New Distributed Source Encryption Framework

Yasutada Oohama and Bagus Santoso
University of Electro-Communications, Tokyo, Japan
Email: [oohama, santoso.bagus]@uec.ac.jp

Abstract—We pose and investigate the distributed secure source coding based on the common key cryptosystem. This cryptosystem includes the secrecy amplification problem for distributed encrypted sources with correlated keys using post-encryption-compression, which was posed investigated by Santoso and Oohama. In this paper we propose a new security criterion which is more natural compared with the commonly used security criterion which is based on the upper-bound of mutual information between the plaintext and the ciphertext. Under this criterion, we establish the necessary and sufficient condition for the secure transmission of correlated sources.

I. INTRODUCTION

In this paper we pose and investigate the distributed secure source coding based on the common key cryptosystem. This cryptosystem includes the secrecy amplification problem for distributed encrypted sources with correlated keys using post-encryption-compression (PEC), which was posed investigated by Santoso and Oohama [1], [2]. In this paper we propose a new security criterion which is more natural compared with the commonly used security criterion based on the upper-bound of mutual information between the plaintext and the ciphertext. Under this criterion, we establish the necessary and sufficient condition for the secure transmission of correlated sources.

a) We prove that if the mutual information is zero, then the proposed criterion is strictly zero.

b) The proposed criterion depends only on the property of the cryptosystem, implying that this criterion is more natural than the widely-used security metric based mutual information.

For the proposed security criterion, the part a) is quite essential. Without this condition, the criterion is meaningless.

Under the proposed security criterion we prove the strong converse theorem. We further derive a sufficient condition to achieve security. This sufficient condition matches the necessary condition. In our previous works of Santoso and Oohama [1], [2], we have derived a sufficient condition under the security criterion measured by the mutual information. To derive the sufficient condition we use the coding scheme proposed by Santoso and Oohama. We obtain the same sufficient condition as that of Santoso and Oohama [1], [2] under more natural condition than the mutual information.

Our study in this paper has a closely related to several previous works on the PEC, e.g., Johnson et al. [3], Klicl et al. [4]. Our study also has a close connection with several previous works on the Shannon cipher system, e.g. [5], [6], [7].

II. SECURE SOURCE CODING PROBLEM

A. Preliminaries

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

Random Sources of Information and Keys: Let \((X_1, X_2)\) be a pair of random variables from a finite set \(X_1 \times X_2\). Let \((\{X_{1,t}, X_{2,t}\}_{t=1}^{\infty})\) be a stationary discrete memoryless source (DMS) such that for each \(t = 1, 2, \ldots\), the pair \((X_{1,t}, X_{2,t})\) takes values in finite set \(X_1 \times X_2\) and obeys the same distribution as that of \(X_1, X_2\) denoted by \(p_{X_1,X_2} = \{p_{X_{1,t}, X_{2,t}}(x_{1,t}, x_{2,t})\}_{(x_{1,t}, x_{2,t})\in X_1 \times X_2}\). The stationary DMS \((\{X_{1,t}, X_{2,t}\}_{t=1}^{\infty})\) is specified with \(p_{X_1,X_2}\). Also, let \((K_1, K_2)\) be a pair of random variables taken from the same finite set \(X_1 \times X_2\) representing the pair of keys used for encryption at two separate terminals, of which the detailed description will be presented later. Similarly, let \((\{K_{1,t}, K_{2,t}\}_{t=1}^{\infty})\) be a stationary discrete memoryless source such that for each \(t = 1, 2, \ldots\), the pair \((K_{1,t}, K_{2,t})\) takes values in finite set \(X_1 \times X_2\) and obeys the same distribution as that of \(K_1, K_2\) denoted by \(p_{K_1, K_2} = \{p_{K_{1,t}, K_{2,t}}(k_{1,t}, k_{2,t})\}_{(k_{1,t}, k_{2,t})\in X_1 \times X_2}\). The stationary DMS \((\{K_{1,t}, K_{2,t}\}_{t=1}^{\infty})\) is specified with \(p_{K_1, K_2}\).

Random Variables and Sequences: We write the sequence of random variables with length \(n\) from the information source as follows: \(X_1 := X_{1,1} X_{1,2} \cdots X_{1,n}\), \(X_2 := X_{2,1} X_{2,2} \cdots X_{2,n}\). Similarly, the strings with length \(n\) of \(X_1^n\) and \(X_2^n\) are written as \(x_1 := x_{1,1} x_{1,2} \cdots x_{1,n} \in X_1^n\) and \(x_2 := x_{2,1} x_{2,2} \cdots x_{2,n} \in X_2^n\) respectively. For \((x_1, x_2) \in X_1^n \times X_2^n\), \(p_{X_1, X_2}(x_1, x_2)\) stands for the probability of the occurrence of \((x_1, x_2)\). When the information source is memoryless specified with \(p_{X_1, X_2}\), we have the following equation holds: \(p_{X_1, X_2}(x_1, x_2) = \prod_{t=1}^{n} p_{X_1, X_2}(x_{1,t}, x_{2,t})\). In this case we write \(p_{X_1, X_2}(x_1, x_2)\) as \(p_{X_1, X_2}(x_{1,1} x_{1,2})\). 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 \(\odot\) is used to denote the field subtraction operation, i.e., \(a \odot b = a \oplus (\neg b)\) for any elements \(a, b\) of a same finite field. 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 base 2.
B. Basic System Description

First, let the information sources and keys be generated independently by different parties $S_{\text{gen}}$ and $K_{\text{gen}}$ respectively. In our setting, we assume the followings.

- The random keys $K_{1}$ and $K_{2}$ are generated by $K_{\text{gen}}$.
- The key $K_{1}$ is correlated to $K_{2}$.
- The sources $X_{1}$ and $X_{2}$ are generated by $S_{\text{gen}}$ and are correlated to each other.
- The sources are independent to the keys.

Source coding without encryption: The two correlated random sources $X_{1}$ and $X_{2}$ from $S_{\text{gen}}$ be sent to two separated nodes $E_{1}$ and $E_{2}$ respectively. Further settings of the system are described as follows. Those are also shown in Fig. 1

1) Encoding Process: For each $i = 1, 2$, at the node $E_{i}$, the encoder function $\phi_{i}^{(n)} : \mathcal{X}^{m_{1}}_{i} \rightarrow \mathcal{X}^{m_{2}}_{i}$ observes $X_{i}$, and $X_{i}^{\hat{}} = \phi_{i}^{(n)}(X_{i})$. Without loss of generality we may assume that $\phi_{i}^{(n)}$ is surjective.

2) Transmission: Next, the encoded sources $X_{i}^{\hat{}}$, $i = 1, 2$ are sent to the information processing center $D$ through two noiseless channels.

