrm{X}}_i$ denote an arbitrary random variable whose distribution $P_{\overline{\mathrm{X}}_i}$ belongs to $\mathcal{P}_n(\mathcal{X}_i)$. For $p_{\overline{\mathrm{X}}_i} \in \mathcal{P}_n(\mathcal{X}_i)$, set*

$$T^n_{\overline{\mathrm{X}}_i} := \left\{x_i^n : P_{x_i^n} = p_{\overline{\mathrm{X}}_i}\right\}.$$

For set of types and joint types, the following lemma holds. For the detail of the proof, see Csiszár and Körner [25].

Lemma 1.

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

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

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

(c) *For $x_i^n \in T^n_{\overline{\mathrm{X}}_i}$,*

$$p^n_{\mathrm{X}_i}(x_i^n) = \mathrm{e}^{-n[H(\overline{\mathrm{X}}_i)+D(p_{\overline{\mathrm{X}}_i}||p_{\mathrm{X}_i})]}.$$

By Lemma 1 parts (b) and (c), we immediately obtain the following lemma:

Lemma 2. *For $p_{\overline{\mathrm{X}}_i} \in \mathcal{P}_n(\mathcal{X}_i)$,*

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

5.2. Upper Bounds on Reliability and Security

In this subsection, we evaluate upper bounds of $p_{\mathrm{e}}(\phi_i^{(n)}, \psi_i^{(n)}|p^n_{\mathrm{X}_i})$, $i = 1, 2$, and $\Delta_n(\varphi_1^{(n)}, \varphi_2^{(n)}, \varphi_{\mathcal{A}}^{(n)}|p^n_{\mathrm{X}_1\mathrm{X}_2}, p_{ZK_1\ K_2Un})$. For $p_{\mathrm{e}}(\phi_i^{(n)}, \psi_i^{(n)}|p^n_{\mathrm{X}_i})$, we derive an upper bound that

can be characterized with a quantity depending on $(\phi_i^{(n)}, \psi_i^{(n)})$ and type $P_{x_i^n}$ of sequences $x_i^n \in \mathcal{X}_i^n$. We first evaluate $p_{\mathrm{e}}(\phi_i^{(n)}, \psi_i^{(n)} | p_{X_i}^n), i = 1, 2$. For $x_i^n \in \mathcal{X}_i^n$ and $p_{\overline{X}} \in \mathcal{P}_n(\mathcal{X}_i)$, we define the following functions:

$$\Xi_{x_i^n}(\phi_i^{(n)}, \psi_i^{(n)}) := \begin{cases} 1 & \text{if} \quad \psi_i^{(n)}\left(\phi_i^{(n)}(x_i^n)\right) \neq x_i^n, \\ 0 & \text{otherwise,} \end{cases}$$

$$\Xi_{\overline{X}_i}(\phi^{(n)}, \psi^{(n)}) := \frac{1}{|T_{\overline{X}_i}^n|} \sum_{x_i^n \in T_{\overline{X}_i}^n} \Xi_{x_i^n}(\phi_i^{(n)}, \psi_i^{(n)}).$$

Then, we have the following lemma.

Lemma 3. *In the proposed system, for $i = 1, 2$ and for any pair of $(\phi_i^{(n)}, \psi_i^{(n)})$, we have*

$$p_{\mathrm{e}}(\phi_i^{(n)}, \psi_i^{(n)} | p_{X_i}^n) \leq \sum_{p_{\overline{X}_i} \in \mathcal{P}_n(\mathcal{X}_i)} \Xi_{\overline{X}}(\phi_i^{(n)}, \psi_i^{(n)}) \mathrm{e}^{-nD(p_{\overline{X}_i} || p_{X_i})}. \tag{15}$$

Proof of this lemma is found in [26]. We omit the proof.

We next discuss upper bounds of

$$\Delta_n(\varphi_1^{(n)}, \varphi_2^{(n)}, \varphi_{\mathcal{A}}^{(n)} | p_{X_1X_2}^n, p_{ZK_1K_2}^n) = I(\widetilde{C}_1^{m_1} \widetilde{C}_2^{m_2}, M_{\mathcal{A}}^{(n)}; X_1^n X_2^n).$$

On an upper bound of $I(\widetilde{C}_1^{m_1} \widetilde{C}_2^{m_2}, M_{\mathcal{A}}^{(n)}; X_1^n X_2^n)$, we have the following lemma:

Lemma 4.

$$I(\widetilde{C}_1^{m_1} \widetilde{C}_2^{m_2}, M_{\mathcal{A}}^{(n)}; X_1^n X_2^n) \leq D\left(p_{K_1^{m_1} K_2^{m_2} | M_{\mathcal{A}}^{(n)}} \middle|\middle| p_{V_1^{m_1} V_2^{m_2}} \middle| p_{M_{\mathcal{A}}^{(n)}}\right), \tag{16}$$

where $p_{V_1^{m_1} V_2^{m_2}}$ represents the uniform distribution over $\mathcal{X}_1^{m_1} \times \mathcal{X}_2^{m_2}$.

We can prove Lemma 4 using a similar method shown in [4]. The detailed proof is given in Appendix C.

5.3. Random Coding Arguments

We construct a pair of affine encoders $(\varphi_1^{(n)}, \varphi_2^{(n)})$ using the random coding method. For the two decoders $\psi_i^{(n)}, i = 1, 2$, we propose the minimum entropy decoder used in Csiszár [8] and Oohama and Han [27].

Random Construction of Affine Encoders: For each $i = 1, 2$, we first choose m_i such that

$$m_i := \left\lfloor \frac{nR_i}{\log |\mathcal{X}_i|} \right\rfloor,$$

where $\lfloor a \rfloor$ stands for the integer part of a. It is obvious that, for $i = 1, 2$,

$$R_i - \frac{1}{n} \leq \frac{m_i}{n} \log |\mathcal{X}_i| \leq R_i.$$

By the Definition (2) of $\phi_i^{(n)}$, we have that, for $x_i^n \in \mathcal{X}_i^n$,

$$\phi_i^{(n)}(x_i^n) = x_i^n A_i,$$

where A_i is a matrix with n rows and m_i columns. By the definition (2) of $\varphi_i^{(n)}$, we have that, for $k_i^n \in \mathcal{X}_i^n$,

$$\varphi_i^{(n)}(k_i^n) = k_i^n A_i + b_i^{m_i},$$

where for each $i = 1, 2$, $b_i^{m_i}$ is a vector with m_i columns. Entries of A_i and $b_i^{m_i}$ are from the field of $\mathcal{X}_i$. Those entries are selected at random, independently from each other and with uniform distribution. Randomly constructed linear encoder $\phi_i^{(n)}$ and affine encoder $\varphi_i^{(n)}$ have three properties shown in the following lemma.

Lemma 5 (Properties of Linear/Affine Encoders). *For each $i = 1, 2$, we have the following:*

(a) For any $x_i^n, v_i^n \in \mathcal{X}_i^n$ with $x_i^n \neq v_i^n$, we have

$$\Pr[\phi_i^{(n)}(x_i^n) = \phi_i^{(n)}(v_i^n)] = \Pr[(x_i^n \ominus v_i^n)A = 0^{m_i}] = |\mathcal{X}|^{-m_i}. \tag{17}$$

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

$$\Pr[\varphi_i^{(n)}(s_i^n) = \widetilde{s}_i^{m_i}] = \Pr[s^n A_i \oplus b_i^{m_i} = \widetilde{s}_i^{m_i}] = |\mathcal{X}_i|^{-m_i}. \tag{18}$$

(c) For any $s_i^n, t_i^n \in \mathcal{X}_i^n$ with $s_i^n \neq t_i^n$, and for any $\widetilde{s}_i^{m_i} \in \mathcal{X}_i^{m_i}$, we have

$$\Pr[\varphi_i^{(n)}(s_i^n) = \varphi_i^{(n)}(t_i^n) = \widetilde{s}_i^{m_i}] = \Pr[s_i^n A_i \oplus b_i^{m_i} = t_i^n A_i \oplus b_i^{m_i} = \widetilde{s}_i^{m_i}] = |\mathcal{X}_i|^{-2m_i}. \tag{19}$$

Proof of this lemma is found in [26]. We omit the proof.

We next define the decoder function $\psi_i^{(n)} : \mathcal{X}_i^{m_i} \to \mathcal{X}_i^n, i = 1, 2$. To this end, we define the following quantities.

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

Minimum Entropy Decoder: For each $i = 1, 2$, and for $\phi_i^{(n)}(x_i^n) = \widetilde{x}_i^{m_i}$, we define the decoder function $\psi_i^{(n)} : \mathcal{X}_i^{m_i} \to \mathcal{X}_i^n$ as follows:

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

Error Probability Bound: In the following arguments, we let expectations based on the random choice of the affine encoders $\varphi_i^{(n)} i = 1, 2$ be denoted by $\mathbf{E}[\cdot]$. For, $i = 1, 2$, define

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

Then, we have the following lemma.

Lemma 6. *For each $i = 1, 2$, for any n and for any $P_{\overline{X}_i} \in \mathcal{P}_n(\mathcal{X}_i)$,*

$$\mathbf{E}\left[\Xi_{\overline{X}_i}(\phi_i^{(n)}, \psi_i^{(n)})\right] \leq \mathrm{e}(n+1)^{|\mathcal{X}_i|} \Pi_{\overline{X}}(R_i).$$

Proof of this lemma is found in [26]. We omit the proof.

Estimation of Approximation Error: Define

$$\begin{aligned}&\Theta(R_1,R_2,\varphi_{\mathcal{A}}^{(n)}|p_{ZK_1K_2}^n)\\ &:=\sum_{\substack{(a,k_1^n,k_2^n)\\ \in\mathcal{M}_{\mathcal{A}}^{(n)}\times\mathcal{X}_1^n\times\mathcal{X}_2^n}} p_{M_{\mathcal{A}}^{(n)}K^n}(a,k_1^n,k_2^n)\times\log\Big[1+(\mathrm{e}^{nR_1}-1)p_{K_1^n|M_{\mathcal{A}}^{(n)}}(k_1^n|a)+(\mathrm{e}^{nR_2}-1)p_{K_2^n|M_{\mathcal{A}}^{(n)}}(k_2^n|a)\\ &\qquad\qquad+(\mathrm{e}^{nR_1}-1)(\mathrm{e}^{nR_2}-1)p_{K_1^nK_2^n|M_{\mathcal{A}}^{(n)}}(k_1^n,k_2^n|a)\Big].\end{aligned}$$

Then, we have the following lemma.

