

# Secure Lossy Source-Channel Wiretapping with Side Information at the Receiving Terminals

Joffrey Villard\*, Pablo Piantanida\* and Shlomo Shamai (Shitz)<sup>†</sup>

\* Department of Telecommunications

SUPELEC

91192 Gif-sur-Yvette, France

Email: {joffrey.villard, pablo.piantanida}@supelec.fr

<sup>†</sup> Department of Electrical Engineering

Technion - Israel Institute of Technology

Technion city, Haifa 32000, Israel

Email: sshlomo@ee.technion.ac.il

## Abstract

The problem of secure lossy source-channel wiretapping with arbitrarily correlated side informations at both receivers is investigated. This scenario consists of an encoder (referred to as Alice) that wishes to compress a source and send it through a noisy channel to a legitimate receiver (referred to as Bob). In this context, Alice must simultaneously satisfy the desired requirements on the distortion level at Bob, and the equivocation rate at the eavesdropper (referred to as Eve). This setting can be seen as a generalization of the conventional problems of secure source coding with side information at the decoders, and the wiretap channel. Inner and outer bounds on the rate-distortion-equivocation region for the case of arbitrary channels and side informations are derived. In some special cases of interest, it is shown that separation holds. By means of an appropriate coding, the presence of any statistical difference among the side informations, the channel noises, and the distortion at Bob can be fully exploited in terms of secrecy.

## I. INTRODUCTION

Consider a system composed of three nodes (or sensors) where each one is measuring an analogue source (or random field) as a function of time. In order to make reliable decisions, one of these sensors (referred to as Bob) can be helped by another one (referred to as Alice), which will transmit some compressed version of its own measurement through a noisy wireless channel. The third sensor (referred to as Eve) can listen to the wireless medium, and capture some information during the communication. Considering that Eve is not to be trusted (she is an *eavesdropper*), Alice wishes to leak the least possible amount of information about its source.

The above scenario involves most of the major information-theoretic issues on (secure) source and channel coding. In fact, the information-theoretic notion of secrecy was first introduced by Shannon in [1], where security is measured through the equivocation rate, *i.e.*, the remaining uncertainty about the message, at Eve. In terms of source coding,

The work of J. Villard is supported by DGA (French Armament Procurement Agency). This research is partially supported by the FP7 Network of Excellence in Wireless COMMunications NEWCOM++.

Slepian and Wolf [2], and Wyner and Ziv [3] introduced the problem of source coding with side information at the decoder. The corresponding *secure* scenarios *i.e.*, involving an eavesdropper with its own side information, have been recently studied in [4]–[8]. Secure source coding scenarios involving a secure rate-limited channel between Alice and Bob, which allows the use of secret keys, have also been studied in various works [9]–[12]. On the other hand, extensive research has been done during the recent years on secure communications over noisy channels. The wiretap channel was introduced by Wyner [13], who showed that it is possible to send information with perfect secrecy as long as the channel of Bob is less noisy than the channel of Eve. Csiszàr and Kórnér [14] extend this result to the setting of general broadcast channels with arbitrary equivocation rate (allowing also a common message to both receivers). Several extensions of the wiretap channel have since been done (cf. [10], [15]–[17] and references therein). Whereas, secure lossy source-channel coding problems have received fewer attention. In a recent work [15], Merhav considered such a setting by assuming that Eve has a degraded channel with degraded side information with respect to Bob, and that a secret key can be shared between Alice and Bob.

In this paper, we investigate the general problem of secure lossy source-channel wiretapping, with arbitrarily correlated side informations as depicted in Fig. 1. The main goal is to understand how Alice can take advantage of the presence of statistical differences among the side informations and the channel noises to reveal the minimum amount of information to Eve, and satisfy the required distortion level at Bob. It should be emphasized that the central difficulty of this problem lies in the evaluation of the equivocation at Eve. We derive single-letter characterizations of inner and outer bounds on the general rate-distortion-equivocation region (in Section II). Section III provides special cases for which separation holds. The sketches of the proofs are relegated to Sections IV and V. Finally, Section VI presents discussions and an application example to binary sources.