3) Decoding Process: In $D$, the decoder function observes $X_{i}^{\hat{}}$, $i = 1, 2$ to output $(\hat{X}_{1}, \hat{X}_{2})$, using the one-to-one mapping $\psi^{(n)}$ defined by $\psi^{(n)} : \mathcal{X}^{m_{1}}_{1} \times \mathcal{X}^{m_{2}}_{2} \rightarrow \mathcal{X}^{n}_{1} \times \mathcal{X}^{n}_{2}$. Here we set

$$(\hat{X}_{1}, \hat{X}_{2}) := \psi^{(n)}(X_{1}^{\hat{}} \times X_{2}^{\hat{}}) = \psi^{(n)}(\phi_{1}^{(n)}(X_{1}), \phi_{2}^{(n)}(X_{2})) .$$

More concretely, the decoder outputs the unique pair $(\hat{X}_{1}, \hat{X}_{2})$ from $(\phi_{1}^{(n)})^{-1}(X_{1}^{\hat{}}) \times (\phi_{2}^{(n)})^{-1}(X_{2}^{\hat{}})$ in a proper manner.

For the above $(\phi_{1}^{(n)}, \phi_{2}^{(n)}, \psi^{(n)})$, we define the set $D^{(n)}$ of correct decoding by

$$D^{(n)} := \{ (x_{1}, x_{2}) \in \mathcal{X}^{n}_{1} \times \mathcal{X}^{n}_{2} : \psi^{(n)}(\phi_{1}^{(n)}(x_{1}), \phi_{2}^{(n)}(x_{2})) = (x_{1}, x_{2}) \} .$$

On $|D^{(n)}|$, we have the following property.

Property 1: We have the following.

$$|D^{(n)}| = |\mathcal{X}^{m_{1}}_{1}| |\mathcal{X}^{m_{2}}_{2}| . \quad (1)$$

Proof of Property 1 is given in Appendix A.

Remark 1: In brief, the reason that we can assume the decoder as injective mapping without loss of generality is that for any non-injective decoder, we can construct an injective decoder with the same performance. More concretely, for any encoder $\phi^{(n)} : \mathcal{X}^{m_{1}}_{i} \rightarrow \mathcal{X}^{m_{2}}_{i}$, $i = 1, 2$ and any $\psi^{(n)}$ not necessary injective, there exists $(\phi_{1}^{(n)}, \phi_{2}^{(n)}, \psi^{(n)})$ where $\psi^{(n)}$ is injective such that the following holds: $\psi^{(n)}(\hat{\phi}_{1}(X_{i}^{\hat{}}), \hat{\phi}_{2}(X_{j}^{\hat{}})) = \psi^{(n)}(\phi_{1}(X_{i}^{\hat{}}), \phi_{2}(X_{j}^{\hat{}})), \psi^{(n)}(\hat{\phi}_{1}(X_{i}^{\hat{}}), \hat{\phi}_{2}(X_{j}^{\hat{}})) \geq \psi^{(n)}(\phi_{1}(X_{i}^{\hat{}}), \phi_{2}(X_{j}^{\hat{}})), i = 1, 2$.

Distributed source coding with encryption:

The two correlated random sources $X_{1}$ and $X_{2}$ from $S_{\text{gen}}$ are sent to two separated nodes $L_{1}$ and $L_{2}$, respectively. The two random keys $K_{1}$ and $K_{2}$ from $K_{\text{gen}}$ are also sent to $L_{1}$ and $L_{2}$, respectively. Further settings of our system are described as follows. Those are also shown in Fig. 2

1) Source Processing: For each $i = 1, 2$, at the node $i$, $X_{i}$ is encrypted with the key $K_{i}$ using the encryption function $\Phi^{(n)}_{i} : \mathcal{X}^{n}_{i} \times \mathcal{K}^{n}_{i} \rightarrow \mathcal{X}^{m_{i}}_{i}$. For each $i = 1, 2$, the ciphertext $C^{m_{i}}_{i}$ of $X_{i}$ is given by $C^{m}_{i} = \Phi_{i}^{(n)}(K_{i}, X_{i})$. On the encryption function $\Phi^{(n)}_{i}, i = 1, 2$, we use the following notation:

$$\Phi^{(n)}_{i}(K_{i}, X_{i}) = \Phi^{(n)}_{i}(K_{i}, X_{i}) = \Phi^{(n)}_{i}(K_{i}, X_{i}) .$$

2) Transmission: Next, the ciphertext $C^{m}_{i}$, $i = 1, 2$ are sent to the information processing center $D$ through two public communication channels. Meanwhile, the key $K_{i}, i = 1, 2$, are sent to $D$ through two private communication channels.

3) Sink Node Processing: In $D$, we decrypt the ciphertext $(\hat{X}_{1}, \hat{X}_{2})$ from $C^{m}_{i}, i = 1, 2$, using the key $K_{i}, i = 1, 2$, through the corresponding decryption procedure $\Psi^{(n)}$ defined by $\Psi^{(n)} : \mathcal{X}^{n}_{1} \times \mathcal{X}^{n}_{2} \times \mathcal{X}^{m_{1}}_{1} \times \mathcal{X}^{m_{2}}_{2} \rightarrow \mathcal{X}^{n}_{1} \times \mathcal{X}^{n}_{2}$. Here we set

$$(\hat{X}_{1}, \hat{X}_{2}) := \Psi^{(n)}(K_{1}, K_{2}, C^{m}_{1}, C^{m}_{2}) .$$

More concretely, the decoder outputs the unique pair $(\hat{X}_{1}, \hat{X}_{2})$ from $(\Phi_{1}^{(n)}, K_{1})^{-1}(C^{m}_{1}) \times (\Phi_{2}^{(n)}, K_{2})^{-1}(C^{m}_{2})$ in a proper manner. On the decryption function $\Psi^{(n)}$, we use the following notation:

$$\Psi^{(n)}(K_{1}, K_{2}, C^{m}_{1}, C^{m}_{2}) = \Psi^{(n)}(K_{1}, K_{2}, (C^{m}_{1}, C^{m}_{2})) = \Psi^{(n)}(K_{1}, K_{2}, (C^{m}_{1}, C^{m}_{2})) .$$

Fig. 1. Distributed source coding without encryption.

Fig. 2. Distributed source coding with encryption.
Fix any \((K_1, K_2) = (k_1, k_2) \in X_1^n \times X_2^n\). For this \((K_1, K_2)\) and for \((\Phi_1^{(n)}, \Phi_2^{(n)}, \Psi^{(n)})\), we define the set \(D_{k_1, k_2}^{(n)}\) of correct decoders by

\[
D_{k_1, k_2}^{(n)} := \{ (x_1, x_2) \in X_1^n \times X_2^n : \\
\Psi^{(n)}(\Phi_1^{(n)}(k_1, x_1), \Phi_2^{(n)}(k_2, x_2)) = (x_1, x_2) \}.
\]

We require that the cryptosystem \(\Phi_1^{(n)}, \Phi_2^{(n)}, \Psi^{(n)}\) must satisfy the following condition.

**Condition:** For each distributed source encryption system \((\Phi_1^{(n)}, \Phi_2^{(n)}, \Psi^{(n)})\), there exists a distributed source coding system \(\phi_1^{(n)}, \phi_2^{(n)}, \psi^{(n)}\) such that for any \((k_1, k_2) \in X_1^n \times X_2^n\) and for any \((x_1, x_2) \in X_1^n \times X_2^n\),

\[
\Psi^{(n)}(\phi_1^{(n)}(x_1), \phi_2^{(n)}(x_2)) = \psi^{(n)}(\phi_1^{(n)}(x_1), \phi_2^{(n)}(x_2)).
\]

The above condition implies that

\[
D^{(n)} = D_{k_1, k_2}^{(n)} : \forall (k_1, k_2) \in X_1^n \times X_2^n.
\]

We have the following properties on \(D^{(n)}\).