Lemma 7. *For $i=1,2$ and for any n,m_i satisfying $(m_i/n)\log|\mathcal{X}_i|\le R_i$, we have*

$$\mathbf{E}\left[D\left(p_{\tilde{K}^{m_1}\tilde{K}^{m_2}|M_{\mathcal{A}}^{(n)}}\middle|\middle|p_{V_1^{m_1}V_2^{m_2}}\middle|p_{M_{\mathcal{A}}^{(n)}}\right)\right]\le\Theta(R_1,R_2,\varphi_{\mathcal{A}}^{(n)}|p_{ZK_1K_2}^n).\tag{20}$$

Proof of this lemma is given in Appendix D. From the bound (20) in Lemma (7), we know that the quantity $\Theta(R_1,\ R_2,\varphi_{\mathcal{A}}^{(n)}|p_{ZK_1K_2}^n)$ serves as an upper bound of the ensemble average of the conditional divergence $D(p_{\tilde{K}_1^{m_1}\tilde{K}_2^{m_2}|M_{\mathcal{A}}^{(n)}}\ ||p_{V_1^{m_1}V_2^{m_2}}|p_{M_{\mathcal{A}}^{(n)}})$.

From Lemmas 4 and 7, we have the following corollary.

Corollary 2.

$$\mathbf{E}\left[\Delta_n(\varphi_1^{(n)},\varphi_2^{(n)},\varphi_{\mathcal{A}}^{(n)}|p_{X_1X_2}^n,p_{ZK_1K_2}^n)\right]\le\Theta(R_1,R_2,\varphi_{\mathcal{A}}^{(n)}|p_{ZK_1K_2}^n).$$

Existence of Good Code $\{(\varphi_i^{(n)},\psi_i^{(n)})\}_{i=1,2}$:

From Lemma 6 and Corollary 2, we have the following lemma stating an existence of universal code $\{(\varphi_i^{(n)},\psi_i^{(n)})\}_{i=1,2}$.

Lemma 8. *There exists at least one deterministic code $\{(\varphi_i^{(n)},\psi_i^{(n)})\}_{i=1,2}$ satisfying $(m_i/n)\log|\mathcal{X}_i|\le R_i, i=1,2$, such that, for $i=1,2$ and for any $p_{\overline{X}_i}\in\mathcal{P}_n(\mathcal{X}_i)$,*

$$\Xi_{\overline{X}_i}(\phi_i^{(n)},\psi_i^{(n)})\le\mathrm{e}(n+1)^{|\mathcal{X}_i|}\times\{1+(n+1)^{|\mathcal{X}_1|}+(n+1)^{|\mathcal{X}_2|}\}\Pi_{\overline{X}_i}(R_i).$$

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

$$\Delta_n(\varphi_1^{(n)},\varphi_2^{(n)},\varphi_{\mathcal{A}}^{(n)}|p_{X_1X_2}^n,p_{ZK_1K_2}^n)\le\{1+(n+1)^{|\mathcal{X}_1|}+(n+1)^{|\mathcal{X}_2|}\}\Theta(R_1,R_2,\varphi_{\mathcal{A}}^{(n)}|p_{ZK_1K_2}^n).$$

Basically, we can prove Lemma 8 in the same way as to prove a similar lemma shown in [4]. The detailed proof is given in Appendix E.

Proposition 1. *For any $R_{\mathcal{A}},R_1,R_2>0$, and any $p_{ZK_1K_2}$, there exist two sequences of mappings $\{(\varphi_i^{(n)},\psi_i^{(n)})\}_{n=1}^{\infty}, i=1,2$ such that, for $i=1,2$ and for any $p_{X_i}\in\mathcal{P}(\mathcal{X}_i)$, we have*

$$\begin{aligned}&\frac{1}{n}\log|\mathcal{X}_i^{m_i}|=\frac{m_i}{n}\log|\mathcal{X}_i|\le R_i,\\ &p_{\mathrm{e}}(\phi_i^{(n)},\psi_i^{(n)}|p_{X_i}^n)\le\mathrm{e}(n+1)^{2|\mathcal{X}_i|}\times\{1+(n+1)^{|\mathcal{X}_1|}+(n+1)^{|\mathcal{X}_2|}\}\mathrm{e}^{-nE(R_i|p_{X_i})}\end{aligned}\tag{21}$$

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

$$\Delta^{(n)}(\varphi_1^{(n)}, \varphi_2^{(n)}, \varphi_{\mathcal{A}}^{(n)} | p^n_{X_1X_2}, p^n_{ZK_1K_2}) \le \{1 + (n+1)^{|\mathcal{X}_1|} + (n+1)^{|\mathcal{X}_2|}\} \times \Theta(R_1, R_2, \varphi_{\mathcal{A}}^{(n)} | p^n_{ZK_1K_2}). \quad (22)$$

Proof. By Lemma 8, there exists $(\phi_i^{(n)}, \psi_i^{(n)}), i = 1, 2$, satisfying $(m_i/n) \log |\mathcal{X}_i| \le R_i$, such that for $i = 1, 2$ and for any $p_{\overline{X}_i} \in \mathcal{P}_n(\mathcal{X}_i)$,

$$\Xi_{\overline{X}_i}(\phi_i^{(n)}, \psi_i^{(n)}) \le \mathrm{e}(n+1)^{|\mathcal{X}_i|} \times \{1 + (n+1)^{|\mathcal{X}_1|} + (n+1)^{|\mathcal{X}_2|}\} \Pi_{\overline{X}}(R_i). \quad (23)$$

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

$$\Delta_n(\varphi_1^{(n)}, \varphi_2^{(n)}, \varphi_{\mathcal{A}}^{(n)} | p^n_{X_1X_2}, p^n_{ZK_1K_2}) \le \{1 + (n+1)^{|\mathcal{X}_1|} + (n+1)^{|\mathcal{X}_2|}\} \times \Theta(R_1, R_2, \varphi_{\mathcal{A}}^{(n)} | p^n_{ZK_1K_2}). \quad (24)$$

The bound (22) in Proposition 1 has already been proved in (24). Hence, it suffices to prove the bound (21) in Proposition 1 to complete the proof. On an upper bound of $p_{\mathrm{e}}(\phi_i^{(n)}, \psi_i^{(n)} | p^n_{X_i})$, $i = 1, 2$, we have the following chain of inequalities:

$$\begin{aligned} p_{\mathrm{e}}(\phi_i^{(n)}, \psi_i^{(n)} | p^n_{X_i}) &\overset{\text{(a)}}{\le} \mathrm{e}(n+1)^{|\mathcal{X}_i|} \times \{1 + (n+1)^{|\mathcal{X}_1|} + (n+1)^{|\mathcal{X}_2|}\} \times \sum_{p_{\overline{X}_i} \in \mathcal{P}_n(\mathcal{X}_i)} \Pi_{\overline{X}_i}(R_i) \mathrm{e}^{-nD(p_{\overline{X}_i} || p_{X_i})} \\ &\le \mathrm{e}(n+1)^{|\mathcal{X}_i|} \{(n+1)^{|\mathcal{X}_i|} + 1\} |\mathcal{P}_n(\mathcal{X}_i)| \mathrm{e}^{-nE(R_i | p_{X_i})} \\ &\overset{\text{(b)}}{\le} \mathrm{e}(n+1)^{2|\mathcal{X}_i|} \{1 + (n+1)^{|\mathcal{X}_1|} + (n+1)^{|\mathcal{X}_2|}\} \times \mathrm{e}^{-nE(R_i | p_{X_i})}. \end{aligned}$$

Step (a) follows from Lemma 3 and (23). Step (b) follows from Lemma 1 part (a). □

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

In this subsection, we derive an explicit upper bound of $\Theta(R_1, R_2, \varphi_{\mathcal{A}}^{(n)} | p^n_{ZK_1K_2})$, which holds for any eavesdropper $\mathcal{A}$ with $\varphi_{\mathcal{A}}$ satisfying $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$. Define

$$\wp_0 := p_{M_{\mathcal{A}}^{(n)} Z^n K_1^n K_2^n} \left\{ \begin{array}{rl} R_1 \ge \dfrac{1}{n} \log \dfrac{1}{p_{K_1^n | M_{\mathcal{A}}^{(n)}}(K_1^n | M_{\mathcal{A}}^{(n)})} - \eta & \text{or} \\ R_2 \ge \dfrac{1}{n} \log \dfrac{1}{p_{K_2^n | M_{\mathcal{A}}^{(n)}}(K_2^n | M_{\mathcal{A}}^{(n)})} - \eta_2 & \text{or} \\ R_1 + R_2 \ge \dfrac{1}{n} \log \dfrac{1}{p_{K_1^n K_2^n | M_{\mathcal{A}}^{(n)}}(K_1^n, K_2^n | M_{\mathcal{A}}^{(n)})} - \eta_3 & \end{array} \right\}.$$

For $i = 1, 2$, define

$$\wp_i := p_{M_{\mathcal{A}}^{(n)} Z^n K_i^n} \left\{ R_i \ge \frac{1}{n} \log \frac{1}{p_{K_i^n | M_{\mathcal{A}}^{(n)}}(K_i^n | M_{\mathcal{A}}^{(n)})} - \eta_i \right\}.$$

Furthermore, define

$$\wp_3 := p_{M_{\mathcal{A}}^{(n)} Z^n K_1^n K_2^n} \left\{ R_1 + R_2 \ge \frac{1}{n} \log \frac{1}{p_{K_1^n K_2^n | M_{\mathcal{A}}^{(n)}}(K_1^n, K_2^n | M_{\mathcal{A}}^{(n)})} - \eta_3 \right\}.$$

By definition, it is obvious that

$$\wp_0 \leq \sum_{i=1}^{3} \wp_i. \tag{25}$$

We have the following lemma.