### Notations

For any sequence  $(x_i)_{i \in \mathbb{N}^*}$ , notation  $x_k^n$  stands for the collection  $(x_k, x_{k+1}, \dots, x_n)$ .  $x_1^n$  is simply denoted by  $x^n$ . Entropy is denoted by  $H(\cdot)$ , and mutual information by  $I(\cdot; \cdot)$ . Let  $X, Y$  and  $Z$  be three random variables on some alphabets with probability distribution  $p$ . If  $p(x|y, z) = p(x|y)$  for each  $x, y, z$ , then they form a Markov chain, which is denoted by  $X \dashv\vdash Y \dashv\vdash Z$ . The set of nonnegative real numbers is denoted by  $\mathbb{R}_+$ . For each  $x \in \mathbb{R}$ , notation  $[x]_+$  stands for  $\max(0; x)$ .

## II. PROBLEM DEFINITION AND MAIN RESULTS

### A. Problem Definition

In this section, we give a more rigorous formulation of the context depicted in Fig. 1. Let  $\mathcal{A}, \mathcal{B}, \mathcal{E}, \mathcal{X}, \mathcal{Y}$ , and  $\mathcal{Z}$  be six finite sets. Alice, Bob, and Eve observe the sequences of random variables  $(A_i)_{i \in \mathbb{N}^*}$ ,  $(B_i)_{i \in \mathbb{N}^*}$ , and  $(E_i)_{i \in \mathbb{N}^*}$ , respectively, which take values on  $\mathcal{A}, \mathcal{B}$ , and  $\mathcal{E}$ , resp. For each  $i \in \mathbb{N}^*$ , the random variables  $A_i, B_i$ , and  $E_i$  are distributed according to the joint distribution  $p(a, b, e)$  on  $\mathcal{A} \times \mathcal{B} \times \mathcal{E}$ . Moreover, they are independent across time  $i$ . Alice can also communicate with Bob and Eve through a discrete memoryless channel with input  $X$  on  $\mathcal{X}$ , and outputs  $Y, Z$  on  $\mathcal{Y}, \mathcal{Z}$ , respectively. This channel is defined by its transition probability  $P(YZ|X)$ .

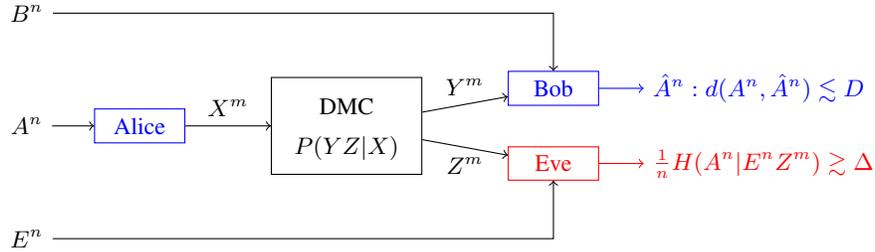


Figure 1: Secure lossy source-channel wiretapping in the presence of side information at the receivers.

Let  $d : \mathcal{A} \times \mathcal{A} \rightarrow [0; d_{\max}]$  be a finite distortion measure *i.e.*, such that  $0 \leq d_{\max} < \infty$ . We also denote by  $d$  the component-wise mean distortion on  $\mathcal{A}^n \times \mathcal{A}^n$  *i.e.*, for each  $a^n, b^n \in \mathcal{A}^n$ ,  $d(a^n, b^n) = \frac{1}{n} \sum_{i=1}^n d(a_i, b_i)$ .

*Definition 1:* An  $(n, m)$ -code for source-channel coding in this setup is defined by

- A (stochastic) encoding function at Alice  $F : \mathcal{A}^n \rightarrow \mathcal{X}^m$ , defined by some transition probability  $P_{X^m|A^n}(\cdot|\cdot)$ ,
- A decoding function at Bob  $g : \mathcal{Y}^m \times \mathcal{B}^n \rightarrow \mathcal{A}^n$ .

The rate of such a code is defined as quantity  $m/n$  (*channel uses per source symbol*).