**Property 2:**

a) If \((x_1, x_2), (x_1', x_2') \in D^{(n)}\) and \((x_1, x_2) \neq (x_1', x_2')\), then

\[
(\Phi_1^{(n)}(x_1), \Phi_2^{(n)}(x_2)) \neq (\Phi_1^{(n)}(x_1'), \Phi_2^{(n)}(x_2')).
\]

b) \(\forall (k_1, k_2)\) and \(\forall (c_1^{m_1}, c_2^{m_2})\), \(\exists (x_1, x_2) \in D^{(n)}\) such that

\[
(\Phi_1^{(n)}(x_1), \Phi_2^{(n)}(x_2)) = (c_1^{m_1}, c_2^{m_2}).
\]

The proof of Property 2 is given in Appendix B. On the above distributed source encryption scheme, we have an important lemma. Before describing this lemma, we give an observation on \(p_{c_1^{m_1}, c_2^{m_2}}(X_1, X_2)\). For \((x_1, x_2) \in X_1^n \times X_2^n\), we set

\[
A_{x_1, x_2}(c_1^{m_1}, c_2^{m_2}) := \{(k_1, k_2) : \Phi_1^{(n)}(k_1, x_1) = c_1^{m_1}, i = 1, 2\}.
\]

We have that for each \((c_1^{m_1}, c_2^{m_2})\), \((x_1, x_2) \in X_1^{m_1} \times X_2^{m_2} \times X_1^n \times X_2^n\),

\[
p_{c_1^{m_1}, c_2^{m_2}}(x_1, x_2) = p_{c_1^{m_1}, c_2^{m_2}}(x_1, x_2) :=
\begin{align*}
\text{Pr}\{K_1, K_2 \in A_{x_1, x_2}(c_1^{m_1}, c_2^{m_2}) | X_1 = x_1, X_2 = x_2\} \\
\rightleftharpoons \text{Pr}\{K_1, K_2 \in A_{x_1, x_2}(c_1^{m_1}, c_2^{m_2})\}.
\end{align*}
\]

We can see from (14) that for each \((x_1, x_2) \in X_1^n \times X_2^n\), the component \(p_{c_1^{m_1}, c_2^{m_2}}(X_1, X_2)\) of the stochastic matrix

\[
p_{c_1^{m_1}, c_2^{m_2}}(X_1, X_2, c_1^{m_1}, c_2^{m_2})
\]

can be written as

\[
p_{c_1^{m_1}, c_2^{m_2}}(X_1, X_2, c_1^{m_1}, c_2^{m_2}) = \Gamma_{K_1, K_2, (x_1, x_2)}(c_1^{m_1}, c_2^{m_2}).
\]

Furthermore, the quantity

\[
\Gamma_{K_1, K_2, (x_1, x_2)} := \{ \Gamma_{K_1, K_2, (x_1, x_2)}(c_1^{m_1}, c_2^{m_2}) | (c_1^{m_1}, c_2^{m_2}) \in X_1^{m_1} \times X_2^{m_2}\}
\]

can be regarded as a joint distribution indexed by \((x_1, x_2) \in X_1^n \times X_2^n\). Here the random pair \((K_1, K_2)\) appearing in \(\Gamma_{K_1, K_2, (x_1, x_2)}\) stands for that the randomness of the joint probability distribution is from that of \((K_1, K_2)\). From Property 2, we have the following result, which is a key result of this paper.

**Lemma 1:** \(\forall (c_1^{m_1}, c_2^{m_2}) \in X_1^{m_1} \times X_2^{m_2}\), we have

\[
\sum_{(x_1, x_2) \in D^{(n)}} \Gamma_{K_1, K_2, (x_1, x_2)}(c_1^{m_1}, c_2^{m_2}) = 1.
\]

Proof of Lemma 1 is given in Appendix C. This lemma can be regarded as an extension of the Birkhoff-von Neumann theorem [8].

**III. MAIN RESULTS**

**A. Proposed Security Criterion**

In this section, we introduce our proposed security criterion. In the following arguments all logarithms are taken to the base natural. The adversary \(A\) tries to estimate \((X_1, X_2) \in X_1 \times X_2^n\) from \((C_1^{m_1}, C_2^{m_2})\).

The mutual information (MI) between \((X_1, X_2)\) and \((C_1^{m_1}, C_2^{m_2})\) denoted by

\[
\Delta_{\text{MI}}^{(n)} := I(C_1^{m_1} C_2^{m_2} ; X_1 X_2)
\]

indicates a leakage of information on \((X_1, X_2)\) from \((C_1^{m_1}, C_2^{m_2})\). In this sense it seems to be quite natural to adopt the mutual information \(\Delta_{\text{MI}}^{(n)}\) as a security criterion. On the other hand, directly using \(\Delta_{\text{MI}}^{(n)}\) as a security criterion of the cryptosystem has some problem that this value depends on the statistical property of \((X_1, X_2)\). In this paper we propose a new security criterion, which is based on \(\Delta_{\text{MI}}^{(n)}\) but overcomes the above problem.

**Definition 1:** Let \((\bar{X}_1, \bar{X}_2)\) be an arbitrary random variable taking values in \(X_1 \times X_2^n\). Set \(C_i = \Phi_i^{(n)}(K_i, \bar{X}_i), i = 1, 2\). Define

\[
\text{Supp}(\bar{X}_1, \bar{X}_2) := \{(x_1, x_2) \in X_1^n \times X_2^n : \\
\text{Pr}(x_1, x_2) > 0\},
\]

\[
\mathcal{P}(D^{(n)}) := \{p_{\bar{X}_1, \bar{X}_2} \in \mathcal{P}(X_1^n \times X_2^n) : \\
D^{(n)} = \text{Supp}(\bar{X}_1, \bar{X}_2)\}.
\]

The maximum mutual information criterion denoted by \(\Delta_{\text{max-MI}}^{(n)}\) is as follows.

\[
\Delta_{\text{max-MI}}^{(n)} = \max_{\bar{X}_1, \bar{X}_2 \in \mathcal{P}(D^{(n)})} I(C_1^{m_1} C_2^{m_2} ; \bar{X}_1 \bar{X}_2).
\]

Note that in contrast to \(\Delta_{\text{MI}}\), \(\Delta_{\text{max-MI}}\) does not depend on the distribution of the source. Intuitively, one can see \(\Delta_{\text{max-MI}}\)
as a metric similar to channel capacity. We further define the following quantity:

\[ \Delta_{\text{max-MI}}^{(n)} = \Delta_{\text{max-MI}}^{(n)}(\Phi_1^{(n)}; \Phi_2^{(n)}|PK_1K_2) = \max_{\mathcal{X}_1, \mathcal{X}_2} n \log \frac{\mathcal{P}(\mathcal{X}_1^n \times \mathcal{X}_2^n)}{\mathcal{P}(\mathcal{X}_1^n; \mathcal{X}_2^n|PK_1K_2)} \]