Lemma 9. *For any $\eta_i > 0, i = 1,2,3$ 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 the following:*

$$\Theta(R_1, R_2, \varphi_{\mathcal{A}}^{(n)} | p_{ZK_1K_2}^n) \leq n(R_1+R_2)\wp_0 + \sum_{i=1}^{3} \mathrm{e}^{-n\eta_i} \tag{26}$$

$$\leq n(R_1+R_2)\left[\sum_{i=1}^{3}\wp_i\right] + \sum_{i=1}^{3} \mathrm{e}^{-n\eta_i}. \tag{27}$$

Specifically, if $n \geq [R_1+R_2]^{-1}$, we have

$$(n[R_1+R_2])^{-1}\Theta(R_1, R_2, \varphi_{\mathcal{A}}^{(n)} | p_{ZK_1K_2}^n) \leq \sum_{i=1}^{3}(\wp_i + \mathrm{e}^{-n\eta_i}). \tag{28}$$

Proof. By (25), it suffices to show (26) to prove Lemma 9. We set

$$\begin{aligned} A_{R_1,R_2}(K_1^n, K_2^n | M_{\mathcal{A}}^{(n)}) := {} & (\mathrm{e}^{nR_1}-1)p_{K_1^n|M_{\mathcal{A}}^{(n)}}(K_1^n|M_{\mathcal{A}}^{(n)}) + (\mathrm{e}^{nR_2}-1)p_{K_2^n|M_{\mathcal{A}}^{(n)}}(K_2^n|M_{\mathcal{A}}^{(n)}) \\ & + (\mathrm{e}^{nR_1}-1)(\mathrm{e}^{nR_2}-1)p_{K_1^nK_2^n|M_{\mathcal{A}}^{(n)}}(K_1^n, K_2^n|M_{\mathcal{A}}^{(n)}). \end{aligned}$$

Then, we have

$$\Theta(R_1, R_2, \varphi_{\mathcal{A}}^{(n)} | p_{ZK_1K_2}^n) = \mathrm{E}\left[\log\left\{1 + A_{R_1,R_2}(K_1^n, K_2^n | M_{\mathcal{A}}^{(n)})\right\}\right]. \tag{29}$$

We further observe the following:

$$\begin{cases} R_1 < \dfrac{1}{n}\log\dfrac{1}{p_{K_1K_2^n|M_{\mathcal{A}}^{(n)}}(K^n|M_{\mathcal{A}}^{(n)})} - \eta_1 \\ R_2 < \dfrac{1}{n}\log\dfrac{1}{p_{K_1K_2^n|M_{\mathcal{A}}^{(n)}}(K^n|M_{\mathcal{A}}^{(n)})} - \eta_2 \\ R_1+R_2 < \dfrac{1}{n}\log\dfrac{1}{p_{K_1K_2^n|M_{\mathcal{A}}^{(n)}}(K^n|M_{\mathcal{A}}^{(n)})} - \eta_3 \end{cases} \Rightarrow A_{R_1,R_2}(K_1^n, K_2^n|M_{\mathcal{A}}^{(n)}) < \sum_{i=1}^{3}\mathrm{e}^{-n\eta_i}$$

$$\overset{\text{(a)}}{\Rightarrow} \log\left\{1 + A_{R_1,R_2}(K_1^n, K_2^n|M_{\mathcal{A}}^{(n)})\right\} \leq \sum_{i=1}^{3}\mathrm{e}^{-n\eta_i}. \tag{30}$$

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

$$\begin{aligned} \log\Big\{1 + {} & (\mathrm{e}^{nR_1}-1)p_{K_1^n|M_{\mathcal{A}}^{(n)}}(K_1^n|M_{\mathcal{A}}^{(n)}) + (\mathrm{e}^{nR_2}-1)p_{K_2^n|M_{\mathcal{A}}^{(n)}}(K_2^n|M_{\mathcal{A}}^{(n)}) \\ & + (\mathrm{e}^{nR_1}-1)(\mathrm{e}^{nR_2}-1) \times p_{K_1^nK_2^n|M_{\mathcal{A}}^{(n)}}(K_1^n, K_2^n|M_{\mathcal{A}}^{(n)})\Big\} \leq \log[\mathrm{e}^{nR_1}\mathrm{e}^{nR_2}] = n(R_1+R_2). \end{aligned} \tag{31}$$

From (29)–(31), we have the bound (26). □

On upper bound of $\wp_i, i = 1,2,3$, we have the following lemma:

Lemma 10. *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 that for each $i = 1, 2$, we have $\wp_i \leq \tilde{\wp}_i$, where*

$$\tilde{\wp}_i := p_{M_{\mathcal{A}}^{(n)} Z^n K_i^n} \left\{ \begin{array}{rll} 0 & \geq \frac{1}{n} \log \frac{\hat{q}_{i, M_{\mathcal{A}}^{(n)} Z^n K_i^n}(M_{\mathcal{A}}^{(n)}, Z^n, K_i^n)}{p_{M_{\mathcal{A}}^{(n)} Z^n K^n}(M_{\mathcal{A}}^{(n)}, Z^n, K_i^n)} - \eta_i, & \text{(a)} \\ 0 & \geq \frac{1}{n} \log \frac{Q_{i,Z^n}(Z^n)}{p_{Z^n}(Z^n)} - \eta_i, & \text{(b)} \\ R_{\mathcal{A}} & \geq \frac{1}{n} \log \frac{Q_{i,Z^n|M_{\mathcal{A}}^{(n)}}(Z^n|M_{\mathcal{A}}^{(n)})}{p_{Z^n}(Z^n)} - \eta_i, & \text{(c)} \\ R_i & \geq \frac{1}{n} \log \frac{1}{Q_{i,K_i^n|M_{\mathcal{A}}}^{(n)}(K_i^n|M_{\mathcal{A}}^{(n)})} - \eta_i & \end{array} \right\} + 3\mathrm{e}^{-n\eta_i} \tag{32}$$

and that for $i = 3$, we have $\wp_3 \leq \tilde{\wp}_3$, where

$$\tilde{\wp}_3 := p_{M_{\mathcal{A}}^{(n)} Z^n K_1^n K_2^n} \left\{ \begin{array}{rll} 0 \geq \frac{1}{n} \log \frac{\hat{q}_{3, M_{\mathcal{A}}^{(n)} Z^n K_1^n K_2^n}(M_{\mathcal{A}}^{(n)}, Z^n, K_1^n, K_2^n)}{p_{M_{\mathcal{A}}^{(n)} Z^n K_1^n K_2^n}(M_{\mathcal{A}}^{(n)}, Z^n, K_1^n K_2^n)} - \eta_3, & \text{(a)} \\ 0 \geq \frac{1}{n} \log \frac{Q_{3,Z^n}(Z^n)}{p_{Z^n}(Z^n)} - \eta_3, & \text{(b)} \\ R_{\mathcal{A}} \geq \frac{1}{n} \log \frac{\tilde{Q}_{3,Z^n|M_{\mathcal{A}}^{(n)}}(Z^n|M_{\mathcal{A}}^{(n)})}{p_{Z^n}(Z^n)} - \eta_3, & \text{(c)} \\ R_1 + R_2 \geq \frac{1}{n} \log \frac{1}{p_{K_1^n K_2^n|M_{\mathcal{A}}^{(n)}}(K_1^n, K_2^n|M_{\mathcal{A}}^{(n)})} - \eta_3 & \end{array} \right\} + 3\mathrm{e}^{-n\eta_3}. \tag{33}$$

The probability distributions appearing in the three inequalities (a), (b), and (c) in the right members of (32) have a property that we can select them arbitrary. In (a), we can choose any probability distribution $\hat{q}_{i, M_{\mathcal{A}}^{(n)} Z^n K_i^n}$ on $\mathcal{M}_{\mathcal{A}}^{(n)} \times \mathcal{Z}^n \times \mathcal{X}_i^n$. In (b), we can choose any distribution Q_{i,Z^n} on $\mathcal{Z}^n$. In (c), we can choose any stochastic matrix $\tilde{Q}_{i,Z^n|M_{\mathcal{A}}^{(n)}} \colon \mathcal{M}_{\mathcal{A}}^{(n)} \to \mathcal{Z}^n$. The probability distributions appearing in the three inequalities (a), (b), and (c) in the right members of (33) have a property that we can select them arbitrary. In (a), we can choose any probability distribution $\hat{q}_{3, M_{\mathcal{A}}^{(n)} Z^n K_1^n K_2^n}$ on $\mathcal{M}_{\mathcal{A}}^{(n)} \times \mathcal{Z}^n \times \mathcal{X}_1^n \times \mathcal{X}_2^n$. In (b), we can choose any distribution Q_{3,Z^n} on $\mathcal{Z}^n$. In (c), we can choose any stochastic matrix $\tilde{Q}_{3,Z^n|M_{\mathcal{A}}^{(n)}} \colon \mathcal{M}_{\mathcal{A}}^{(n)} \to \mathcal{Z}^n$.

The above lemma is the same as Lemma 10 in the previous work [26]. Since the proof of the lemma is in [26], we omit the proof of Lemma 10 in the present paper. We have the following proposition.

Proposition 2. *For any $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$ and any $n \geq [R_1 + R_2]^{-1}$, we have*

$$(n[R_1 + R_2])^{-1} \Theta(R_1, R_2, \varphi_{\mathcal{A}}^{(n)} | p_{ZK_1K_2}^n) \leq 15\mathrm{e}^{-nF_{\min}(R_{\mathcal{A}}, R_1, R_2 | p_{ZK_1K_2})}. \tag{34}$$

Proof: By Lemmas 9 and 10, we have for any

$$(n[R_1 + R_2])^{-1} \Theta(R_1, R_2, \varphi_{\mathcal{A}}^{(n)} | p_{ZK_1K_2}^n) \leq \sum_{i=1}^{3} (\tilde{\wp}_i + \mathrm{e}^{-n\eta_i}). \tag{35}$$

The quantity $\tilde{\wp}_i + \mathrm{e}^{-n\eta_i}, i = 1, 2, 3.$ is the same as the upper bound on the correct probability of decoding for one helper source coding problem in Lemma 1 in Oohama [11] (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 $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$, there exist $\eta_i^*, i = 1,2,3$ such that for $i = 1,2,3$, we have

$$\tilde{\wp}_i + \mathrm{e}^{-n\eta_i^*} \leq 5\mathrm{e}^{-nF(R_{\mathcal{A}},R_i|p_{ZK_i})}. \tag{36}$$

From (35) and (36), we have that for any $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$ and any $n \geq [R_1+R_2]^{-1}$,

$$(n[R_1+R_2])^{-1}\Theta(R_1,R_2,\varphi_{\mathcal{A}}^{(n)}|p_{ZK_1K_2}^n) \leq 5\sum_{i=1}^{3}\mathrm{e}^{-nF(R_{\mathcal{A}},R_i|p_{ZK_i})} \leq 15\mathrm{e}^{-nF_{\min}(R_{\mathcal{A}},R_1,R_2|p_{ZK_1K_2})},$$

completing the proof. □

6. Alternative Formulation

Here, we show an alternative way to formulate the main problem we consider in this paper. Originally, we consider a problem of having a reliable and secure broadcasting communication in the presence of a side-channel adversary in the case where the sender uses one-time-pad encryption. We can also formulate it in a slightly more general way as follows.

Let consider a problem of having a reliable and secure broadcasting communication in the presence of a side-channel adversary, in the case that the sender uses the encoding scheme $\Phi_i^{(n)}$ at node L_i, where $\Phi_i^{(n)}$ encodes $X_i^{(n)}$ and $K_i^{(n)}$ into $\widetilde{C}_i^{(m_i)}$ for $i = 1,2$. We denote the system resulted from the alternative formulation as AltSys. We illustrate AltSys in Figure 6.