*Definition 2:* A tuple  $(k, D, \Delta) \in \mathbb{R}_+^3$  is said to be *achievable* if, for any  $\varepsilon > 0$ , there exists an  $(n, m)$ -code  $(F, g)$  s.t.:

$$\begin{aligned} \frac{m}{n} &\leq k + \varepsilon, \\ \mathbb{E}[d(A^n, g(Y^m, B^n))] &\leq D + \varepsilon, \\ \frac{1}{n} H(A^n | E^n Z^m) &\geq \Delta - \varepsilon, \end{aligned}$$

when the input of the channel  $X^m$  is the output of the encoder  $F(A^n)$ . The set of all achievable tuples is denoted by  $\mathcal{R}^*$  and is referred to as the *rate-distortion-equivocation region*.

## B. Main Results

The following theorem gives an inner bound on  $\mathcal{R}^*$  *i.e.*, it defines region  $\mathcal{R}_{\text{in}} \subset \mathcal{R}^*$ . The proof is outlined in Section IV.

*Theorem 1 (Inner Bound):* The set of all tuples  $(k, D, \Delta)$  in  $\mathbb{R}_+^3$  such that there exist random variables  $U, V, Q, T$  on some finite sets  $\mathcal{U}, \mathcal{V}, \mathcal{Q}, \mathcal{T}$ , respectively, with joint distribution  $p(uvqtabyxyz) = p(u|v)p(v|a)p(abe)p(q|t)p(t|x)p(xyz)$ , and a function  $\hat{A} : \mathcal{V} \times \mathcal{B} \rightarrow \mathcal{A}$ , verifying the following inequalities, is achievable:

$$\begin{aligned} I(U; A|B) &\leq kI(Q; Y), \\ I(V; A|B) &\leq kI(T; Y), \\ D &\geq \mathbb{E}[d(A, \hat{A}(V, B))], \\ \Delta &\leq H(A|UE) - \left[ I(V; A|UB) - k \left( I(T; Y|Q) - I(T; Z|Q) \right) \right]_+. \end{aligned}$$

The first two inequalities in Theorem 1 correspond to sufficient conditions for the transmission of two source layers  $U, V$  in channel variables  $Q, T$ , resp. The first layer ( $U \mapsto Q$ ) can be seen as a *common* message which is

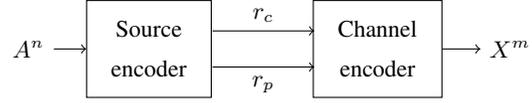
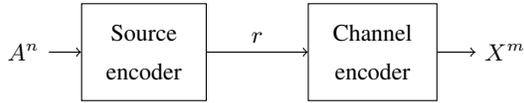


Figure 2: Traditional (“informational”) separation. Figure 3: Proposed system (“operational” separation).

considered to be known at Eve, as shown by the term  $H(A|UE)$  in the equivocation. The second layer ( $V \mapsto T$ ) forms a *private* message which is (partially) protected by adding an independent random noise [14], [17]. The term inside the brackets in the fourth inequality corresponds to the information that Eve can still obtain on this protected layer.

The following theorem gives an outer bound on  $\mathcal{R}^*$  *i.e.*, it defines region  $\mathcal{R}_{\text{out}} \supset \mathcal{R}^*$ . The proof is outlined in Section V.

*Theorem 2 (Outer Bound):* For each achievable tuple  $(k, D, \Delta)$ , there exist random variables  $U, V, Q, T$  on some finite sets  $\mathcal{U}, \mathcal{V}, \mathcal{Q}, \mathcal{T}$ , respectively, and a function  $\hat{A} : \mathcal{V} \times \mathcal{B} \rightarrow \mathcal{A}$ , such that  $p(uvqtabexyz) = p(uv|a)p(abe)p(q|t)p(t|x)p(xyz)$ , and

$$\begin{aligned} I(V; A|B) &\leq kI(T; Y) , \\ D &\geq \mathbb{E}[d(A, \hat{A}(V, B))] , \\ \Delta &\leq H(A|UE) - \left[ I(V; A|B) - I(U; A|B) - k \left( I(T; Y|Q) - I(T; Z|Q) \right) \right]_+ . \end{aligned}$$

Notice that the inner and outer bounds do not meet in general. In Section III, we provide several cases where  $\mathcal{R}_{\text{in}}$  is optimal. In fact, there are two main differences between  $\mathcal{R}_{\text{in}}$  and  $\mathcal{R}_{\text{out}}$ :

- The first inequality of Theorem 1, which is needed in our scheme to characterize the equivocation at Eve, may not be optimal for the general case,
- The Markov chain  $U \text{---} V \text{---} A \text{---} (B, E)$  is assumed in Theorem 1 while only  $(U, V) \text{---} A \text{---} (B, E)$  is proved for arbitrary codes in Theorem 2.

