

## On Information Leakage During Secure Verification of Compatibility Between Signals

Wei Sun, Shantanu Rane

TR2009-026 June 2009

### Abstract

We consider a secure verification problem in which Alice wants to verify whether her signal  $X_{1:n}$  is compatible with Bob's signal  $Y_{1:n}$ , where  $X_{1:n}$  and  $Y_{1:n}$  are drawn i.i.d. according to a joint distribution  $p(x,y)$ . The notion of compatibility is defined as the requirement that  $p(x,y)$  belongs to a certain set  $A$  of allowable joint distributions. For privacy, Alice jointly encrypts and encodes  $X_{1:n}$  and transmits the result over a public channel to Bob. Using the information leaked by the encryption algorithm, Bob verifies the compatibility of  $X_{1:n}$  with  $Y_{1:n}$ . We characterize the minimum information that Alice's encryption and coding algorithm must leak in order to guarantee reliable verification results. Further, we determine the maximum information that Bob can hope to extract about  $X_{1:n}$  if he is curious. It is shown that a source/channel separation theorem holds for this scenario.

*Canadian Workshop on Information Theory, Canada*

This work may not be copied or reproduced in whole or in part for any commercial purpose. Permission to copy in whole or in part without payment of fee is granted for nonprofit educational and research purposes provided that all such whole or partial copies include the following: a notice that such copying is by permission of Mitsubishi Electric Research Laboratories, Inc.; an acknowledgment of the authors and individual contributions to the work; and all applicable portions of the copyright notice. Copying, reproduction, or republishing for any other purpose shall require a license with payment of fee to Mitsubishi Electric Research Laboratories, Inc. All rights reserved.



# On Information Leakage during Secure Verification of Compatibility between Signals

Wei Sun and Shantanu Rane

Mitsubishi Electric Research Laboratories, Cambridge, MA 02139

{weisun,rane}@merl.com

**Abstract**—We consider a secure verification problem in which Alice wants to verify whether her signal  $X^n$  is compatible with Bob’s signal  $Y^n$ , where  $X^n$  and  $Y^n$  are drawn i.i.d. according to a joint distribution  $p(x, y)$ . The notion of compatibility is defined as the requirement that  $p(x, y)$  belongs to a certain set  $\mathcal{A}$  of allowable joint distributions. For privacy, Alice jointly encrypts and encodes  $X^n$  and transmits the result over a public channel to Bob. Using the information leaked by the encryption algorithm, Bob verifies the compatibility of  $X^n$  with  $Y^n$ . We characterize the minimum information that Alice’s encryption and coding algorithm must leak in order to guarantee reliable verification results. Further, we determine the maximum information that Bob can hope to extract about  $X^n$  if he is curious. It is shown that a source/channel separation theorem holds for this scenario.

**KEYWORDS** – Slepian-Wolf coding, Types, Secure Classification, Encryption

## I. INTRODUCTION

It is often necessary to compare two signals to determine whether they are compatible. The notion of what constitutes compatibility may differ according to the application; for instance, one may be interested in whether the signals are within a specified distortion, or whether they arose from a specified joint probability distribution, or whether they contain the same number of zeros, and so on. Given the two signals, and the compatibility criterion, a computer can perform a suitable measurement and confirm or reject the compatibility hypothesis. However, when one or both of the signals are encrypted, this task is much more difficult because encryption obfuscates the structural properties that are needed to verify compatibility.

Consider, for instance, an authentication scenario in which Bob maintains a database of legitimate fingerprints in an access control system. A user, Alice, would like to participate in a login procedure, but in the interest of privacy, she would not like to reveal her fingerprint to Bob. Therefore, Alice encrypts her fingerprint and sends it to Bob via a public transmission channel. However, if Alice’s encryption completely destroys all the information that is required to implement authentication, then Bob will be unable to verify whether she is a genuine user or not. In other words, Alice must leak some information about her fingerprint to Bob to ensure that authentication is possible in the first place. On the other hand, Bob may be very curious and may want to recover as much information as he can about Alice’s fingerprint from her encrypted transmission. For this situation, it is useful to ask: What is the minimum information leakage rate that Alice

must allow to enable Bob to confirm or reject her request for authentication? Further, what is the maximum information that Bob can hope to extract about Alice’s signal?