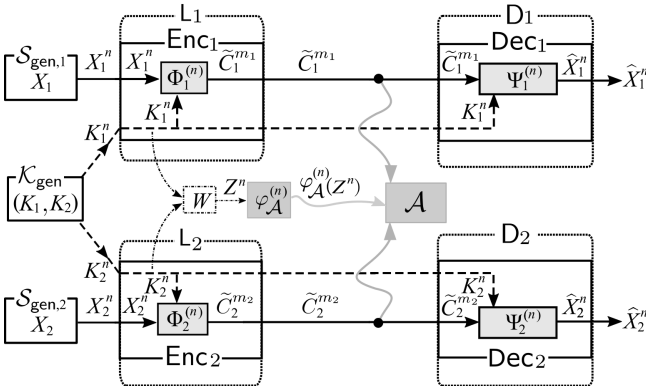

Figure 6. Broadcasting system AltSys from alternative formulation.

6.1. Explanation on Sys *and* AltSys *and Their Comparison*

First, recall the "communication" channel W which is present in both systems, Sys and AltSys. The channel W represents the process of transforming analog raw physical data from the side-channel into raw digital data which later can be processed further by the side-channel adversary $\mathcal{A}$.

In the broadcasting encryption system with post-encryption coding Sys shown in Figure 3, the *main* problem we consider to solve is how to strengthen the secrecy on broadcasting encrypted sources against side-channel adversary $\mathcal{A}$, where the encryption function is one-time-pad encryption. In Sys, since the encryption has been explicitly described as one-time-pad encryption in the beginning, we always treat W as an immediate consequence of the side-channel attacks launched on one-time-pad encryption processes.

In the broadcasting system AltSys from our alternative formulation, shown in Figure 6, the problem we consider here is slightly different to the one in Sys. In AltSys, the problem we consider to solve is whether we can find or construct good encoding schemes that can guarantee the reliability and security against side-channel adversary $\mathcal{A}$. In AltSys, we can have the properties of W fixed first, and then we will find good encoding schemes under the condition of the properties of W.

6.2. Reliability and Security of Alternative Formulation

We can also define the reliability and security of AltSys as follows in the same manner as the ones shown in Section 2.2.

Defining Reliability and Security: From the description of AltSys shown in Figure 6, the decoding process is successful if $\widehat{X}_i^n = X_i^n$ holds. The decoding error probabilities $p_{\mathrm{e},i}, i = 1, 2$, are defined as follows:

$$p_{\mathrm{e},i} = p_{\mathrm{e}}(\Phi_i^{(n)}, \Psi_i^{(n)} | p_{X_i}^n, p_{K_i}^n) := \Pr[\Psi_i^{(n)}(\Phi_i^{(n)}(X_i^n, K_i^n)) \neq X_i^n].$$

Recall that X_i and K_i are assumed to be independent. Let us set $M_{\mathcal{A}}^{(n)} = \varphi_{\mathcal{A}}^{(n)}(Z^n)$. The information leakage $\Delta^{(n)}$ on (X_1^n, X_2^n) from $(\widetilde{C}_1^{m_1}, \widetilde{C}_2^{m_2}, M_{\mathcal{A}}^{(n)})$ is measured by the mutual information between (X_1^n, X_2^n) and $(\widetilde{C}_1^{m_1}, \widetilde{C}_2^{m_2}, M_{\mathcal{A}}^{(n)})$. We can formally define this quantity by

$$\Delta^{(n)} = \Delta^{(n)}(\Phi_1^{(n)}, \Phi_2^{(n)}, \varphi_{\mathcal{A}}^{(n)} | p_{X_1X_2}^n, p_{ZK_1K_2}^n) := I(X_1^n X_2^n; \widetilde{C}_1^{m_2}, \widetilde{C}_2^{m_2}, M_{\mathcal{A}}^{(n)}).$$

Definition 7. *A pair (R_1, R_2) is achievable under $R_{\mathcal{A}} > 0$ for the system* AltSys *if there exists two sequences $\{(\Phi_i^{(n)}, \Psi_i^{(n)})\}_{n \geq 1}, i = 1, 2$, such that $\forall \epsilon > 0$, $\exists n_0 = n_0(\epsilon) \in \mathbb{N}_0$, $\forall n \geq n_0$, we have for $i = 1, 2$,*

$$\frac{1}{n} \log |\mathcal{X}_i^{m_i}| = \frac{m_i}{n} \log |\mathcal{X}_i| \leq R_i, p_{\mathrm{e}}(\Phi_i^{(n)}, \Psi_i^{(n)} | p_{X_i}^n, p_{K_i}^n) \leq \epsilon,$$

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

$$\Delta^{(n)}(\Phi_1^{(n)}, \Phi_2^{(n)}, \varphi_{\mathcal{A}}^{(n)} | p_{X_1X_2}^n, p_{ZK_1K_2}^n) \leq \epsilon.$$

Definition 8 (Reliable and Secure Rate Region). *Let $\mathcal{R}_{\mathsf{AltSys}}(p_{X_1X_2}, p_{ZK_1K_2})$ denote the set of all $(R_{\mathcal{A}}, R)$ such that R is achievable under $R_{\mathcal{A}}$. We call $\mathcal{R}_{\mathsf{AltSys}}(p_{X_1X_2}, p_{ZK_1K_2})$ the* **reliable and secure rate** *region.*

Definition 9. *A five tuple (R_1, R_2, E_1, E_2, F) is achievable under $R_{\mathcal{A}} > 0$ for the system* AltSys *if there exists a sequence $\{(\Phi_i^{(n)}, \Psi_i^{(n)})\}_{n \geq 1}, i = 1, 2$, such that $\forall \epsilon > 0$, $\exists n_0 = n_0(\epsilon) \in \mathbb{N}_0$, $\forall n \geq n_0$, we have for $i = 1, 2$,*

$$\frac{1}{n} \log |\mathcal{X}_i^{m_i}| = \frac{m_i}{n} \log |\mathcal{X}_i| \leq R_i, p_{\mathrm{e}}(\Phi_i^{(n)}, \Psi_i^{(n)} | p_{X_i}^n, p_{K_i}^n) \leq \mathrm{e}^{-n(E_i - \epsilon)},$$

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

$$\Delta^{(n)}(\Phi_1^{(n)}, \Phi_2^{(n)}, \varphi_{\mathcal{A}}^{(n)} | p_{X_1X_2}^n, p_{ZK_1K_2}^n) \leq \mathrm{e}^{-n(F - \epsilon)}.$$

Definition 10 (Rate, Reliability, and Security Region). *Let $\mathcal{D}_{\mathsf{AltSys}}(p_{X_1X_2}, p_{K_1K_2}, W)$ denote the set of all $(R_{\mathcal{A}}, R, E, F)$ such that (R_1, R_2, E_1, E_2, F) is achievable under $R_{\mathcal{A}}$. We call $\mathcal{D}_{\mathsf{AltSys}}(p_{X_1X_2}, p_{K_1K_2}, W)$ the* **rate, reliability, and security** *region.*

Theoretical Results on the Reliable and Security for Broadcasting System from Alternative Formulation: In order to provide solution for the problem from our alternative formulation, it is sufficient to show the existence of encoders and decoders $\{(\Phi_i^{(n)}, \Psi_i^{(n)})\}, i = 1, 2$ which can guarantee reliable and security in the presence of a side-channel adversary. Based on the approach and theoretical results shown in Section 4 on proving the reliability and security of the broadcast system where the sender sends encrypted sources using one-time-pad encryption, it is easy to see that we can achieve the reliability and security for the broadcasting system from alternative formulation of the problem

(Figure 6) such that the decoding error probabilities $p_{e,i}$ ($i = 1, 2$) and the information leakage $\Delta^{(n)}$ decay into zero in exponential rates by specifying $\Phi_i^{(n)}$ and $\Psi_i^{(n)}$, $i = 1, 2$, as follows:

$$\begin{aligned} \Phi_i^{(n)}(X_i^n, K_i^n) &:= \varphi_i^{(n)}(\mathsf{EncOTP}_i^{(n)}(X_i^n, K_i^n)) \quad \text{for } i = 1, 2, \\ \Psi_i^{(n)}(\widetilde{C}_i^{m_i}, K_i^n) &:= \psi_i^{(n)}(\mathsf{DecOTP}_i^{(n)}(\widetilde{C}_i^{m_i}, \varphi_i^{(n)}(K_i^n))) \quad \text{for } i = 1, 2, \end{aligned} \tag{37}$$

where:

- $\mathsf{EncOTP}_i^{(n)} : \mathcal{X}_i^n \times \mathcal{X}_i^n \to \mathcal{X}_i^n$ is the one-time-pad encryption function defined as $\mathsf{EncOTP}_i^{(n)}(a, b) := a \oplus b$ for $(a, b) \in \mathcal{X}_i^n \times \mathcal{X}_i^n$,
- $\varphi_i^{(n)} : \mathcal{X}_i^n \to \mathcal{X}_i^{m_i}$ is an affine encoder constructed based on a linear encoder $\phi_i^{(n)} : \mathcal{X}_i^n \to \mathcal{X}_i^{m_i}$ as shown in Section 5.3,
- $\mathsf{DecOTP}_i^{(n)} : \mathcal{X}_i^{m_i} \times \mathcal{X}_i^{m_i} \to \mathcal{X}_i^{m_i}$ is the one-time-pad decryption function defined as $\mathsf{DecOTP}_i^{(n)}(a, b) := a \ominus b$ for $(a, b) \in \mathcal{X}_i^{m_i} \times \mathcal{X}_i^{m_i}$,
- $\psi_i^{(n)} : \mathcal{X}_i^{m_i} \to \mathcal{X}_i^n$ is a decoder function for linear encoder $\phi_i^{(n)}$ which is associated with the affine encoder $\varphi_i^{(n)}$. (See Section 5.3 for the detailed construction.).

It is easy to see that Theorem 1 actually shows the achievability of reliability and security for broadcasting system in the presence of a side-channel adversary with the specification of $\Phi_i^{(n)}$ and $\Psi_i^{(n)}$, $i = 1, 2$ stated in Equation (37). Hence, the following theorem automatically holds.