### C. Coding Scheme Based on “Operational” Separation

In traditional *separated* schemes, two *stand-alone* components successively perform source and channel coding, as depicted in Fig. 2. However the proposed scheme (which achieves region  $\mathcal{R}_{\text{in}}$ ) does not satisfy this separation principle: The source encoder outputs two layers (as in [8]) which are further encoded by using the channel code for a *broadcast channel with a confidential message* [14]. This results in two independent (but not stand-alone) source and channel components leading to statistically independent source and channel variables (as in [18] for Slepian-Wolf coding over broadcast channels) *i.e.*, “operational” separation holds (see Fig. 3). As a matter of fact, the first inequality of Theorem 1 *i.e.*,  $I(U; A|B) \leq kI(Q; Y)$ , prevents from separately choosing variables  $U$  and  $Q$  which would maximize the equivocation rate at Eve.

### III. SPECIAL CASES OF INTEREST

In this section, we characterize the optimality of the inner bound  $\mathcal{R}_{\text{in}}$  for some special cases.

#### A. Bob Has Less Noisy Side Information

*Definition 3:* Random variable  $B$  is *less noisy* than  $E$  w.r.t.  $A$ , if  $I(U; B) \geq I(U; E)$  for each r.v.  $U$  s.t.  $U \text{---} A \text{---} (B, E)$  form a Markov chain. This relation is denoted by  $B \succeq_A E$ .

*Proposition 1:* If  $B \succeq_A E$ , then region  $\mathcal{R}^*$  reduces to the set of all tuples  $(k, D, \Delta) \in \mathbb{R}_+^3$  such that there exist random variables  $V, Q, T$  on some finite sets  $\mathcal{V}, \mathcal{Q}, \mathcal{T}$ , respectively, with joint distribution  $p(vqt abexyz) = p(v|a)p(abe)p(q|t)p(t|x)p(xyz)$ , and a function  $\hat{A} : \mathcal{V} \times \mathcal{B} \rightarrow \mathcal{A}$ , verifying the following inequalities:

$$\begin{aligned} I(V; A|B) &\leq kI(T; Y) , \\ D &\geq \mathbb{E}[d(A, \hat{A}(V, B))] , \\ \Delta &\leq H(A|E) - \left[ I(V; A|B) - k \left( I(T; Y|Q) - I(T; Z|Q) \right) \right]_+ . \end{aligned}$$

*Remark 1:* In this case, the optimal coding reduces to a *Wyner-Ziv* source encoder [3] followed by a classical *wiretap* channel encoder [14], [17], and hence the conventional separation principle holds (Fig. 2).

*Proof:* The above region is achievable by setting variable  $U$  to a constant value in Theorem 1. On the other hand, the third inequality of Theorem 2 writes:

$$\begin{aligned} \Delta &\leq H(A|UE) \\ \Delta &\leq H(A|VB) + I(A; B|U) - I(A; E|U) - k \left( I(T; Y|Q) - I(T; Z|Q) \right) . \end{aligned}$$

Since  $B \succeq_A E$ , and  $U \text{---} A \text{---} (B, E)$  form a Markov chain,  $I(A; B|U) - I(A; E|U) \leq I(A; B) - I(A; E)$ . Moreover  $H(A|UE) \leq H(A|E)$ . In this case, the outer bound  $\mathcal{R}_{\text{out}}$  is thus included in (and consequently equal to)  $\mathcal{R}_{\text{in}}$ . ■

If the informations at Eve (both side information, and channel output) are degraded versions of Bob's ones *i.e.*, if both Markov chains  $A \text{---} B \text{---} E$ , and  $X \text{---} Y \text{---} Z$  hold, then Proposition 1 reduces to the results in [15]. In this case, variable  $Q$  is set to a constant value, and  $T = X$ .