In this paper we answer these questions from the point of view of information theory. Specifically, we consider verification of compatibility between two vectors  $X^n$  and  $Y^n$  owned by Alice and Bob respectively. Alice jointly encrypts and encodes her data using a secret key before sending it to the verifier over a public channel. The public channel is modeled as a memoryless noisy channel. Bob does not have access to Alice’s key. He must then determine whether  $X^n$  and  $Y^n$  are compatible in the sense that they are generated i.i.d. according to some joint probability distribution  $p(x, y)$  in a prescribed compatible probability set  $\mathcal{A}$ . Alice may choose to leak some information about her data to Bob in return for his services. We characterize the minimum information leakage rate achievable by Alice and the maximum information leakage rates achievable by Bob.

The groundwork for information-theoretic studies of secrecy and privacy was laid by Shannon in [9]. However, the study of cipher systems from an information theoretic viewpoint was undertaken relatively recently [11], [6]. The tradeoff between lossy compression and secrecy for Shannon cipher systems is studied in [12]. Recently, joint compression-encryption systems have been investigated within the framework of distributed source coding [7], [5]. In this setting, the encryption key is used by the decoder as side information during signal recovery. Closer in spirit to this work, [1] considers the problem of the signal identification from compressed data, and derives achievable compression rates for the case in which a third-party verifier, Charlie identifies whether Alice’s and Bob’s compressed signals satisfy a single-letter distortion criterion without decompressing them. In this work, we consider a more general compatibility criterion and further allow Alice to leak a small portion of her signal to Bob as payment for verification. Our work is also related to [4], where secure collaboration between two users is enabled via Slepian-Wolf coding [10]; however, in that work, information leakage is determined by the Slepian-Wolf code and the parties do not encrypt their data for security.

The remainder of this paper is organized as follows: Section II sets up the notation, presents a mathematical formulation of the problem and states the main results. In Section III, we sketch the proof of Theorem 2.1. Section IV sketches the proof of the achievability of Theorem 2.2 using a random en-

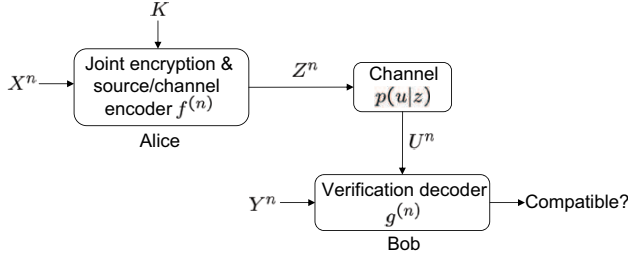


Fig. 1. Bob verifies whether  $Y^n$  is  $\delta$ -compatible with  $X^n$  upon receiving an encrypted version of  $X^n$  over a noisy channel.

ryption and source/channel coding scheme. We also prove the converse of Theorem 2.2. Concluding remarks are presented in Section V.

## II. NOTATION AND PROBLEM SETTING

Throughout the paper, random variables are assumed to be drawn from finite alphabets. A random variable, its realization and alphabet are denoted by uppercase, lowercase and script letters respectively. For example,  $S$  is a random variable over its alphabet  $\mathcal{S}$  and a realization  $s \in \mathcal{S}$  is drawn according to its probability distribution  $p_S(s)$ . When there is no ambiguity, the subscript in  $p_S(s)$  is omitted and we write  $p_S(s)$  as  $p(s)$ . The number of elements in  $\mathcal{S}$  will be denoted by  $|\mathcal{S}|$ , and  $\mathcal{S}^n$  denotes the set of all  $n$ -tuples  $s_1^n = (s_1, s_2, \dots, s_n)$  with elements from  $\mathcal{S}$ . Let  $s_m^n = (s_m, s_{m+1}, \dots, s_n)$  and for simplicity write  $s_1^n$  as  $s^n$ . For a given  $s^n$ , we use  $p_{s^n}$  to denote the empirical probability distribution of singleton random variables derived from  $s^n$ . Finally, all logarithms use base 2.