Theorem 2. *For any $R_{\mathcal{A}}, R_1, R_2 > 0$ and any $p_{ZK_1K_2}$, there exist two sequences of mappings $\{(\Phi_i^{(n)}, \Psi_i^{(n)})\}_{n=1}^{\infty}, i = 1, 2$ such that for any p_{X_i} and p_{K_i} for $i = 1, 2$, and any $n \geq (R_1 + R_2)^{-1}$, we have*

$$\begin{aligned} \frac{1}{n} \log |\mathcal{X}_i^{m_i}| = \frac{m_i}{n} \log |\mathcal{X}_i| \leq R_i, \\ p_{\mathrm{e}}(\Phi_i^{(n)}, \Psi_i^{(n)} | p_{X_i}^n, p_{K_i}^n) \leq \mathrm{e}^{-n[E(R_i|p_{X_i}) - \delta_{i,n}]}, i = 1, 2 \end{aligned} \tag{38}$$

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

$$\Delta^{(n)}(\Phi_1^{(n)}, \Phi_2^{(n)}, \varphi_{\mathcal{A}}^{(n)} | p_{X_1X_2}^n, p_{K_1K_2}^n, W^n) \leq \mathrm{e}^{-n[F_{\min}(R_{\mathcal{A}}, R_1, R_2 | p_{ZK_1K_2}) - \delta_{3,n}]}, \tag{39}$$

where $\delta_{i,n}, i = 1, 2, 3$ are defined by

$$\begin{aligned} \delta_{i,n} &:= \frac{1}{n} \log \left[\mathrm{e}(n+1)^{2|\mathcal{X}_i|} \times \left\{ 1 + (n+1)^{|\mathcal{X}_1|} + (n+1)^{|\mathcal{X}_2|} \right\} \right], \text{ for } i = 1, 2, \\ \delta_{3,n} &:= \frac{1}{n} \log \left[15n(R_1 + R_2) \times \left\{ 1 + (n+1)^{|\mathcal{X}_1|} + (n+1)^{|\mathcal{X}_2|} \right\} \right]. \end{aligned}$$

Note that, for $i = 1, 2, 3$, $\delta_{i,n} \to 0$ as $n \to \infty$.

It is easy to see that the proof of Theorem 1 that has been explained in Section 5 is also the proof of Theorem 2. Note that the functions $E(R_i|p_{X_i})$ and $F(R_{\mathcal{A}}, R_1, R_2|p_{ZK_1K_2})$ take positive values if $(R_{\mathcal{A}}, R_1, R_2)$ belongs to the set

$$\mathcal{R}_{\mathsf{AltSys}}^{(\mathrm{in})}(p_{X_1X_2}, p_{ZK_1K_2}) := \{R_1 > H(X_1)\} \cap \{R_2 > H(X_2)\} \bigcap_{i=1,2,3} \mathcal{R}_i^{\mathrm{c}}(p_{ZK_i}).$$

Then, define the following:

$$\begin{aligned} \mathcal{D}_{\mathsf{AltSys}}^{(\mathrm{in})}(p_{X_1X_1}, p_{ZK_1K_2}) := \{(R_{\mathcal{A}}, R_1, R_2, E(R_1|p_{X_1}), E(R_2|p_{X_2}), F_{\min}(R_{\mathcal{A}}, R_1, R_2|p_{K_1K_2})) : \\ (R_1, R_2) \in \mathcal{R}_{\mathsf{Sys}}^{(\mathrm{in})}(p_{X_1X_2}, p_{ZK_1K_2})\}. \end{aligned}$$

Hence, we have the following corollary.

Corollary 3.

$$\mathcal{R}^{(\mathrm{in})}_{\mathsf{AltSys}}(p_{X_1X_1}, p_{ZK_1K_2}) \subseteq \mathcal{R}_{\mathsf{AltSys}}(p_{X_1X_1}, p_{ZK_1K_2}),$$
$$\mathcal{D}^{(\mathrm{in})}_{\mathsf{AltSys}}(p_{X_1X_1}, p_{ZK_1K_2}) \subseteq \mathcal{D}_{\mathsf{AltSys}}(p_{X_1X_1}, p_{ZK_1K_2}).$$

7. Comparison to Previous Results

The following Table 1 shows the comparison between our result in this paper and already existing published research results which use the PEC paradigm for amplifying secrecy of the system.

Table 1. Comparison of research on application of PEC for secrecy amplification.

	Network System	**Side-Channel Adversary**	**Correlated Keys**
Previous work 1 [5,6]	Distributed Encryption (2 senders, 2 receivers)	No	Yes
Previous work 2 [4,7]	Two Terminals (1 sender, 1 receiver)	Yes	No
This paper	Broadcast Encryption (1 sender, 2 receivers)	**Yes**	**Yes**

8. Discussion on the Outer-Bounds of Rate Regions and Open Problems

In this paper, we have shown the inner-bound of $\mathcal{R}_{\mathsf{Sys}}$ (resp. $\mathcal{R}_{\mathsf{AltSys}}$). Although we have not touched the issue on the outer-bound of $\mathcal{R}_{\mathsf{Sys}}$ (resp. $\mathcal{R}_{\mathsf{AltSys}}$) in this paper, one may find the hints to derive the outer-bounds in Yamamoto [28]. However, it should be remarked that, in this paper, we are dealing with the side-channel adversary model, which is different from the wiretap model in Yamamoto [28]. In order to apply the method in Yamamoto [28] to find the outer-bound of $\mathcal{R}_{\mathsf{Sys}}$ (resp. $\mathcal{R}_{\mathsf{AltSys}}$), one may need to extend the method in Yamamoto [28] so that it can handle the rate constraint introduced by the side-channel adversary. We left the outer-bounds of $\mathcal{R}_{\mathsf{Sys}}$ and $\mathcal{R}_{\mathsf{AltSys}}$ as open problems.

Furthermore, in contrast to the case of $\mathcal{R}_{\mathsf{Sys}}$ (resp. $\mathcal{R}_{\mathsf{AltSys}}$) where we found hints in Yamamoto [28], we are not able to find any hints in the literature on determining the upper-bound of $\mathcal{D}_{\mathsf{Sys}}$ (resp. $\mathcal{R}_{\mathsf{AltSys}}$). We also left the outer-bounds of $\mathcal{D}_{\mathsf{Sys}}$ (resp. $\mathcal{R}_{\mathsf{AltSys}}$) as open problems.

9. Conclusions

In this paper, we have proposed a new model for analyzing the reliability and the security of broadcasting encrypted sources in the case of one-time-pad encryption, in the presence of an adversary that is not only eavesdropping the public communication channel to obtain ciphertexts but is also obtaining some physical information leaked by multiple devices owned by the sender while performing the encryption. We have also presented a countermeasure against such an adversary by utilizing affine encoders with certain properties. The main distinguishing feature of our countermeasure is that its performance is independent from the characteristics or the types of physical information leaked from the devices exploited by the adversary.

Author Contributions: Both B.S. and Y.O. contributed for the writing of the original draft of this paper. Other contributions of the B.S. 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 Y.O. 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.

Appendix A. Computation of $\mathcal{R}^{(\mathrm{in})}_{\mathrm{Sys,ex1}}(p_{X_1X_2}, p_{ZK_1K_2})$

In this appendix, we compute the region $\mathcal{R}^{(\mathrm{in})}_{\mathrm{Sys,ex1}}(p_{X_1X_2}, p_{ZK_1K_2})$. Since $H(X_i) = h(s_i), i = 1, 2$, we have

$$\mathcal{R}^{(\mathrm{in})}_{\mathrm{Sys}}(p_{X_1X_2}, p_{ZK_1K_2}) = \{R_1 > h(s_1)\} \cap \{R_2 > h(s_2)\} \bigcap_{i=1,2,3} \mathcal{R}^c_i(p_{ZK_i}). \tag{A1}$$

We compute $\mathcal{R}(p_{ZK_1})$, $\mathcal{R}(p_{ZK_2})$, and $\mathcal{R}(p_{ZK_1K_2})$ explicitly. Then, we obtain the form of the region $\mathcal{R}^{(\mathrm{in})}_{\mathrm{Sys,ex1}}(p_{X_1X_2}, p_{ZK_1K_2})$ given by (13). We first compute $\mathcal{R}(p_{ZK_i}), i = 1, 2$. Let $\tilde{N}_{\mathcal{A}}$ be a binary random variable with $p_{\tilde{N}_{\mathcal{A}}}(1) = \rho_{\mathcal{A}}$. We assume that $\tilde{N}_{\mathcal{A}}$ is independent from Z. Let N be a binary random variable with $p_N(1) = \rho$. We assume that N is independent from $(Z, \tilde{N}_{\mathcal{A}})$. Using $\tilde{N}_{\mathcal{A}}$ and N, $K_i, i = 1, 2$ can be written as

$$K_1 = Z \oplus \tilde{N}_{\mathcal{A}},\ K_2 = Z \oplus \tilde{N}_{\mathcal{A}} \oplus N = K_1 \oplus N.$$

Then, by Example 10.2 (p. 265 in [24]), we have

$$\mathcal{R}(p_{ZK_1}) = \{(R_{\mathcal{A}}, R_1) : R_{\mathcal{A}} \geq \log 2 - h(\theta), R_1 \geq h(\rho_{\mathcal{A}} * \theta) \text{ for some } \theta \in [0, 1]\}, \tag{A2}$$

$$\mathcal{R}(p_{ZK_2}) = \{(R_{\mathcal{A}}, R_2) : R_{\mathcal{A}} \geq \log 2 - h(\theta), R_2 \geq h(\rho * \rho_{\mathcal{A}} * \theta) \text{ for some } \theta \in [0, 1]\}. \tag{A3}$$

We next compute $\mathcal{R}(p_{ZK_1K_2})$. Note that

$$\begin{aligned} H(K_1K_2|U) &= H(K_1|U) + H(K_2|K_1U) \overset{(a)}{=} H(K_1|U) + H(K_2|K_1) \\ &= H(K_1|U) + H(N) = H(K_1|U) + h(\rho). \end{aligned} \tag{A4}$$

Step (a) follows from $U \leftrightarrow K_1 \leftrightarrow K_2$. From (A4) and Example 10.2 (p. 265 in [24]), we have

$$\begin{aligned} \mathcal{R}(p_{ZK_1K_2}) = \{(R_{\mathcal{A}}, R_1, R_2) : R_{\mathcal{A}} \geq &\log 2 - h(\theta), \\ R_1 + R_2 \geq &h(\rho) + h(\rho_{\mathcal{A}} * \theta) \text{ for some } \theta \in [0, 1]\}. \end{aligned} \tag{A5}$$

From (A1)–(A3) and (A5), we have the form of the region $\mathcal{R}^{(\mathrm{in})}_{\mathrm{Sys,ex1}}(p_{X_1X_2}, p_{ZK_1K_2})$ given by (13).