#### B. Eve Has Less Noisy Channel Output

*Proposition 2:* If  $Z \succeq_X Y$ , then region  $\mathcal{R}^*$  reduces to the set of all tuples  $(k, D, \Delta) \in \mathbb{R}_+^3$  such that there exist random variables  $U, V$  on some finite sets  $\mathcal{U}, \mathcal{V}$ , respectively, with joint distribution  $p(uv abexyz) = p(u|v)p(v|a)p(abe)p(xyz)$ , and a function  $\hat{A} : \mathcal{V} \times \mathcal{B} \rightarrow \mathcal{A}$ , verifying the following inequalities:

$$\begin{aligned} I(V; A|B) &\leq kI(X; Y) , \\ D &\geq \mathbb{E}[d(A, \hat{A}(V, B))] , \\ \Delta &\leq H(A|VB) + I(A; B|U) - I(A; E|U) . \end{aligned}$$

*Remark 2:* In this case, the optimal scheme reduces to a *secure* source encoder [8] followed by a conventional channel encoder, and hence separation principle holds (Fig. 2).

*Proof:* The above region is achievable by setting  $Q = T = X$  in Theorem 1. However, a new proof is needed to obtain the converse part of Proposition 2. Here, auxiliary variables are defined as follows, for each  $i \in \{1, \dots, n\}$ , and each  $j \in \{1, \dots, m\}$ :

$$\begin{aligned} U_i &= (B_{i+1}^n, E^{i-1}, Y^m), \\ V_i &= (A^{i-1}, B^{i-1}, B_{i+1}^n, E^{i-1}, Y^m), \\ Q_j &= (E^n, Y^{j-1}, Z_{j+1}^m), \\ T_j &= (A^n, E^n, Y^{j-1}, Z_{j+1}^m). \end{aligned}$$

Now, both  $U_i \text{---} V_i \text{---} A_i \text{---} (B_i, E_i)$ , and  $Q_j \text{---} T_j \text{---} X_j \text{---} (Y_j, Z_j)$  form Markov chains. Following the arguments given at Section V, we can define new auxiliary variables verifying the above Markov chains and the following inequalities:

$$\begin{aligned} I(V; A|B) &\leq kI(T; Y), \\ D &\geq \mathbb{E}[d(A, \hat{A}(V, B))], \\ \Delta &\leq H(A|UE) - I(V; A|UB) + k(I(T; Y|Q) - I(T; Z|Q)). \end{aligned}$$

Since  $Z \succeq_X Y$ , and  $Q \text{---} T \text{---} X \text{---} (Y, Z)$  form a Markov chain,  $I(T; Y|Q) - I(T; Z|Q) \leq 0$ . Noting that  $I(T; Y) \leq I(X; Y)$ , this concludes the proof. ■

Defining the transmitted rate as  $R = kI(X; Y)$ , Proposition 2 provides the *rate-distortion-equivocation* region in the secure *source* coding setup [8, Theorem 1].

#### IV. SKETCH OF PROOF OF THEOREM 1 (INNER BOUND)

The proof is based on the use of a secure source coding scheme [8], and a channel coding scheme for wiretap channel [14], [17]. Full details are omitted due to the lack of space and will be provided in an extended version of this paper.

*Source Encoder:* The source encoder is formed of two layers corresponding to variables  $U, V$ , with respective rates  $R_1, R_2$ . Random binning *a la* Wyner-Ziv [3] is performed prior to transmission. The next constraints ensure that Bob can decode  $(U, V)$  from bin indices  $(r_1, r_2)$  with an arbitrarily small error probability:

$$\begin{aligned} R_1 &> I(U; A|B), \\ R_2 &> I(V; A|UB). \end{aligned}$$

*Bits Recombination:* Bin indices  $(r_1, r_2)$  are mapped to indices  $r_c$  and  $r_p$ , with respective rates  $R_c, R_p$ , through a one-to-one mapping, such that  $r_1 = M'(r_c)$  for some mapping  $M'$ . This requires the following constraints:

$$R_1 + R_2 = R_c + R_p ,$$

$$R_1 \leq R_c .$$

*Channel Encoder:* The channel encoder is composed of two layers corresponding to variables  $Q, X$ , transmitting messages  $r_c, r_p$ , respectively. Following [14], [17], an independent random noise  $r_f$ , with rate  $R_f$  s.t.  $R_f < kI(X; Z|Q)$ , is also transmitted with message  $r_p$ . The following constraints ensure that Bob can decode  $r_c, (r_p, r_f)$  from his channel output  $Y$  with an arbitrarily small probability of error:

$$R_c < kI(Q; Y) ,$$

$$R_p + R_f < kI(X; Y|Q) .$$

*Distortion at Bob:* Provided the above constraints are verified, Bob can decode  $V$  with an arbitrarily small probability of error, and compute an estimate  $\hat{A}$  of  $A$  with mean distortion  $\mathbb{E}[d(A, \hat{A}(V, B))]$ .

*Equivocation Rate at Eve:* After some algebraic manipulations, it can be proved that the proposed scheme achieves any equivocation rate verifying the following inequality:

$$\Delta \leq H(A|UE) - R_2 + R_p + R_f - kI(X; Z|Q) .$$

The proof (which is omitted here due to the lack of space) follows the arguments of both [8, Section IV-A], and [17, Section 2.3], and relies on relation  $r_1 = M'(r_c)$ .

*End of Proof:* Putting all inequalities together, using Fourier-Motzkin elimination, and prefixing an arbitrary DMC  $P(X|T)$  to the DMC  $P(Y, Z|X)$  prove Theorem 1. ■

## V. SKETCH OF PROOF OF THEOREM 2 (OUTER BOUND)

Due to the lack of space, we only provide some of the basic ideas underlying the proof of Theorem 2. Details will be provided in an extended version of this paper.

For each  $i \in \{1, \dots, n\}$  (resp. each  $j \in \{1, \dots, m\}$ ), define the source (resp. channel) auxiliary random variables  $U_i, V_i$  (resp.  $Q_j, T_j$ ) as

$$U_i = ( B_{i+1}^n, E^{i-1}, Z^m ) ,$$

$$V_i = ( A^{i-1}, B^{i-1}, B_{i+1}^n, E^{i-1}, Y^m ) ,$$

$$Q_j = ( B^n, Y^{j-1}, Z_{j+1}^m ) ,$$

$$T_j = ( A^n, B^n, Y^{j-1}, Z_{j+1}^m ) .$$

Note that  $(U_i, V_i) \text{---} A_i \text{---} (B_i, E_i)$ , and  $Q_j \text{---} T_j \text{---} X_j \text{---} (Y_j, Z_j)$  form Markov chains.

*Rate:* Using the chain rule for conditional mutual information, the Markov chain  $(A_i, Y^m) \ominus (A^{i-1}, B^n) \ominus E^{i-1}$ , and the fact that random variables  $A_i$ ,  $B_i$ , and  $E_i$  are independent across time, we can prove that  $I(A^n; Y^m | B^n) = \sum_{i=1}^n I(A_i; V_i | B_i)$ .

From the chain rule, and the non-negativity of mutual information, we can also prove the following upper bound:  $I(A^n; Y^m | B^n) \leq \sum_{j=1}^m I(T_j; Y_j)$ .

The above equations yield

$$\sum_{i=1}^n I(A_i; V_i | B_i) \leq \sum_{j=1}^m I(T_j; Y_j) .$$

*Distortion at Bob:* Bob reconstructs  $g(Y^m, B^n)$ . The  $i$ -th coordinate of this estimate is  $g_i(Y^m, B^{i-1}, B_i, B_{i+1}^n) \triangleq \hat{A}_i(V_i, B_i)$ . The component-wise mean distortion at Bob thus writes:

$$\mathbb{E}[d(A^n, g(Y^m, B^n))] = \frac{1}{n} \sum_{i=1}^n \mathbb{E} \left[ d(A_i, \hat{A}_i(V_i, B_i)) \right] .$$