By definition it is obvious that \( \Delta_{\text{max-MI}}^{(n)} \leq \Delta_{\text{max-MI}}^{(n)} \) and \( \Delta_{\text{max-MI}}^{(n)} \leq \Delta_{\text{max-MI}}^{(n)} \). We have the following proposition on \( \Delta_{\text{max-MI}}^{(n)}, \Delta_{\text{max-MI}}^{(n)}, \) and \( \Delta_{\text{max-MI}}^{(n)} \):

**Proposition 1:**

a) We have the following:

\[ \max\{\Delta_{\text{MI}}^{(n)}, \Delta_{\text{max-MI}}^{(n)}\} \leq \Delta_{\text{max-MI}}^{(n)} \]

b) We assume that \( D^{(n)} \subseteq \text{Supp}(p_X^{(n)}, p_{X_2}^{(n)}) = \text{Supp}(p_{X_1}^{(n)}, p_{X_2}^{(n)}) \)

Under this assumption, if \( \Delta_{\text{MI}}^{(n)} = I(C_{1n}^{(n)}; C_{2n}^{(n)}; X_1^n; X_2^n) = 0 \), then we have \( \Delta_{\text{max-MI}}^{(n)} = 0 \). This implies that \( \Delta_{\text{max-MI}}^{(n)} \) is valid as a measure of information leakage.

c) We have the following:

\[ \Delta_{\text{max-MI}}^{(n)} \geq \max\{m_1 \log |X_1| - nH(K_1), m_2 \log |X_2| - nH(K_2), m_1 \log |X_1| + m_2 \log |X_2| - nH(K_1K_2)\} \]

Proof of Proposition 1 is given in Appendix 1.

**Remark 2:** The part b) in the above proposition is quite essential. If we have a security criterion \( \Delta_{\text{MI}}^{(n)} \) not satisfying this condition, it may happen that \( \Delta_{\text{MI}}^{(n)} = I(C_{1n}^{(n)}; C_{2n}^{(n)}; X_1^n; X_2^n) = 0 \), but \( \Delta_{\text{MI}}^{(n)} > 0 \). Such \( \Delta_{\text{MI}}^{(n)} \) is invalid for the security criterion.

**Remark 3:** The property stated in the part c) is a key important property of \( \Delta_{\text{max-MI}}^{(n)} \), which plays an important role in establishing the strong converse theorem. Lemma 1 is a key result for the proof of the part b).

**Defining Reliability and Security:** The decoding process is successful if \( (X_1^n, X_2^n) = (X_1^n, X_2^n) \) holds. Hence the decoding error probability is given by

\[ \Pr[\Psi^{(n)}(K_1, K_2, \phi^{(n)}(K_1, X_1^n), \phi^{(n)}(K_2, X_2^n)) \neq (X_1^n, X_2^n)] \]

\[ = \Pr[\Psi^{(n)}(K_1, K_2, \phi^{(n)}(K_1, X_1^n), \phi^{(n)}(K_2, X_2^n)) \neq (X_1^n, X_2^n)] \]

\[ = \Pr[\Psi^{(n)}(X_1^n, X_2^n) \notin D^{(n)}] \]

Since the above quantity depends only on \( (\phi^{(n)}_1, \phi^{(n)}_2, \psi^{(n)}) \), we write the error probability \( p_e \) of decoding as

\[ p_e = p_e(\phi^{(n)}_1, \phi^{(n)}_2, \psi^{(n)}|p_X^{n}, p_{X_2}^{n}, PK_1K_2) \]

\[ = \Pr[(X_1^n, X_2^n) \notin D^{(n)}] \]

**Definition 2:** We fix some positive constant \( \varepsilon_0 \). For a fixed pair \( (\varepsilon, \delta) \in [0, \varepsilon_0] \times (0, 1) \), \( (R_1, R_2) \) is \( (\varepsilon, \delta) \)-admissible if there exists a sequence \( \{(\Phi_1^{(n)}, \Phi_2^{(n)}, \Psi^{(n)})\}_{n \geq 1} \) such that \( \forall\gamma > 0, \exists n_0 = n_0(\gamma) \in \mathbb{N}, \forall n \geq n_0 \), we have

\[ \frac{1}{n} \log |\mathcal{X}_1^{(n)}| = \frac{m_1}{n} \log |\mathcal{X}_1| \in [R_1 - \gamma, R_1 + \gamma], i = 1, 2, \]

\[ p_e(\phi^{(n)}_1, \phi^{(n)}_2, \psi^{(n)}|p_X^{n}, p_{X_2}^{n}, PK_1K_2) \leq \delta, \]

\[ \Delta_{\text{max-MI}}^{(n)}(\Phi_1^{(n)}, \Phi_2^{(n)}, \Psi^{(n)}|PK_1K_2) \leq \varepsilon. \]

**Definition 3:** (Reliable and Secure Rate Set) Let \( \mathcal{R}(\varepsilon, \delta|p_{X_1}^{(n)}, p_{X_2}^{(n)}, PK_1K_2) \) denote the set of all \( (R_1, R_2) \) such that \( (R_1, R_2) \) is \( (\varepsilon, \delta) \)-admissible. Furthermore, set

\[ \mathcal{R}(p_{X_1}^{(n)}, p_{X_2}^{(n)}, PK_1K_2) = \bigcap_{(\varepsilon, \delta) \in [0, \varepsilon_0] \times (0, 1)} \mathcal{R}(\varepsilon, \delta|p_{X_1}^{(n)}, p_{X_2}^{(n)}, PK_1K_2). \]

We call \( \mathcal{R}(p_{X_1}^{(n)}, p_{X_2}^{(n)}, PK_1K_2) \) the reliable and secure rate set.

**B. Strong Converse for the Distributed Source Encryption**

To state our results on \( \mathcal{R}(\varepsilon, \delta|p_{X_1}^{(n)}, p_{X_2}^{(n)}, PK_1K_2) \) for \( (\varepsilon, \delta) \in [0, \varepsilon_0] \times (0, 1) \), define the following two regions:

\[ \mathcal{R}_{\text{sw}}(p_{X_1}^{(n)}, p_{X_2}^{(n)}) := \{(R_1, R_2) : R_1 \geq H(X_1^n|X_2), R_2 \geq H(X_2^n|X_1), R_1 + R_2 \geq H(X_1^n, X_2^n)\}, \]

\[ \mathcal{R}_{\text{key}}(p_{PK_1K_2}) := \{(R_1, R_2) : R_1 \leq H(K_1), R_2 \leq H(K_2), R_1 + R_2 \leq H(K_1K_2)\}. \]

Santos and Oohama \[1, 2\] proved that the bound \( \mathcal{R}_{\text{key}}(p_{PK_1K_2}) \cap \mathcal{R}_{\text{sw}}(p_{X_1}^{(n)}, p_{X_2}^{(n)}) \) serves as an inner bound of \( \mathcal{R}(p_{X_1}^{(n)}, p_{X_2}^{(n)}, PK_1K_2) \) in the case where the security criterion is measured by the mutual information \( \Delta_{\text{MI}}^{(n)} \). By a simple observation we can see that their post encryption compression scheme yields the same bound in the present case of security criterion measured by \( \Delta_{\text{max-MI}}^{(n)} \). Hence we have the following theorem:

**Theorem 1:** For each \( (\varepsilon, \delta) \in [0, \varepsilon_0] \times (0, 1) \), we have

\[ \mathcal{R}_{\text{key}}(p_{PK_1K_2}) \cap \mathcal{R}_{\text{sw}}(p_{X_1}^{(n)}, p_{X_2}^{(n)}) \subseteq \mathcal{R}(\varepsilon, \delta|p_{X_1}^{(n)}, p_{X_2}^{(n)}, PK_1K_2). \]

Outline of the proof of this theorem will be given in the next section. We next derive one outer bound by a simple observation based on previous works on the distributed source coding for correlated sources. From the communication scheme we can see that the common key cryptosystem can be regarded as the data compression system, where for each \( i = 1, 2 \), the encoder \( \Phi^{(n)}_i \) and the decoder \( \Psi^{(n)} \) can use the common side information \( K_i \). By the strong converse coding theorem for this data compression system \[2\], we have that if

\[ R_1 < H(X_1^n|X_2^n, K_1K_2) = H(X_1^n|X_2^n) \]

\[ R_2 < H(X_2^n|X_1^n, K_1K_2) = H(X_2^n|X_1^n) \]

\[ R_1 + R_2 < H(X_1^n, X_2^n|K_1K_2) = H(X_1^n, X_2^n) \]
then $\forall \tau \in (0, 1)$, $\forall \gamma > 0$, and $\forall \{(\phi^{(n)}_1, \phi^{(n)}_2, \psi^{(n)})\}_{n \geq 1}$, $
exists n_0 = n_0(\tau, \gamma) \in \mathbb{N}$, $\forall n \geq n_0$, we have the following:

$$\frac{m}{n} \log |X_i| \leq R_i + \gamma, i = 1, 2,$$

$$p_{\phi^{(n)}_1, \phi^{(n)}_2, \psi^{(n)}|p^n_{X_1X_2}, p^n_{K_1K_2}} \geq 1 - \tau.$$

Hence we have the following theorem.

**Theorem 2:** For each $(\varepsilon, \delta) \in (0, \varepsilon_0) \times (0, 1)$, we have

$$\mathcal{R}(\varepsilon, \delta|p_{X_1X_2}, p_{K_1K_2}) \subseteq \mathcal{R}_{\text{sw}}(p_{X_1X_2}).$$

In this paper we prove that for some $\varepsilon_0 > 0$, the set $\mathcal{R}_{\text{key}}(p_{K_1K_2})$ serves as an outer bound of $\mathcal{R}(\varepsilon, \delta|p_{X_1X_2}, p_{K_1K_2})$ for $(\varepsilon, \delta) \in (0, \varepsilon_0) \times (0, 1)$. As an immediate consequence of Proposition 1 part c), we have the following proposition.

**Proposition 2:** If $(R_1, R_2) \in \mathcal{R}(\varepsilon, \delta|p_{X_1X_2}, p_{K_1K_2})$, then we have that $\forall \gamma > 0$, $\exists n_0(\gamma)$, $\forall n \geq n_0(\gamma)$, we have

$$R_i \leq H(K_i) + \gamma + \frac{\varepsilon}{n}, i = 1, 2,$$

$$R_1 + R_2 \leq H(K_1K_2) + \gamma + \frac{\varepsilon}{n}.$$

From this proposition we have the following theorem.

**Theorem 3:** For each $(\varepsilon, \delta) \in (0, \varepsilon_0) \times (0, 1)$, we have

$$\mathcal{R}(\varepsilon, \delta|p_{X_1X_2}, p_{K_1K_2}) \subseteq \mathcal{R}_{\text{key}}(p_{K_1K_2}).$$

Combining Theorems 1 and 2 and 3 we establish the following:

**Theorem 4:** For each $(\varepsilon, \delta) \in (0, \varepsilon_0) \times (0, 1)$, we have

$$\mathcal{R}_{\text{key}}(p_{K_1K_2}) \cap \mathcal{R}_{\text{sw}}(p_{X_1X_2}) = \mathcal{R}(\varepsilon, \delta|p_{X_1X_2}, p_{K_1K_2}).$$

IV. OUTLINE OF THE PROOF OF THEOREM 1

In this section we outline the proof of Theorem 1. Our construction of $(\Phi^{(n)}_1, \Phi^{(n)}_2, \Psi^{(n)})$ is the same as that of Santoso and Oohama 11, 12 for the post encryption compression scheme.

Let $\phi^{(n)}_1 := (\phi^{(n)}_1, \phi^{(n)}_2)$ be a pair of linear mappings $\phi^{(n)}_1: X_n \to X_{m_1}^{m_1}$ and $\phi^{(n)}_2: X_n \to X_{m_2}^{m_2}$. For each $i = 1, 2$, we define the mapping $\psi^{(n)}_i: X_n \to X_{m_1}^{m_1}$ by

$$\phi^{(n)}_1(x_i) = x_i A_i$$

where $A_i$ is a matrix with $n$ rows and $m_i$ columns. For each $i = 1, 2$, entries of $A_i$ are from $X_i$. We fix $b^{m_i}_{m_i}$, $i = 1, 2$. For each $i = 1, 2$, define the mapping $\phi^{(n)}_i: X_n \to X_{m_1}^{m_1}$ by

$$\psi^{(n)}_i(k_i) := \phi^{(n)}_i(k_i) \oplus b^{m_i}_{m_i} = k_i A_i \oplus b^{m_i}_{m_i},$$

for $k_i \in X_{n}$. For each $i = 1, 2$, the mapping $\phi^{(n)}_i$ is called the affine mapping induced by the linear mapping $\phi^{(n)}_i$ and constant vector $b^{m_i}_{m_i}$. For each $i = 1, 2$, define $\Phi^{(n)}_i$ by

$$\Phi^{(n)}_i(k_i, x_i) = \psi^{(n)}_i(k_i \oplus x_i).$$

By the definition 4 of $\psi^{(n)}_i$, $i = 1, 2$, we have

$$\Phi^{(n)}_i(k_i, x_i) = \psi^{(n)}_i(x_i \oplus k_i),$$

$$= (x_i \oplus k_i) A_i \oplus b^{m_i}_{m_i} = x_i A_i \oplus (k_i A_i \oplus b^{m_i}_{m_i})$$

$$= \phi^{(n)}_i(x_i) \oplus \psi^{(n)}_i(k_i),$$

for $x_i, k_i \in X_{m_1}^{m_1}$.