Appendix B. Computation of $\mathcal{R}^{(\mathrm{in})}_{\mathrm{Sys,ex2}}(p_{X_1X_2}, p_{ZK_1K_2})$

In this appendix, we compute the region $\mathcal{R}^{(\mathrm{in})}_{\mathrm{Sys,ex2}}(p_{X_1X_2}, p_{ZK_1K_2})$. Since $H(X_i) = h(s_i), i = 1, 2$, we have

$$\mathcal{R}^{(\mathrm{in})}_{\mathrm{Sys}}(p_{X_1X_2}, p_{ZK_1K_2}) = \{R_1 > h(s_1)\} \cap \{R_2 > h(s_2)\} \bigcap_{i=1,2,3} \mathcal{R}^c_i(p_{ZK_i}). \tag{A6}$$

We compute $\mathcal{R}(p_{ZK_1})$, $\mathcal{R}(p_{ZK_2})$, and $\mathcal{R}(p_{ZK_1K_2})$ explicitly. Then, we obtain the form of the region $\mathcal{R}^{(\mathrm{in})}_{\mathrm{Sys,ex1}}(p_{X_1X_2}, p_{ZK_1K_2})$ given by (14). We first compute $\mathcal{R}(p_{ZK_i}), i = 1, 2$. We can easily verify that for each $i = 1, 2$, K_i is independent from Z. Then, for each $i = 1, 2$, we have

$$\mathcal{R}(p_{ZK_i}) = \{(R_{\mathcal{A}}, R_i) : R_{\mathcal{A}} \geq \log 2 - h(\theta), R_i \geq \log 2 \text{ for some } \theta \in [0, 1]\}. \tag{A7}$$

We next compute $\mathcal{R}(p_{ZK_1K_2})$. To this end, we prove the following lemma.

Lemma A1. *For Example 2, we have*

$$H(K_1K_2|U) = H(K_2) + H(K_1 \oplus K_2|U) = \log 2 + H(K_1 \oplus K_2|U).$$

Proof. Note that

$$\begin{aligned} H(K_1K_2|U) &= H(K_1 + K_2|U) + H(K_2|K_1 \oplus K_2, U) \\ &= H(K_1 \oplus K_2|U) + H(K_2) - I(K_2; K_1 \oplus K_2, U). \end{aligned} \tag{A8}$$

On the upper bound of $I(K_2; K_1 \oplus K_2, U)$, we have the following chain of inequalities:

$$\begin{aligned} I(K_2; K_1 \oplus K_2, U) &\le I(K_2; K_1 \oplus K_2, U, Z) = I(K_2; K_1 \oplus K_2, Z) + I(K_2; U|K_1 \oplus K_2, Z) \\ &\le I(K_2; K_1 \oplus K_2, Z) + I(K_1 \oplus K_2, K_2; U|Z) \overset{\text{(a)}}{=} I(K_2; N, N_{\mathcal{A}}) + I(K_1, K_2; U|Z) \overset{\text{(b)}}{=} 0. \end{aligned} \tag{A9}$$

Step (a) follows from $K_2 = K_1 \oplus N$ and $Z = K_1 \oplus K_2 \oplus N_{\mathcal{A}}$. Step (b) follows from $U \leftrightarrow Z \leftrightarrow (K_1, K_2)$. From (A8) and (A9), we have Lemma A1. □

Let $\hat{N}_{\mathcal{A}}$ be a binary random variable with $p_{\hat{N}_{\mathcal{A}}}(1) = \rho_{\mathcal{A}}$. We assume that $\hat{N}_{\mathcal{A}}$ is independent from Z. Using $\hat{N}_{\mathcal{A}}$, $X_1 \oplus X_2$ can be written as

$$X_1 \oplus X_2 = Z \oplus \hat{N}_{\mathcal{A}}. \tag{A10}$$

From Lemma A1, (A10), and Example 10.2 (p. 265 in [24]), we have

$$\begin{aligned} \mathcal{R}(p_{ZK_1K_2}) = \{(R_{\mathcal{A}}, R_1, R_2) : R_{\mathcal{A}} &\ge \log 2 - h(\theta), \\ R_1 + R_2 &\ge \log 2 + h(\rho_{\mathcal{A}} * \theta) \text{ for some } \theta \in [0,1]\}. \end{aligned} \tag{A11}$$

From (A6), (A7), and (A11), we have the form of the region $\mathcal{R}^{(\text{in})}_{\text{Sys,ex2}}(p_{X_1X_2}, p_{ZK_1K_2})$ given by (14).

Appendix C. Proof of Lemma 4

We have the following chain of inequalities:

$$\begin{aligned} I(\widetilde{C}_1^{m_1}\widetilde{C}_2^{m_2}, M_{\mathcal{A}}^{(n)}; X_1^n X_2^n) &\overset{\text{(a)}}{=} I(\widetilde{C}_1^{m_2}\widetilde{C}_2^{m_2}; X_1^n X_2^n | M_{\mathcal{A}}^{(n)}) \\ &\le \log(|\mathcal{X}_1^{m_1}||\mathcal{X}_2^{m_2}|) - H(\widetilde{C}_1^{m_1}\widetilde{C}_2^{m_2}|X_1^n X_2^n, M_{\mathcal{A}}^{(n)}) \\ &\overset{\text{(b)}}{=} \log(|\mathcal{X}_1^{m_1}||\mathcal{X}_2^{m_2}|) - H(\widetilde{K}_1^{m_1}\widetilde{K}_2^{m_2}|X_1^n X_2^n, M_{\mathcal{A}}^{(n)}) \\ &\overset{\text{(c)}}{=} \log(|\mathcal{X}_1^{m_1}||\mathcal{X}_2^{m_2}|) - H(\widetilde{K}_1^{m_1}\widetilde{K}_2^{m_2}|M_{\mathcal{A}}^{(n)}) \\ &= D\left(p_{K_1^{m_1}K_2^{m_2}|M_{\mathcal{A}}^{(n)}} \middle|\middle| p_{V_1^{m_1}V_2^{m_2}} \middle| p_{M_{\mathcal{A}}^{(n)}}\right). \end{aligned}$$

Step (a) follows from $(X_1^n, X_2^n) \perp M_{\mathcal{A}}^{(n)}$. Step (b) follows from that for $i = 1, 2$, $\widetilde{C}_i^{m_i} = \widetilde{K}_i^{m_i} \oplus \widetilde{X}_i^{m_i}$ and $\widetilde{X}_i^{m_i} = \phi_i^{(n)}(X_i^n)$. Step (c) follows from $(\widetilde{K}_1^{m_1}, \widetilde{K}_2^{m_2}, M_{\mathcal{A}}^{(n)}) \perp (X_1^n, X_2^n)$.

Appendix D. Proof of Lemma 7

In this appendix, we prove Lemma 7. This lemma immediately follows from the following lemma:

Lemma A2. *For $i = 1, 2$ and for any n, m_i satisfying $(m_i/n)\log|\mathcal{X}_i| \le R_i$, we have*

$$\begin{aligned}
&\mathbf{E}\left[D\left(p_{\tilde{K}^{m_1}\tilde{K}^{m_2}|M_{\mathcal{A}}^{(n)}}\middle\|p_{V^{m_1}V^{m_2}}\middle|p_{M_{\mathcal{A}}^{(n)}}\right)\right]\\
&\le \sum_{\substack{(a,k_1^n,k_2^n)\\ \in\mathcal{M}_{\mathcal{A}}^{(n)}\times\mathcal{X}_1^n\times\mathcal{X}_2^n}} p_{M_{\mathcal{A}}^{(n)}K^n}(a,k_1^n,k_2^n)\times\log\Big[1+(|\mathcal{X}_1^{m_1}|-1)p_{K_1^n|M_{\mathcal{A}}^{(n)}}(k_1^n|a)+(|\mathcal{X}_2^{m_2}|-1)p_{K_2^n|M_{\mathcal{A}}^{(n)}}(k_2^n|a)\\
&\qquad\qquad +(|\mathcal{X}_1^{m_1}|-1)(|\mathcal{X}_2^{m_2}|-1)p_{K_1^nK_2^n|M_{\mathcal{A}}^{(n)}}(k_1^n,k_2^n|a)\Big]. \qquad \text{(A12)}
\end{aligned}$$

In fact, from $|\mathcal{X}_i^{m_i}|\le \mathrm{e}^{nR_i}$ and (A12) in Lemma A2, we have the bound (20) in Lemma 7. In this appendix we prove Lemma A2. In the following arguments, we use the following simplified notations:

$$\begin{aligned}
k_i^n, K_i^n\in\mathcal{X}_i^n &\Longrightarrow k_i, K_i\in\mathcal{K}_i\\
\tilde{k}_i^{m_i}, \tilde{K}_i^{m_i}\in\mathcal{X}_i^{m_i} &\Longrightarrow l_i, L_i\in\mathcal{L}_i\\
\varphi_i^{(n)}:\mathcal{X}_i^n\to\mathcal{X}_i^{m_i} &\Longrightarrow \varphi_i:\mathcal{K}_i\to\mathcal{L}_i\\
\varphi_i^{(n)}(k_i^n)=k_i^nA_i+b_i^{m_i} &\Longrightarrow \varphi_i(k_i)=k_iA_i+b_i\\
V_i^{m_i}\in\mathcal{X}_i^{m_i} &\Longrightarrow V_i\in\mathcal{L}_i\\
M_{\mathcal{A}}^{(n)}\in\mathcal{M}_{\mathcal{A}}^{(n)} &\Longrightarrow M\in\mathcal{M}.
\end{aligned}$$

We define

$$\chi_{l',l}=\begin{cases}1, \text{ if } l'=l,\\ 0, \text{ if } l'\ne l.\end{cases}$$

Then, the conditional distribution of the random pair (L_1,L_2) for given $M=a\in\mathcal{M}$ is

$$\begin{aligned}
&p_{L_1L_2|M}(l|a)=\sum_{k\in\mathcal{K}}p_{K_1K_2|M}(k_1,k_2|a)\chi_{\varphi_1(k_1),l_1}\chi_{\varphi_2(k_2),l_2}\\
&\text{for } (l_1,l_2)\in\mathcal{L}_1\times\mathcal{L}_2.
\end{aligned}$$

Set

$$\mathrm{Y}_{(\varphi_1(k_1),l_1),(\varphi_2(k_2),l_2)}:=\chi_{\varphi_1(k_1),l_1}\chi_{\varphi_2(k_2),l_2}\times\log\left[|\mathcal{L}_1||\mathcal{L}_2|\left\{\sum_{\substack{(k_1',k_2')\\ \in\mathcal{K}_1\times\mathcal{K}_2}}p_{K_1K_2|M}(k_1',k_2'|a)\chi_{\varphi_1(k_1'),l_1}\chi_{\varphi_2(k_2'),l_2}\right\}\right].$$

Then, the conditional divergence between $p_{L_1L_2|M}$ and $p_{V_1V_2}$ for given M is given by

$$D\left(p_{L_1L_2|M}\middle\|p_{V_1V_2}\middle|p_M\right)=\sum_{\substack{(a,k_1,k_2)\\ \in\mathcal{M}\times\mathcal{K}_1\times\mathcal{K}_2}}\ \sum_{\substack{(l_1,l_2)\\ \in\mathcal{L}_1\times\mathcal{L}_2}}p_{MK_1K_2}(a,k_1,k_2)\mathrm{Y}_{(\varphi_1(k_1),l_1),(\varphi_2(k_2),l_2)}. \qquad \text{(A13)}$$