Let  $\mathcal{X}, \mathcal{Y}$  be arbitrary finite sets, and  $\mathcal{P}(X \times Y)$  be the set of all joint probability distributions of two random variables  $X \in \mathcal{X}$  and  $Y \in \mathcal{Y}$ . Consider a set  $\mathcal{A} \subset \mathcal{P}(X \times Y)$ . We refer to  $\mathcal{A}$  as a “compatible set”. One example of a compatible set is  $\mathcal{A} = \{p(x, y) : I(X; Y) \geq \theta\}$  for some  $\theta \geq 0$ . Let  $D(p(x, y) \| q(x, y))$  denote the KL divergence between probability distributions  $p(x, y)$  and  $q(x, y)$ , and let  $\delta > 0$ . Define a ball with radius  $\delta$  centered at  $p(x, y)$  by  $B(p(x, y), \delta) = \{q(x, y) \in \mathcal{P}(X \times Y) \mid D(q(x, y) \| p(x, y)) < \delta\}$ .

**Definition 2.1:** Suppose  $n$  is large enough. The realizations  $x^n$  and  $y^n$  are said to be  $\delta$ -**compatible** with respect to  $\mathcal{A}$  if and only if the joint empirical distribution  $p_{x^n, y^n}(x, y) \in B(p(x, y), \delta)$  for some  $p(x, y) \in \mathcal{A}$ . Further, the random variables  $X^n$  and  $Y^n$  are  $\delta$ -compatible with respect to  $\mathcal{A}$  if and only if they are generated i.i.d. according to a joint probability distribution  $q(x, y) \in B(p(x, y), \delta)$  for some  $p(x, y) \in \mathcal{A}$ .

The problem setting is shown in Figure 1.  $X^n$  and  $Y^n$  are generated i.i.d according to some joint distribution  $q(x, y)$ . Alice jointly encrypts and encodes  $X^n$  into  $Z^n \in \mathcal{Z}^n$  using her secret key  $K$  independently and uniformly chosen from her key space  $\mathcal{K}$ . Bob receives  $U^n \in \mathcal{U}^n$  which is the output of a noisy channel  $p(u|z)$  with input  $Z^n$ . The channel models not just noisy transmission of  $X^n$  but can also be used to model the actions of an attacker. In the following, we always

assume that the capacity  $C$  of the channel  $p(u|z)$  is positive. Now, without completely decrypting  $U^n$ , Bob wants to verify whether  $X^n$  and  $Y^n$  are  $\delta$ -compatible with respect to  $\mathcal{A}$ .

**Definition 2.2:** Let  $\mathcal{A}$  be a compatible set. A function  $f^{(n)} : \mathcal{X}^n \times \mathcal{K}_1 \rightarrow \mathcal{Z}^n$  is called an  $n$ -length joint encryption/source/channel encoder with information leakage rate  $0 \leq \alpha \leq 1$  if

$$\frac{1}{n} H(X^n | Z^n) \geq (1 - \alpha) H(X)$$

for  $Z^n = f^{(n)}(X^n, K)$ . The verification decoder is defined by  $g^{(n)} : \mathcal{U}^n \times \mathcal{Y}^n \rightarrow \{0, 1\}$ . Here, 0 denotes the event that  $X^n$  and  $Y^n$  are not  $\delta$ -compatible, and 1 denotes the event that  $X^n$  and  $Y^n$  are  $\delta$ -compatible.

For a code  $(f^{(n)}, g^{(n)})$ , we can define a false negative probability  $p_1(f^{(n)}, g^{(n)})$  as

$$\Pr\{g^{(n)}(U^n, Y^n) = 0 \mid q(x, y) \in \bigcup_{p(x, y) \in \mathcal{A}} B(p(x, y), \delta)\},$$

and a false positive probability  $p_2(f^{(n)}, g^{(n)})$  as

$$\Pr\{g^{(n)}(U^n, Y^n) = 1 \mid q(x, y) \notin \bigcup_{p(x, y) \in \mathcal{A}} B(p(x, y), \delta)\}.$$

**Definition 2.3:** A number  $0 \leq \alpha \leq 1$  is an achievable information leakage rate for verification with respect to a compatible set  $\mathcal{A}$  if, for any  $\epsilon > 0$  and any large enough  $n$ , there exists a joint encryption/source/channel-verification code  $(f^{(n)}, g^{(n)})$  with information leakage rate  $\alpha$  such that  $p_1(f^{(n)}, g^{(n)}) \leq \epsilon$  and  $p_2(f^{(n)}, g^{(n)}) \leq \epsilon$ .

**Question 1:** For a given compatible set  $\mathcal{A}$  and a memoryless channel  $p(u|z)$  with capacity  $C > 0$ , what is the set of all achievable information leakage rate  $\alpha$  for verification?