Set $\psi^{(n)} := (\psi^{(n)}_1, \psi^{(n)}_2)$. Next, let $\psi^{(n)}$ be the corresponding joint decoder for $\phi^{(n)}$ such that $\psi^{(n)}: X_{m_1} \times X_{m_2} \to X_{m_1} \times X_{m_2}$. Note that $\psi^{(n)}$ 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 of Ciphertexts: First, we use $\psi^{(n)}_1$ and $\psi^{(n)}_2$ to encode the ciphertexts $X_1 \oplus K_1$ and $X_2 \oplus K_2$. Let $C_{m_1} := \psi^{(n)}_1(X_1 \oplus K_1)$ for $i = 1, 2$. By the affine structure 5 of encoders we have that for each $i = 1, 2$,

$$\Phi^{(n)}_i(K_i, X_i) = C^{m_1}_i = \phi^{(n)}_i(X_i \oplus K_i)$$

$$= \phi^{(n)}(X_i) \oplus \psi^{(n)}(K_i) = \tilde{X}_i \oplus \tilde{K}_i,$$

where $\tilde{X}_i := \psi^{(n)}_i(X_i)$, $\tilde{K} := \psi^{(n)}(K)$.

2) Decoding at Joint Sink Node $D$: First, using the pair of linear encoders $(\phi^{(n)}_1, \phi^{(n)}_2)$, $D$ encodes the keys $(K_1, K_2)$ which are received through private channel into $(\tilde{K}_1, \tilde{K}_2) = (\psi^{(n)}_1(K_1), \psi^{(n)}_2(K_2))$. Receiving $(\tilde{K}_1, \tilde{K}_2)$ from public communication channel, $D$ computes $\tilde{X}_1 \oplus \tilde{K}_1$, $i = 1, 2$. In the following way. From 6, we have that for each $i = 1, 2$, the decoder can obtain $\tilde{X}_i = \phi^{(n)}_i(X_i)$ by subtracting $\tilde{K} := \psi^{(n)}(K)$ from $C^{m_1}_i$. Finally, $D$ outputs $(\tilde{X}_1, \tilde{X}_2)$ by applying the joint decoder $\psi^{(n)}$ to $(\tilde{X}_1, \tilde{X}_2)$ as follows:

$$\tilde{X}_1, \tilde{X}_2 = (\psi^{(n)}(\tilde{X}_1 \oplus \tilde{K}_1), \psi^{(n)}(\tilde{X}_2 \oplus \tilde{K}_2)).$$

We summarize the above argument. For $(K_1, K_2)$ and $(C^{m_1}_1, C^{m_2}_2)$, define $\psi^{(n)}$ by

$$\psi^{(n)}(K_1, K_2, C^{m_1}_1, C^{m_2}_2) := \psi^{(n)}_1(C^{m_1}_1 \oplus \tilde{K}_1, C^{m_2}_2 \oplus \tilde{K}_2)$$

$$= \psi^{(n)}(\tilde{X}_1 \oplus \tilde{K}_1, \tilde{X}_2 \oplus \tilde{K}_2).$$

By the above definition and $C^{m_1}_i := \Phi^{(n)}_i(K_i, X_i)$, $i = 1, 2$, we have

$$\psi^{(n)}_1(K_i, X_i) \oplus C^{m_1}_i = \psi^{(n)}_1(\tilde{X}_1 \oplus \tilde{K}_1, \tilde{X}_2 \oplus \tilde{K}_2)$$

$$= \psi^{(n)}_1(\tilde{X}_1, \tilde{X}_2) = \psi^{(n)}(\phi^{(n)}_1(X_i), \phi^{(n)}_2(X_i)).$$

Hence we have the condition which $(\Phi^{(n)}_1, \Phi^{(n)}_2, \psi^{(n)})$ must satisfy.

In this paper, we use the minimum entropy decoder for our joint decoder $\psi^{(n)}$. 

Minimum Entropy Decoder: For all $i = 1, 2$, $\psi^{(n)} : \mathcal{X}_1 \times \mathcal{X}_2 \rightarrow \mathcal{X}_1 \times \mathcal{X}_2^2$ is defined as follows:

$$\psi^{(n)}(\tilde{x}_1, \tilde{x}_2) := \begin{cases} (\hat{x}_1, \hat{x}_2) & \text{if } \phi^{(n)}_1(\tilde{x}_1) = \tilde{x}_1^m, \ i = 1, 2, \\ \phi^{(n)}_2(\tilde{x}_2) & \text{if } \phi^{(n)}_1(\tilde{x}_1) = \tilde{x}_1^m, \ i = 1, 2, \\ \phi^{(n)}_2(\tilde{x}_1) & \text{if } \phi^{(n)}_1(\tilde{x}_1) = \tilde{x}_1^m, \ i = 1, 2, \\ (\tilde{x}_1, \tilde{x}_2) & \text{if } \phi^{(n)}_1(\tilde{x}_1) \neq \tilde{x}_1^m, \ i = 1, 2, \\ \phi^{(n)}_2(\tilde{x}_1) & \text{arbitrary if there is no such } (\tilde{x}_1, \tilde{x}_2) \in \mathcal{X}_1 \times \mathcal{X}_2^2. \end{cases}$$

Our privacy amplified system described above is illustrated in Fig. 3.

Evaluations of the reliability and security: On the error probability $p_e$ of decoding we have

$$p_e = \Pr[\tilde{x}_1, \tilde{x}_2] \neq \tilde{x}_1^m, \ i = 1, 2.$$

We have the following upper bound of $\Delta^{(n)}_{\text{max-MI}}(\psi^{(n)})$,

$$\Delta^{(n)}_{\text{max-MI}}(\psi^{(n)}) \leq \Delta^{(n)}_{\text{max-MI}}(\phi^{(n)}, \psi^{(n)}).$$

Lemma 2: For the proposed construction of $(\Phi^{(n)}, \Phi^{(n)}, \Psi^{(n)})$, we have

$$\Delta^{(n)}_{\text{max-MI}}(\Phi^{(n)}, \Phi^{(n)}, \Psi^{(n)}) \leq \Delta^{(n)}_{\text{max-MI}}(\phi^{(n)}, \psi^{(n)}).$$

On the error probability $p_e$ of decoding we have

$$p_e = \Pr[\tilde{x}_1, \tilde{x}_2] \neq \tilde{x}_1^m, \ i = 1, 2.$$

Proof: By Proposition [1] part a), it suffices to prove the upper bound of $\Delta^{(n)}_{\text{max-MI}}(\Phi^{(n)}, \Phi^{(n)}, \Psi^{(n)})$. The proposed construction of $(\Phi^{(n)}, \Phi^{(n)}, \Psi^{(n)})$, we have

$$\Delta^{(n)}_{\text{max-MI}}(\Phi^{(n)}, \Phi^{(n)}, \Psi^{(n)}) = \Delta^{(n)}_{\text{max-MI}}(\phi^{(n)}, \psi^{(n)}).$$

Theorem 1

According to Santos and Oohama [2], the following inequalities hold:

$$\sum_{i=1}^{n} \log |X_i| + m_2 \log |X_2| \leq H(K_1, K_2).$$

Step (a) follows from (8). Step (b) follows from (9). Since (9) holds for any $(X_1, X_2)$, we have

$$\Delta^{(n)}_{\text{max-MI}}(\Phi^{(n)}, \Phi^{(n)}, \Psi^{(n)}) \leq \frac{m_1 \log |X_1| + m_2 \log |X_2| - H(K_1, K_2)}{n}.$$
APPENDIX

A. Proof of Property $[\text{[1]}]$

Proof of Property $[\text{[1]}]$: We have the following:

$$
\mathcal{D}(n) \triangleq \{(x_1, x_2) : \psi_n(x_1, x_2) = \psi_n(x_1', x_2') \in \phi_{1,1}^{(n)}(X_1^m) \times \phi_{2,2}^{(n)}(X_2^m) \}.
$$

$$(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (d)$$

The above equality contradicts (13). Hence we must have that $\forall (k_1, k_2), \forall (c_1^{m_1}, c_2^{m_2}), \exists (x_1, x_2) \in \mathcal{D}(n)$ such that $\Phi_{k_1, k_2}(x_i) = c_i^{m_i}, i = 1, 2$. ■

B. Proof of Property $[\text{[2]}]$

We first prove the part (a) and then prove the part (b).