The quantity $\mathrm{Y}_{(\varphi_1(k_1),l_1),(\varphi_2(k_2),l_2)}$ has the following form:

$$\begin{aligned}
\mathrm{Y}_{(\varphi_1(k_1),l_1),(\varphi_2(k_2),l_2)}=\chi_{\varphi_1(k_1),l_1}\chi_{\varphi_2(k_2),l_2}\times\log\Bigg[&|\mathcal{L}_1||\mathcal{L}_2|\Bigg\{p_{K_1K_2|M}(k_1,k_2|a)\chi_{\varphi_1(k_1),l_1}\chi_{\varphi_2(k_2),l_2}\\
&+\sum_{k_2'\in\{k_2\}^{\mathrm{c}}}p_{K_1K_2|M}(k_1,k_2'|a)\chi_{\varphi_1(k_1),l_1}\chi_{\varphi_2(k_2'),l_2}\\
&+\sum_{k_1'\in\{k_1\}^{\mathrm{c}}}p_{K_1K_2|M}(k_1',k_2|a)\chi_{\varphi_1(k_1'),l_1}\chi_{\varphi_2(k_2),l_2}
\end{aligned}$$

$$+ \sum_{\substack{(k_1',k_2') \\ \in\{k_1\}^c\times\{k_2\}^c}} p_{K_1K_2|M}(k_1',k_2'|a)\chi_{\varphi_1(k_1'),l_1}\chi_{\varphi_2(k_2'),l_2} \Bigg\}\Bigg]. \quad \text{(A14)}$$

The above form is useful for computing $\mathbf{E}[\mathrm{Y}_{(\varphi_1(k_1),l_1)\ ,(\varphi_2(k_2),l_2)}]$.

Proof of Lemma A2. Taking expectation of both side of (A14) with respect to the random choice of the entry of the matrix A_i and the vector b_i representing the affine encoder φ, we have

$$\mathbf{E}\left[D\left(p_{L_1L_2|M}\middle\|\, p_{V_1V_2}\middle|\, p_M\right)\right] = \sum_{\substack{(a,k_1,k_2) \\ \in\mathcal{M}\times\mathcal{K}_1\times\mathcal{K}_2}} \sum_{\substack{(l_1,l_2) \\ \in\mathcal{L}_1\times\mathcal{L}_2}} p_{MK_1K_2}(a,k_1,k_2)\mathbf{E}\left[\mathrm{Y}_{(\varphi_1(k_1),l_1),(\varphi_2(k_2),l_2)}\right]. \quad \text{(A15)}$$

To compute the expectation $\mathbf{E}\left[\mathrm{Y}_{(\varphi_1(k_1),l_1),(\varphi_2(k_2),l_2)}\right]$, we introduce an expectation operator useful for the computation. Let $\mathbf{E}_{\varphi_1(k_1)=l_{k_1},\varphi_2(k_2)=l_{k_2}}[\cdot]$ be an expectation operator based on the conditional probability measures $\Pr\left(\cdot|\varphi_1(k_1)=l_{k_1},\varphi_2(k_2)=l_{k_2}\right)$. Using this expectation operator, the quantity $\mathbf{E}\left[\mathrm{Y}_{(\varphi_1(k_1),l_1),(\varphi_2(k_2),l_2)}\right]$ can be written as

$$\mathbf{E}\left[\mathrm{Y}_{(\varphi_1(k_1),l_1),(\varphi_2(k_2),l_2)}\right] = \sum_{\substack{(l_{k_1},l_{k_2}) \\ \in\mathcal{L}_1\times\mathcal{L}_2}} \Pr\left(\varphi_1(k_1)=l_{k_1},\varphi_2(k_2)=l_{k_2}\right)\times\mathbf{E}_{\varphi_1(k_1)=l_{k_1},\varphi_2(k_2)=l_{k_2}}\left[\mathrm{Y}_{(l_{k_1},l_1),(l_{k_2},l_2)}\right]. \quad \text{(A16)}$$

Note that

$$\mathrm{Y}_{(l_{k_1},l_1),(l_{k_2},l_2)} = \begin{cases} 1, \text{ if } \varphi_1(k_1)=l_1,\varphi_2(k_2)=l_2, \\ 0, \text{ otherwise.} \end{cases} \quad \text{(A17)}$$

From (A16) and (A17), we have

$$\begin{aligned}\mathbf{E}\left[\mathrm{Y}_{(\varphi_1(k_1),l_1),(\varphi_2(k_2),l_2)}\right] &= \Pr\left(\varphi_1(k_1)=l_1,\varphi_2(k_2)=l_2\right)\times\mathbf{E}_{\varphi_1(k_1)=l_1,\varphi_2(k_2)=l_2}\left[\mathrm{Y}_{(l_1,l_1),(l_2,l_2)}\right] \\ &= \frac{1}{|\mathcal{L}_1||\mathcal{L}_2|}\mathbf{E}_{\varphi_1(k_1)=l_1,\varphi_2(k_2)=l_2}\left[\mathrm{Y}_{(l_1,l_1),(l_2,l_2)}\right]. \end{aligned} \quad \text{(A18)}$$

Using (A14), the expectation $\mathbf{E}_{\varphi_1(k_1)=l_1,\varphi_2(k_2)=l_2}\left[\mathrm{Y}_{(l_1,l_1),(l_2,\ l_2)}\right]$ can be written as

$$\begin{aligned}\mathbf{E}_{\varphi_1(k_1)=l_1,\varphi_2(k_2)=l_2}\left[\mathrm{Y}_{(l_1,l_1),(l_2,l_2)}\right] = \mathbf{E}_{\varphi_1(k_1)=l_1,\varphi_2(k_2)=l_2}\Bigg[\log\Bigg\{|\mathcal{L}_1||\mathcal{L}_2|\Bigg(&p_{K_1K_2|M}(k_1,k_2|a) \\ &+ \sum_{k_2'\in\{k_2\}^c} p_{K_1K_2|M}(k_1,k_2'|a)\chi_{\varphi_2(k_2'),l_2} \\ &+ \sum_{k_1'\in\{k_1\}^c} p_{K_1K_2|M}(k_1',k_2|a)\chi_{\varphi_1(k_1'),l_1} \\ &+ \sum_{\substack{(k_1',k_2') \\ \in\{k_1\}^c\times\{k_2\}^c}} p_{K_1K_2|M}(k_1',k_2'|a)\chi_{\varphi_1(k_1'),l_1}\chi_{\varphi_2(k_2'),l_2}\Bigg)\Bigg\}\Bigg]. \end{aligned} \quad \text{(A19)}$$

Applying Jensen's inequality to the right member of (A19), we obtain the following upper bound of $\mathbf{E}_{\varphi_1(k_1)=l_1,\varphi_2(\ k_2)=l_2}\left[\mathrm{Y}_{(l_1,l_1),(l_2,l_2)}\right]$

$$\mathbf{E}_{\varphi_1(k_1)=l_1,\varphi_2(k_2)=l_2}\left[\mathrm{Y}_{(l_1,l_1),(l_2,l_2)}\right]$$

$$\leq \log\left\{|\mathcal{L}_1||\mathcal{L}_2|\left(p_{K_1K_2|M}(k_1,k_2|a)+\sum_{k_2'\in\{k_2\}^{\mathrm{c}}}p_{K_1K_2|M}(k_1,k_2'|a)\mathbf{E}_2+\sum_{k_1'\in\{k_1\}^{\mathrm{c}}}p_{K_1K_2|M}(k_1',k_2|a)\mathbf{E}_1\right.\right.$$
$$\left.\left.+\sum_{\substack{(k_1',k_2')\\ \in\{k_1\}^{\mathrm{c}}\times\{k_2\}^{\mathrm{c}}}}p_{K_1K_2|M}(k_1',k_2'|a)\mathbf{E}_{12}\right)\right\}, \tag{A20}$$

where we set

$$\mathbf{E}_1 := \mathbf{E}_{\varphi_1(k_1)=l_1,\varphi_2(k_2)=l_2}\left[\chi_{\varphi_1(k_1'),l_1}\right],$$
$$\mathbf{E}_2 := \mathbf{E}_{\varphi_1(k_1)=l_1,\varphi_2(k_2)=l_2}\left[\chi_{\varphi_2(k_2'),l_2}\right],$$
$$\mathbf{E}_{12} := \mathbf{E}_{\varphi_1(k_1)=l_1,\varphi_2(k_2)=l_2}\left[\chi_{\varphi_1(k_1'),l_1}\chi_{\varphi_2(k_2'),l_2}\right].$$

Computing $\mathbf{E}_1$, we have

$$\mathbf{E}_1 = \Pr\left(\varphi_1(k_1')=l_1|\varphi_1(k_1)=l_1,\varphi_2(k_2)=l_2\right) \overset{\text{(a)}}{=} \Pr\left(\varphi_1(k_1')=l_1|\varphi_1(k_1)=l_1\right) \overset{\text{(b)}}{=} \frac{1}{|\mathcal{L}_1|}. \tag{A21}$$

Step (a) follows from that the random constructions of φ_1 and φ_2 are independent. Step (b) follows from Lemma 5 parts (b) and (c). In a similar manner we compute $\mathbf{E}_2$ to obtain

$$\mathbf{E}_2 = \frac{1}{|\mathcal{L}_2|}. \tag{A22}$$

We further compute $\mathbf{E}_{12}$ to obtain

$$\begin{aligned}\mathbf{E}_{12} &= \Pr\left(\varphi_1(k_1')=l_1,\varphi_2(k_2')=l_2\ |\varphi_1(k_1)=l_1,\varphi_2(k_2)=l_2\right)\\ &\overset{\text{(a)}}{=} \Pr\left(\varphi_1(k_1')=l_1|\varphi_1(k_1)=l_1\right)\times\Pr\left(\varphi_2(k_2')=l_2|\varphi_2(k_2)=l_2\right) \overset{\text{(b)}}{=} \frac{1}{|\mathcal{L}_1||\mathcal{L}_2|}.\end{aligned} \tag{A23}$$