We also consider scenarios in which the verifier (Bob) is curious and will try to recover a fraction  $\alpha$  of the original data  $x^n$ . Alternatively, Alice may leak a public (non-secret) portion of  $x^n$  to Bob in return for his services. This public information may be leaked by the joint encryption/source/channel-verification code.

**Definition 2.4:** A joint encryption/source/channel encoder  $f^{(n)}$  with information leakage rate  $\alpha$  is defined in the same way as that Definition 2.2. A “curious” verification decoder is given by  $g^{(n)} : \mathcal{U}^n \times \mathcal{Y}^n \rightarrow \mathcal{X}^{\alpha n}$  that can decode  $\alpha n$  components of  $X^n$  with high probability if  $(X^n, Y^n)$  are  $\delta$ -compatible with respect to  $\mathcal{A}$ , i.e.,  $p_e(f^{(n)}, g^{(n)}) = \Pr\{g^{(n)}(U^n, Y^n) \neq (X_{t_1}, \dots, X_{t_{\alpha n}})\} \leq \epsilon$ .

As above, we can similarly define an achievable information leakage rate for curious verification. Then, a natural question arises for the curious verifier:

**Question 2:** For a given compatible set  $\mathcal{A}$  and a memoryless channel  $p(u|z)$  with capacity  $C > 0$ , what is maximum achievable information leakage rate  $\alpha$  for curious verification?

Our purpose in this paper is to answer Question 1 and Question 2 using the following two theorems respectively. First, define

$$H_0 = \sup_{q(x, y) \in B(p(x, y), \delta), p(x, y) \in \mathcal{A}} H(X|Y). \quad (1)$$

**Theorem 2.1:** If the compatible set  $\mathcal{A}$  is finite and the channel capacity  $C > 0$ . Then, any  $0 < \alpha \leq 1$  is an achievable information leakage rate for non-curious verification.

**Theorem 2.2:** If the compatible set  $\mathcal{A}$  is finite and the channel capacity  $C > 0$ . Then, the maximum achievable information leakage rate for curious verification is  $\min\{1, \frac{C}{H_0}\}$ , that is, any  $0 < \alpha \leq \min\{1, \frac{C}{H_0}\}$  is achievable for curious verification.

**Discussion:**

- Obviously, if  $\alpha = 0$  or  $C = 0$ , then, the correlation between  $X$  and  $Y$  is totally lost, and the verification will fail;
- Theorem 2.1 implies that as long as the information leakage rate is nonzero, then successful verification will be achieved with high probability. The price of successful verification at low information leakage rate is that the verifier has to wait for a very long time. This will become clear in the proof of Theorem 2.1 in Section III;
- Theorem 2.2 implies that because of the channel constraint, the curious verifier cannot decode a large portion of  $x^n$  if the channel capacity  $C$  is far smaller than  $H_0$ ;
- Theorem 2.2 also implies that a source/channel separation theorem holds for the curious verification framework.

### III. PROOF OF THEOREM 2.1

We shall show that for any  $\alpha > 0$  and large enough  $n$ , there exists a  $n$ -length joint encryption/source/channel-verification code  $(f^{(n)}, g^{(n)})$  with information leakage rate  $\alpha$  such that  $p_1(f^{(n)}, g^{(n)}) < \epsilon$  and  $p_2(f^{(n)}, g^{(n)}) < \epsilon$ . The approach of the proof is similar to that of Theorem 1 in [1]. Let  $\mathcal{A} = \{p_1(x, y), \dots, p_t(x, y)\}$  and  $\epsilon > 0$ . According to the law of large numbers and properties of KL distance, there exists  $m_i$  such that for any  $m \geq m_i$

$$\Pr\{D(p_{X_1^m, Y_1^m}(x, y) \| p_i(x, y)) < \delta\} > 1 - \epsilon \quad (2)$$

if  $(X_1^m, Y_1^m)$  is generated i.i.d. by  $q(x, y) \in B(p_i(x, y), \delta)$ . Let  $m_0 = \max_{i=1, \dots, t} m_i$ . Next, let  $\Theta$  be an  $n$ -length optimal channel code with  $|\mathcal{Z}|^{nC}$  codewords in the sense that the error probability of decoding over this public channel  $p(u|z)$  is arbitrarily small, and define a one-to-one mapping from  $|\mathcal{X}|^{m_0}$  to  $\Theta$ . This is achieved by letting  $n$  be large enough.