Proof of Property $[\text{[2]}]$ part a): Under $(x_1, x_2), (x_1', x_2') \in \mathcal{D}(n)$ and $(x_1, x_2) \neq (x_1', x_2')$, we assume that

$$
(\Phi_{1,k_1}^{(n)}(x_1), \Phi_{2,k_2}^{(n)}(x_2)) = (\Phi_{1,k_1}^{(n)}(x_1'), \Phi_{2,k_2}^{(n)}(x_2')).
$$

Then we have the following:

$$
(x_1, x_2) \Rightarrow (x_1', x_2') \Rightarrow (x_1, x_2) \Rightarrow (x_1', x_2'),
$$

Proof of Property $[\text{[2]}]$ part b): We assume that $\exists (k_1, k_2)$ and $\exists (c_1^{m_1}, c_2^{m_2})$ such that $\forall (x_1, x_2) \in \mathcal{D}(n), (\Phi_{1,k_1}^{(n)}(x_1), \Phi_{2,k_2}^{(n)}(x_2)) \neq (c_1^{m_1}, c_2^{m_2})$. Set

$$
B := \left\{ (\Phi_{1,k_1}^{(n)}(x_1), \Phi_{2,k_2}^{(n)}(x_2)) : (x_1, x_2) \in \mathcal{D}(n) \right\}.
$$

Then by the above assumption we have

$$
B \subseteq \mathcal{X}_1^{m_1} \times \mathcal{X}_2^{m_2} - \{(c_1^{m_1}, c_2^{m_2})\}.
$$

From (14), we have the following chain of equalities:

$$
\sum_{(x_1, x_2) \in \mathcal{D}(n)} p_{C_1^{m_1}C_2^{m_2}}(X_1, X_2 | (c_1^{m_1}, c_2^{m_2}) (x_1, x_2) = (\Phi_{1,k_1}^{(n)}(x_1), \Phi_{2,k_2}^{(n)}(x_2))) = 1.
$$

Step (a) follows from (15). Step (b) follows from (16). ■

D. Proof of Proposition $[\text{[3]}]$

In this appendix we prove Proposition $[\text{[3]}]$

Proof of Proposition $[\text{[3]}]$: The part a) is obvious. We first prove the part b). Using the quntities

$$
\Gamma_{K_1, K_2}(x_1, x_2) \in \mathcal{A}_{x_1, x_2}(c_1^{m_1}, c_2^{m_2}),
$$

components $p_{C_1^{m_1}C_2^{m_2}}(X_1, X_2 | (c_1^{m_1}, c_2^{m_2})$ of the joint distribution $p_{C_1^{m_1}C_2^{m_2}}$ can be computed as

$$
p_{C_1^{m_1}C_2^{m_2}}(c_1^{m_1}, c_2^{m_2}) = \sum_{(x_1, x_2)} p_{X_1, X_2}(x_1, x) \Gamma_{K_1, K_2}(x_1, x_2) (c_1^{m_1}, c_2^{m_2}).
$$

Set

$$
\Gamma_{K_1, K_2}(c_1^{m_1}, c_2^{m_2}) = \sum_{(x_1, x_2)} p_{X_1, X_2}(x_1, x) \Gamma_{K_1, K_2}(x_1, x_2) (c_1^{m_1}, c_2^{m_2}) = p_{C_1^{m_1}C_2^{m_2}}(c_1^{m_1}, c_2^{m_2}).
$$

Furthermore, set

$$
\Gamma_{K_1, K_2}(c_1^{m_1}, c_2^{m_2}) = \sum_{(x_1, x_2)} p_{X_1, X_2}(x_1, x) \Gamma_{K_1, K_2}(x_1, x_2) (c_1^{m_1}, c_2^{m_2}) = p_{C_1^{m_1}C_2^{m_2}}.
$$
Using $\Gamma_{K_1K_2}(x_1,x_2), (x_1,x_2) \in \mathcal{X}_1^n \times \mathcal{X}_2^n$ and $\Gamma(\mathcal{P},x_1,x_2)$, we compute $\Delta_{\text{MI}}^{(n)}$ to obtain

$$
\Delta_{\text{MI}}^{(n)} = I(C_1^{(m_1)} C_2^{(m_2)}; X_1X_2) = \sum_{(x_1,x_2) \in \mathcal{X}_1^n \times \mathcal{X}_2^n} p_{X_1X_2}(x_1,x_2)
$$

$$
\times D\left(\Gamma_{K_1K_2}(x_1,x_2) \mid \mid \Gamma(\mathcal{P},x_1,x_2)\right)
$$

$$
\geq \sum_{(x_1,x_2) \in \mathcal{D}(n)} p_{X_1X_2}(x_1,x_2)
$$

$$
\times D\left(\Gamma_{K_1K_2}(x_1,x_2) \mid \mid \Gamma(\mathcal{P},x_1,x_2)\right).
$$

(17)

By the assumption $\mathcal{D}(n) \subseteq \text{Supp}\{p_{X_1X_2}\}$, we have that

$$
p_{X_1X_2}(x_1,x_2) = \prod_{t=1}^n p_{X_1X_2}(x_{1,t}, x_{2,t}) > 0,$$

$$\forall (x_1,x_2) \in \mathcal{D}(n),$$

(18)

Now we suppose that $\Delta_{\text{MI}}^{(n)} = 0$. Then from (17) and (18), we have

$$
\Gamma_{K_1K_2}(x_1,x_2) = \Gamma_{K_1K_2}(x_1,x_2),
$$

$$\forall (x_1,x_2) \in \mathcal{D}(n),$$

(19)

where $(x_1^*, x_2^*)$ is an element of $\mathcal{D}(n)$. Let $(\mathcal{X}_{1,\text{opt}}, \mathcal{X}_{2,\text{opt}})$ be the optimal random variable, the distribution $p_{\mathcal{X}_{1,\text{opt}}^{(n)}, \mathcal{X}_{2,\text{opt}}^{(n)}}$ of which attains the maximum in the definition of $\Delta_{\text{max}}^{(n)}$. We set $\mathcal{C}_{1,\text{opt}} = \Phi_i^{(n)}(K_i, \mathcal{X}_{i,\text{opt}})$, $i = 1, 2$. By definition we have

$$
\Delta_{\text{max}^{(n)}-\text{MI}} = I(\mathcal{C}_{1,\text{opt}}; C_{2,\text{opt}}; \mathcal{X}_{1,\text{opt}}; \mathcal{X}_{2,\text{opt}}).
$$