Step (a) follows from that the random constructuions of φ_1 and φ_2 are independent. Step (b) follows from Lemma 5 parts (b) and (c), From (A20)–(A23), we have

$$\begin{aligned}&\mathbf{E}_{\varphi_1(k_1)=l_1,\varphi_2(k_2)=l_2}\left[\mathrm{Y}_{(l_1,l_1),(l_2,l_2)}\right]\\ &\leq \log\left\{|\mathcal{L}_1||\mathcal{L}_2|\left(p_{K_1K_2|M}(k_1,k_2|a)+\sum_{k_2'\in\{k_2\}^{\mathrm{c}}}p_{K_1K_2|M}(k_1,k_2'|a)\frac{1}{|\mathcal{L}_2|}\right.\right.\\ &\qquad\left.\left.+\sum_{k_1'\in\{k_1\}^{\mathrm{c}}}p_{K_1K_2|M}(k_1',k_2|a)\frac{1}{|\mathcal{L}_1|}+\sum_{\substack{(k_1',k_2')\\ \in\{k_1\}^{\mathrm{c}}\times\{k_2\}^{\mathrm{c}}}}p_{K_1K_2|M}(k_1',k_2'|a)\frac{1}{|\mathcal{L}_1||\mathcal{L}_2|}\right)\right\}\\ &= \log\Big\{1+(|\mathcal{L}_1|-1)p_{K_1|M}(k_1|a)+(|\mathcal{L}_2|-1)p_{K_2|M}(k_2|a)+(|\mathcal{L}_1|-1)(|\mathcal{L}_2|-1)p_{K_1K_2|M}(k_1,k_2|a)\Big\}.\end{aligned} \tag{A24}$$

From (A15), (A18), and (A24), we have the bound (A12) in Lemma A2. □

Appendix E. Proof of Lemma 8

We have the following chain of inequalities:

$$\begin{aligned}
&\mathbf{E}\left[\frac{\Delta_n(\varphi_1^{(n)},\varphi_2^{(n)},\varphi_{\mathcal{A}}^{(n)}|p^n_{X_1X_2},p^n_{ZK_1K_2})}{\Theta(R_1,R_2,\varphi_{\mathcal{A}}^{(n)}|p^n_{ZK_1K_2})}+\sum_{i=1,2}\sum_{p_{\overline{X}_i}\in\mathcal{P}_n(\mathcal{X}_i)}\frac{\Xi_{\overline{X}_i}(\phi_i^{(n)},\psi_i^{(n)})}{\mathrm{e}(n+1)^{|\mathcal{X}_i|}\Pi_{\overline{X}_i}(R_i)}\right]\\
&=\frac{\mathbf{E}\left[\Delta_n(\varphi_1^{(n)},\varphi_2^{(n)},\varphi_{\mathcal{A}}^{(n)}|p^n_{X_1X_2},p^n_{ZK_1K_2})\right]}{\Theta(R_1,R_2,\varphi_{\mathcal{A}}^{(n)}|p^n_{ZK_1K_2})}+\sum_{i=1,2}\sum_{p_{\overline{X}_i}\in\mathcal{P}_n(\mathcal{X}_i)}\frac{\mathbf{E}\left[\Xi_{\overline{X}_i}(\phi_i^{(n)},\psi_i^{(n)})\right]}{\mathrm{e}(n+1)^{|\mathcal{X}_i|}\Pi_{\overline{X}_i}(R_i)}\\
&\overset{(a)}{\leq}1+\sum_{i=1,2}\sum_{p_{\overline{X}_i}\in\mathcal{P}_n(\mathcal{X}_i)}1\overset{(b)}{\leq}1+\sum_{i=1,2}(n+1)^{|\mathcal{X}_i|}.
\end{aligned}$$

Step (a) follows from Lemma 6 and Corollary 2. Step (b) follows from Lemma 1 part (a). Hence, there exists at least one deterministic code $\{(\varphi_i^{(n)},\psi_i^{(n)})\}_{i=1,2}$ such that

$$\frac{\Delta_n(\varphi_1^{(n)},\varphi_2^{(n)},\varphi_{\mathcal{A}}^{(n)}|p^n_{X_1X_2},p^n_{ZK_1K_2})}{\Theta(R_1,R_2,\varphi_{\mathcal{A}}^{(n)}|p^n_{ZK_1K_2})}+\sum_{i=1,2}\sum_{p_{\overline{X}_i}\in\mathcal{P}_n(\mathcal{X}_i)}\frac{\Xi_{\overline{X}_i}(\phi_i^{(n)},\psi_i^{(n)})}{\mathrm{e}(n+1)^{|\mathcal{X}_i|}\Pi_{\overline{X}_i}(R_i)}\leq 1+\sum_{i=1,2}(n+1)^{|\mathcal{X}_i|},$$

from which we have that, for $i=1,2$ and for any $p_{\overline{X}_i}\in\mathcal{P}_n(\mathcal{X}_i)$,

$$\frac{\Xi_{\overline{X}_i}(\phi_i^{(n)},\psi_i^{(n)})}{\mathrm{e}(n+1)^{|\mathcal{X}_i|}\Pi_{\overline{X}_i}(R_i)}\leq 1+\sum_{j=1,2}(n+1)^{|\mathcal{X}_j|}.$$

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

$$\frac{\Delta_n(\varphi_1^{(n)},\varphi_2^{(n)},\varphi_{\mathcal{A}}^{(n)}|p^n_{X_1X_2},p^n_{ZK_1K_2})}{\Theta(R_1,R_2,\varphi_{\mathcal{A}}^{(n)}|p^n_{ZK_1K_2})}\leq 1+\sum_{j=1,2}(n+1)^{|\mathcal{X}_j|},$$

completing the proof.

References

1. Kocher, P.C. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 18–22 August 1996; Volume 1109, pp. 104–113.
2. Kocher, P.C.; Jaffe, J.; Jun, B. Differential Power Analysis. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 15–19 August 1999; Volume 1666, pp. 388–397.
3. Agrawal, D.; Archambeault, B.; Rao, J.R.; Rohatgi, P. The EM Side—Channel(s). *Cryptographic Hardware and Embedded Systems-CHES 2002*; Kaliski, B.S., Koç, Ç.K., Paar, C., Eds.; Springer: Berlin/Heidelberg, Germany, 2003; pp. 29–45.
4. Santoso, B.; Oohama, Y. Information Theoretic Security for Shannon Cipher System under Side-Channel Attacks. *Entropy* **2019**, *21*, 469. [CrossRef]
5. Santoso, B.; Oohama, Y. Secrecy Amplification of Distributed Encrypted Sources with Correlated Keys using Post-Encryption-Compression. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 3042–3056. [CrossRef]
6. Santoso, B.; Oohama, Y. Privacy amplification of distributed encrypted sources with correlated keys. In Proceedings of the 2017 IEEE International Symposium on Information Theory (ISIT), Aachen, Germany, 25–30 June 2017; pp. 958–962.

7. 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.
8. Csiszár, I. Linear Codes for Sources and Source Networks: Error Exponents, Universal Coding. *IEEE Trans. Inform. Theory* **1982**, *28*, 585–592. [CrossRef]
9. Oohama, Y. Intrinsic Randomness Problem in the Framework of Slepian-Wolf Separate Coding System. *IEICE Trans. Fundam.* **2007**, *90*, 1406–1417. [CrossRef]
10. Santoso, B.; Oohama, Y. Post Encryption Compression with Affine Encoders for Secrecy Amplification in Distributed Source Encryption with Correlated Keys. In Proceedings of the 2018 International Symposium on Information Theory and Its Applications (ISITA), Singapore, 28–31 October 2018; pp. 769–773.
11. 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, China, 14–19 June 2015; pp. 1575–1579. Available online: https://arxiv.org/pdf/1504.05891.pdf (accessed on 17 January 2019).
12. Johnson, M.; Ishwar, P.; Prabhakaran, V.; Schonberg, D.; Ramchandran, K. On compressing encrypted data. *IEEE Trans. Signal Process.* **2004**, *52*, 2992–3006. [CrossRef]
13. Maurer, U.; Wolf, S. Unconditionally Secure Key Agreement and The Intrinsic Conditional Information. *IEEE Trans. Inform. Theory* **1999**, *45*, 499–514. [CrossRef]
14. Maurer, U.; Wolf, S. Infromation-Theoretic Key Agreement: From Weak to Strong Secrecy for Free. In Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques, Bruges, Belgium, 14–18 May 2000; Volume 1807, pp. 351–368.
15. Brier, E.; Clavier, C.; Olivier, F. Correlation Power Analysis with a Leakage Model. In *Cryptographic Hardware and Embedded Systems—CHES 2004*; Joye, M., Quisquater, J.J., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; pp. 16–29.
16. Coron, J.; Naccache, D.; Kocher, P.C. Statistics and secret leakage. *ACM Trans. Embed. Comput. Syst.* **2004**, *3*, 492–508. [CrossRef]
17. Köpf, B.; Basin, D.A. An information-theoretic model for adaptive side-channel attacks. In Proceedings of the 14th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, 29 October–2 November 2007; pp. 286–296.
18. Backes, M.; Köpf, B. Formally Bounding the Side-Channel Leakage in Unknown-Message Attacks. In Proceedings of the European Symposium on Research in Computer Security, Málaga, Spain, 6–8 October 2008; Volume 5283, pp. 517–532.
19. Micali, S.; Reyzin, L. Physically Observable Cryptography (Extended Abstract). In Proceedings of the Theory of Cryptography Conference, Cambridge, MA, USA, 19–21 February 2004; Volume 2951, pp. 278–296.
20. Standaert, F.; Malkin, T.; Yung, M. A Unified Framework for the Analysis of Side-Channel Key Recovery Attacks. In Proceedings of the Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, 26–30 April 2009; Volume 5479, pp. 443–461.
21. de Chérisey, E.; Guilley, S.; Rioul, O.; Piantanida, P. An Information-Theoretic Model for Side-Channel Attacks in Embedded Hardware. In Proceedings of the 2019 IEEE International Symposium on Information Theory, Paris, France, 7–12 July 2019.
22. de Chérisey, E.; Guilley, S.; Rioul, O.; Piantanida, P. Best Information is Most Successful Mutual Information and Success Rate in Side-Channel Analysis. *IACR Trans. Cryptogr. Hardw. Embed. Syst.* **2019**, *2019*, 49–79.
23. 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. [CrossRef]
24. El Gamal, A.; Kim, Y.H. *Network Information Theory*; Cambridge University Press: Cambridge, UK, 2011.
25. Csiszár, I.; Körner, J. *Information Theory, Coding Theorems for Discrete Memoryless Systems*, 2nd ed.; Cambridge University Press: Cambridge, UK, 2011.
26. Oohama, Y.; Santoso, B. Information Theoretic Security for Side-Channel Attacks to The Shannon Cipher System. Preprint. 2018. Available online: https://arxiv.org/pdf/1801.02563.pdf (accessed on 18 January 2019).

27. 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. [CrossRef]
28. Yamamoto, H. Coding theorems for Shannon's cipher system with correlated source outputs, and common information. *IEEE Trans. Inf. Theory* **1994**, *40*, 85–95. [CrossRef]