Now, define the joint encryption/source/channel encoder  $f^{(n)}$  as follows: given  $(X^n, K)$ , choose a perfect encryption system to encrypt  $X_{m_0+1}^n$  by the key  $K$ . Then,  $f^{(n)}(X^n, K)$  is defined as the codeword in the channel code  $\Theta$  corresponding to  $X_1^{m_0}$ , via the one-to-one mapping defined above. Let the verification rule  $g^{(n)}$  be given as follows:  $X^n$  and  $Y^n$  are  $\delta$ -compatible if and only if

$$D(p_{\hat{X}_1^{m_0}, Y_1^{m_0}}(x, y) \| p_i(x, y)) < \delta \quad (3)$$

for some  $p_i(x, y) \in \mathcal{A}$  where  $\hat{X}_1^{m_0}$  is the random vector corresponding to the decoded codeword in  $\Theta$ . Since  $m_0$  is fixed, the information leakage rate for this code is  $\frac{m_0}{n} \rightarrow 0$  as  $n \rightarrow \infty$ ; in other words,  $\alpha > 0$  is achievable. ■

### IV. PROOF OF THEOREM 2.2

We sketch the proof of the achievability part of Theorem 2.2, relying heavily on the method used in [8] in the context of universal coding for the Slepian-Wolf coding problem. Let  $p_{x^n}$  denote the ‘‘type’’ ([3], [2]) of a sequence  $x^n \in \mathcal{X}^n$ . This is the same as the empirical probability distribution of symbols in  $\mathcal{X}$ . Similarly, let  $p_{x^n, y^n}$ ,  $p_{x^n|y^n}$  and  $p_{y^n|x^n}$  denote the joint and conditional types.

**Lemma 4.1:** [3] The number of different types of sequences in  $\mathcal{X}^n$  is less than or equal to  $(n+1)^{|\mathcal{X}|}$ .

Let  $\alpha H_0 \leq C$ , where  $H_0$  is defined in (1) and  $\mathcal{A}$  is a finite compatible set. Let  $\epsilon$  be an arbitrary fixed positive number. To show that  $\alpha$  is achievable, that is, there exists for large  $n$ , a curious joint encryption and source/channel code  $(f^{(n)}, g^{(n)})$  with  $p_e(f^{(n)}, g^{(n)}) < \epsilon$ , we employ a random coding scheme consisting of a perfect encryption system, an optimal channel code  $\Theta$  and a random source coding scheme. To begin, label all types over  $\mathcal{X}^{\alpha n}$  by indices  $i' \in \mathcal{I}' = \{1, 2, \dots, (\alpha n + 1)^{|\mathcal{X}|}\}$ .

#### A. Achievability with Random Coding Scheme

- Choose a perfect encryption system  $\Phi$ , such as a one-time pad, and an optimal channel code  $\Theta$  with  $|\mathcal{Z}|^{nC}$  codewords such that the error probability of decoding  $p_e(\Theta) < \epsilon$ . The existence of such a channel code is guaranteed by the standard Channel Coding Theorem since the channel capacity is  $C > 0$  by the assumption.
- Alice uniformly distributes all  $x^{\alpha n}$  among  $2^{n\alpha H_0}$  bins, indexed by  $i \in \mathcal{I} = \{1, 2, \dots, 2^{n\alpha H_0}\}$ .
- Define a one-to-one mapping from  $\mathcal{I} \times \mathcal{I}'$  to  $\Theta$ . Since  $\alpha H_0 \leq C$  and  $\log(|\mathcal{I}'|)/n$  goes to zero as  $n \rightarrow \infty$ , such a mapping exists.
- Random encoding: Given  $X^n = (X_1^{(1-\alpha)n}, X_{(1-\alpha)n+1}^n)$  and key  $K$ , Alice uses the key  $K$  to encrypt  $X_1^{(1-\alpha)n}$  using the encryption scheme  $\Phi$ . From her random codebook, Alice finds the bin containing  $X_{(1-\alpha)n+1}^n$ , and records the bin index  $I$ . Then, she computes the type (empirical distribution) of  $X_{(1-\alpha)n+1}^n$  and records the type index  $I'$ . Finally, Alice transmits the codeword  $Z^n \in \Theta$  corresponding to the pair  $(I, I')$  to the verifier.
- Curious decoding and verification: Upon receiving  $U^n$ , the verifier first performs channel decoding with the code  $\Theta$ . By the Channel Coding Theorem, with probability one, the verifier decodes  $(I, I')$  correctly, and computes entropy  $H(I')$  of the type with index  $I'$ . Now consider the following cases:
  - If  $H(I') \leq H_0$ , then there exists a unique  $X_{(1-\alpha)n+1}^n$  with type  $I'$  in the codebook bin  $I$ . Thus, the portion  $X_{(1-\alpha)n+1}^n$  can be decoded correctly without using the side information  $Y^n$ .
  - If  $H(I') > H_0$ , then, in the codebook bin  $I$ , the verifier decodes  $\hat{X}_{(1-\alpha)n+1}^n = \arg \min H(p_{\hat{X}_{(1-\alpha)n+1}^n | Y_{(1-\alpha)n+1}^n})$ , where the minimum is taken over all  $\tilde{X}_{(1-\alpha)n+1}^n$  of type  $I'$  that also lie in the codebook bin  $I$ ,