Using (19), we compute $\Gamma_{\mathcal{K}_1\mathcal{K}_2}(\mathcal{X}_{1,\text{opt}}, \mathcal{X}_{2,\text{opt}})$ to obtain

$$
\Gamma_{\mathcal{K}_1\mathcal{K}_2}(\mathcal{X}_{1,\text{opt}}, \mathcal{X}_{2,\text{opt}})(c_1^{(m_1)}, c_2^{(m_2)}) = \sum_{(x_1,x_2) \in \mathcal{D}(n)} p_{\mathcal{X}_{1,\text{opt}}; \mathcal{X}_{2,\text{opt}}}(x_1,x_2)
$$

$$
\times \Gamma_{\mathcal{K}_1\mathcal{K}_2}(x_1,x_2)(c_1^{(m_1)} c_2^{(m_2)}) = \Gamma_{\mathcal{K}_1\mathcal{K}_2}(x_1,x_2)(c_1^{(m_1)} c_2^{(m_2)}).
$$

Hence we have

$$
\Gamma_{\mathcal{K}_1\mathcal{K}_2}(\mathcal{X}_{1,\text{opt}}, \mathcal{X}_{2,\text{opt}})(c_1^{(m_1)}, c_2^{(m_2)}) = \Gamma_{\mathcal{K}_1\mathcal{K}_2}(x_1,x_2)(c_1^{(m_1)} c_2^{(m_2)}), \forall (x_1,x_2) \in \mathcal{D}(n).
$$

(20)

From (20), we have

$$
\Delta_{\text{max}^{(n)}-\text{MI}} = I(\mathcal{C}_{1,\text{opt}}; C_{2,\text{opt}}; \mathcal{X}_{1,\text{opt}}; \mathcal{X}_{2,\text{opt}}) = \sum_{(x_1,x_2) \in \mathcal{D}(n)} p_{\mathcal{X}_{1,\text{opt}}; \mathcal{X}_{2,\text{opt}}}(x_1,x_2)
$$

$$
\times D\left(\Gamma_{\mathcal{K}_1\mathcal{K}_2}(x_1,x_2) \mid \mid \Gamma_{\mathcal{P}; \mathcal{X}_{1,\text{opt}}; \mathcal{X}_{2,\text{opt}}}\right) = 0.
$$

We next prove the part c). Let $(\mathcal{X}_1, \mathcal{X}_2)$ be a pair of uniformly distributed random vectors over $\mathcal{D}(n)$. Set $\mathcal{C}_i^{(n)} = \Phi_i(K_i, \mathcal{X}_i)$, $i = 1, 2$. We claim that $(C_1^{(n)}, C_2^{(n)})$ is the uniformly distributed random pair over $\mathcal{X}_1^{(n)} \times \mathcal{X}_2^{(n)}$. In fact for each $(c_1^{(m_1)}, c_2^{(m_2)}) \in \mathcal{X}_1^{(n)} \times \mathcal{X}_2^{(n)}$, we have the following chain of equalities:

$$
|X_1^{(m_1)}| |X_2^{(m_2)}| p_{C_1^{(m_1)} C_2^{(m_2)}}(c_1^{(m_1)} c_2^{(m_2)}) = |D(n)| \sum_{(x_1,x_2) \in \mathcal{D}(n)} 1
$$

$$
\times p_{C_1^{(m_1)} C_2^{(m_2)}}(x_1^{(m_1)} x_2^{(m_2)}; x_1, x_2) = \sum_{(x_1,x_2) \in \mathcal{D}(n)} \Gamma_{K_1K_2}(x_1, x_2)(c_1^{(m_1)} c_2^{(m_2)}) = 1.
$$

(21)

Step (a) follows from Property [1]. Step (b) follows from Lemma [1]. Since we have (21) for every $(c_1^{(m_1)}, c_2^{(m_2)}) \in \mathcal{X}_1^{(n)} \times \mathcal{X}_2^{(n)}$, we have that $(\mathcal{C}_1^{(n)}, \mathcal{C}_2^{(n)})$ is the uniformly distributed random pair over $\mathcal{X}_1^{(n)} \times \mathcal{X}_2^{(n)}$. We have the following chain of inequalities:

$$
\Delta_{\text{max}^{(n)}-\text{MI}} \geq I(\mathcal{C}_1^{(m_1)} \mathcal{C}_2^{(m_2)}; \mathcal{X}_1 \mathcal{X}_2) = H(\mathcal{C}_1^{(m_1)} \mathcal{C}_2^{(m_2)}) - H(\mathcal{C}_1^{(m_1)} \mathcal{C}_2^{(m_2)}; \mathcal{X}_1 \mathcal{X}_2)
$$

$$
= m_1 \log |X_1| + m_2 \log |X_2| - H(\mathcal{C}_1^{(m_1)} \mathcal{C}_2^{(m_2)}; \mathcal{X}_1 \mathcal{X}_2),
$$

$$
= m_1 \log |X_1| + m_2 \log |X_2| - H(\Phi_i^{(n)}(K_i, \mathcal{X}_i)|X_i, \mathcal{X}_i)
$$

$$
\geq m_1 \log |X_1| + m_2 \log |X_2| - h(K_i h(K_i).
$$

Step (a) follows from that $(\mathcal{C}_1^{(m_1)}, \mathcal{C}_2^{(m_2)})$ is the uniformly distributed random pair over $\mathcal{X}_1^{(n)} \times \mathcal{X}_2^{(n)}$. Step (b) follows from the data processing inequality. Furthermore for $i = 1, 2$, we have the following chain of inequalities:

$$
\Delta_{\text{max}^{(n)}-\text{MI}} \geq I(\mathcal{C}_i^{(m)} \mathcal{C}_2^{(m)}; \mathcal{X}_i \mathcal{X}_2) \geq I(\mathcal{C}_i^{(m)}; \mathcal{X}_i)
$$

$$
= H(\mathcal{C}_i^{(m)}; \mathcal{X}_i) = m_1 \log |X_i| - h(\Phi_i^{(n)}(K_i, \mathcal{X}_i)|X_i)
$$

$$
\geq m_1 \log |X_i| - h(K_i |X_i).$$

Step (a) follows from that for $i = 1, 2$, $\mathcal{C}_i^{(m)}$ is the uniformly distributed random variable over $\mathcal{X}_i$. Step (b) follows from the data processing inequality.
[7] M. Iwamoto, K. Ohta, and J. Shikata, “Security formalizations and their relationships for encryption and key agreement in information-theoretic cryptography,” *IEEE Trans. Inf. Theory*, vol. 64, no. 1, pp. 654–685, 2018. [Online]. Available: [https://doi.org/10.1109/TIT.2017.2744650](https://doi.org/10.1109/TIT.2017.2744650)

[8] M. Iwamoto, “Security notions for information theoretically secure encryptions,” in *Proc. IEEE Int. Symp. Inf. Theory 2011*, Saint-Petersburg, Russia, 2011, pp. 1777–1781.

[9] Y. Oohama and T. S. Han, “Universal coding for the Slepian-Wolf data compression system and the strong converse theorem,” *IEEE Trans. Inform. Theory*, vol. 40, no. 6, pp. 1908–1919, November 1994.