and  $Y_{(1-\alpha)n+1}^n$  is the (small) portion of  $Y^n$  corresponding to the leaked portion of  $X^n$ .

- Verification: Bob obtains  $\hat{X}_{(1-\alpha)n+1}^n$  from the above decoding step, and then computes the empirical probability distribution from it. Finally, he employs the verification rule using KL divergence in (3) as described in the proof of Theorem 2.1.

### B. Information Leakage Rate and Error Probability

Since Alice transmits a codeword in  $\Theta$  corresponding to a pair comprising of a codebook bin index and a type index, the information about Alice's vector leaked to the verifier by the protocol described earlier is given by

$$\begin{aligned} \frac{1}{n}H(X^n|Z^n) &= \frac{1}{n}H(X^n|(I, I')) \\ &\geq \frac{1}{n}H(X^n|X_{(1-\alpha)n+1}^n) \\ &= \frac{1}{n}H(X_1^{(1-\alpha)n}) = (1-\alpha)H(X). \end{aligned}$$

Following the counting approach in [8], the error probability of the event  $X_{(1-\alpha)n+1}^n \neq \hat{X}_{(1-\alpha)n+1}^n$  is less than  $\epsilon$  if there is no error occurrence in the channel decoding step. For this channel code  $\Theta$ , the error probability of decoding is less than  $\epsilon$  for large enough  $n$ . Therefore, the total average error probability of the event  $X_{(1-\alpha)n+1}^n \neq \hat{X}_{(1-\alpha)n+1}^n$  is less than  $2\epsilon$ . Following the analysis in Section III, for large  $n$ , there exists a joint encryption/source/channel-verification code  $(f^{(n)}, g^{(n)})$  such that  $p_1(f^{(n)}, g^{(n)}) < \epsilon$  and  $p_2(f^{(n)}, g^{(n)}) < \epsilon$ . This completes the proof of achievability in Theorem 2.2. ■

### C. Proof of Converse in Theorem 2.2

In this section, we shall prove the converse part of Theorem 2.2. Assume that for an arbitrary number  $\epsilon > 0$ , there exists for any sufficiently large  $n$ , an  $n$ -length curious joint encryption/source/channel-verification code  $(f^{(n)}, g^{(n)})$  with information leakage rate  $\alpha$  for the compatible joint probability set  $\mathcal{A}$  such that, for any  $q(x, y) \in B(p(x, y), \delta)$  and  $p(x, y) \in \mathcal{A}$ ,  $\Pr\{g^n(U^n, Y^n) \neq X_{(1-\alpha)n+1}^n\} \leq \epsilon$ . We want to show that  $\alpha H_0 \leq C$ , where  $C$  is the channel capacity of the discrete memoryless channel  $p(u|z)$ .

We have

$$\begin{aligned} nH(X|Y) &= H(X^n|Y^n) \\ &= I(X^n; U^n|Y^n) + H(X^n|U^n, Y^n) \\ &= H(U^n|Y^n) - H(U^n|X^n, Y^n) + H(X^n|U^n, Y^n) \\ &\stackrel{(a)}{\leq} H(U^n) - H(U^n|X^n) + H(X_1^{(1-\alpha)n}|U^n, Y^n) \\ &\quad + H(X_{(1-\alpha)n+1}^n|U^n, Y^n, X_1^{(1-\alpha)n}) \\ &\leq I(U^n; X^n) + H(X_1^{(1-\alpha)n}|Y_1^{(1-\alpha)n}) \\ &\quad + H(X_{(1-\alpha)n+1}^n|U^n, Y^n) \\ &\stackrel{(b)}{\leq} I(U^n; Z^n) + (1-\alpha)nH(X|Y) + n\epsilon, \end{aligned}$$

which yields

$$n\alpha H(X|Y) \leq I(U^n; Z^n) + n\epsilon \leq nC + n\epsilon,$$

where (a) follows from fact that  $Y^n \rightarrow X^n \rightarrow U^n$  is a Markov chain; (b) follows from Fano's inequality, i.e.,  $\frac{1}{n}H(X_{(1-\alpha)n+1}^n|U^n, Y^n) \leq \epsilon$ . Thus,  $\alpha H(X|Y) \leq C + \epsilon$  for any  $q(x, y) \in B(p(x, y), \delta)$  where  $p(x, y) \in \mathcal{A}$ . Since  $\epsilon$  can be arbitrary small, therefore  $\alpha H_0 \leq C$ . The proof of the converse part is thus complete. ■

## V. CONCLUSIONS

This paper considers information leakage for encryption schemes in a distributed source coding setting. Given an encrypted vector  $X^n$  from Alice, Bob determines whether  $X^n$  is  $\delta$ -compatible with his vector  $Y^n$ , i.e., whether they are drawn from one of many permissible joint distributions. Using identification via compressed data, it is shown that compatibility in this sense can be verified at asymptotically zero rate. Further, we consider the scenario in which the verifier (Bob) is curious, or is allowed to decode a certain portion of  $X^n$  as payment for his services. It is shown that the maximum information that Bob can obtain about Alice's signal depends upon the capacity of the noisy channel between Alice and Bob and on the Slepian-Wolf rates for the compatible set. This region can be achieved by universal random coding schemes. The converse also suggests a source/channel separation theorem for the curious verifier.

## REFERENCES

- [1] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, vol. 28, pp. 656–715, Oct. 1949.
- [2] H. Yamamoto, "Information Theory in Cryptology," *IEICE Transactions*, vol. E.74, no. 9, pp. 2456–2464, Sept. 1991.
- [3] U. M. Maurer, "The Role of Information Theory in Cryptography," in *Proceedings of the Fourth IMA Conference on Cryptography and Coding*, Cirencester, England, 1993.
- [4] H. Yamamoto, "Rate-Distortion Theory for the Shannon Cipher System," *IEEE Transactions on Information Theory*, vol. 43, no. 3, pp. 827–835, May 1997.
- [5] N. Merhav, "On the Shannon Cipher System with a Capacity-Limited Key-Distribution Channel," *IEEE Transactions on Information Theory*, vol. 52, no. 3, pp. 1269–1273, Mar. 2006.
- [6] M. Johnson, P. Ishwar, V. Prabhakaran, D. Schonberg, and K. Ramchandran, "On Compressing Encrypted Data," *IEEE Transactions on Signal Processing*, vol. 52, no. 10, pp. 2992–3006, Oct. 2004.
- [7] R. Ahlswede, E.-H. Yang, and Z. Zhang, "Identification via Compressed Data," *IEEE Transactions on Information Theory*, vol. 43, no. 1, pp. 48–70, Jan. 1997.
- [8] D. He, A. Jagmohan, and L. Lu, "Secure Collaboration Using Slepian-Wolf Codes," in *Proceedings of the IEEE International Conference on Image Processing*, San Diego, CA, Oct. 2008.
- [9] D. Slepian and J. K. Wolf, "Noiseless Coding of Correlated Information Sources," *IEEE Transactions on Information Theory*, pp. 471–480, July 1973.
- [10] Y. Oohama and T. S. Han, "Universal Coding for the Slepian-Wolf Data Compression System and the Strong Converse Theorem," *IEEE Transactions on Information Theory*, vol. 40, no. 6, pp. 1908–1919, Nov. 1994.
- [11] I. Csiszár and J. Körner, "Information theory: Coding theorems for discrete memoryless systems," New York: Academic Press, 1981.
- [12] T. M. Cover and J. A. Thomas, "Elements of information theory," New York: Wiley, 1991.