*Equivocation Rate at Eve:* From the chain rule for conditional entropy, and the Markov chain  $A_i \ominus (A_{i+1}^n, E^i, Z^m) \ominus (B_{i+1}^n, E_{i+1}^n)$ , we can prove the following upper bound on the equivocation at Eve:

$$H(A^n | E^n Z^m) \leq \sum_{i=1}^n H(A_i | U_i E_i) .$$

Using the Markov chain  $B^n \ominus A^n \ominus Z^m$ , we expand the equivocation at Eve as follows:

$$H(A^n | E^n Z^m) = \underbrace{I(A^n; Y^m | B^n) - I(A^n; Z^m | B^n)}_{\Delta_c} + \underbrace{H(A^n | B^n Y^m) + I(A^n; B^n | Z^m) - I(A^n; E^n | Z^m)}_{\Delta_s} .$$

Following [14, Section VI], [17, Section 2.4], we can prove that  $\Delta_c = \sum_{j=1}^m I(T_j; Y_j | Q_j) - I(T_j; Z_j | Q_j)$ , and following [8, Section IV-B],  $\Delta_s = \sum_{i=1}^n H(A_i | V_i B_i) + I(A_i; B_i | U_i) - I(A_i; E_i | U_i)$ .

*End of Proof:* Following the usual technique, we define independent random variables  $K$ , and  $J$ , uniformly distributed over the sets  $\{1, \dots, n\}$ , and  $\{1, \dots, m\}$ , respectively. We also define random variables  $A = A_K$ ,  $B = B_K$ ,  $E = E_K$ ,  $U = (K, U_K)$ ,  $V = (K, V_K)$ ,  $X = X_J$ ,  $Y = Y_J$ ,  $Z = Z_J$ ,  $Q = (J, Q_j)$ , and  $T = (J, T_j)$ .  $(U, V) \ominus A \ominus (B, E)$  and  $Q \ominus T \ominus X \ominus (Y, Z)$  still form Markov chains. Using these definitions, we prove the three inequalities of Theorem 2. Since they only involve *marginal* distributions of auxiliary variables, w.r.t. corresponding source/channel variables *i.e.*,  $p(uv|a)$  and  $p(qt|x)$ , we can define new auxiliary variables  $\tilde{U}$ ,  $\tilde{V}$ ,  $\tilde{Q}$ , and  $\tilde{T}$ , with identical marginal distributions, such that the (global) joint distribution writes  $p(uvqtabexyz) = p(uv|a)p(abe)p(q|t)p(t|x)p(xyz)$  *i.e.*, source and channel variables are independent. ■

## VI. APPLICATION EXAMPLE AND DISCUSSION

Consider the source model depicted in Fig. 4, where the source is binary and the side information at Bob, resp. Eve, is the output of a binary erasure channel (BEC) with erasure probability  $\beta \in [0, 1]$ , resp. a binary symmetric channel (BSC) with crossover probability  $\epsilon \in [0, 1/2]$ , with input  $A$ . The communication channel is similar to the one of [13]: It consists of a noiseless channel from Alice to Bob, and a BSC with crossover probability  $\zeta \in [0, 1/2]$ , from Alice to Eve.

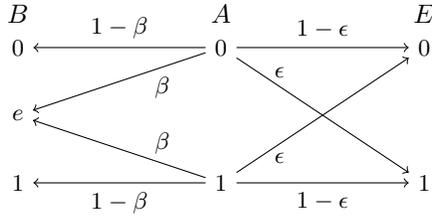
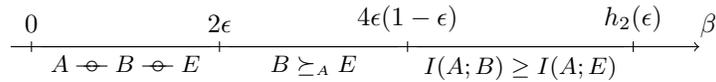


Figure 4: Binary erasure/binary symmetric side informations.

This model is of interest since neither Bob nor Eve can always be a lessnoisy decoder for all values of  $(\beta, \epsilon)$ . Let  $h_2$  denotes the binary entropy function given by  $h_2(x) = -x \log_2(x) - (1-x) \log_2(1-x)$ . According to the values of the parameters  $(\beta, \epsilon)$ , it can be shown by means of standard manipulations [19] that the side informations satisfy the properties summarized in Fig. 5.

Figure 5: Relative properties of the side informations as a function of  $(\beta, \epsilon)$ .

From now on, let the distortion level at Bob be zero *i.e.*, he performs *lossless* reconstruction, and assume for simplicity that the source is uniformly distributed *i.e.*,  $\Pr\{A=0\} = \Pr\{A=1\} = 1/2$ . We focus on rate  $k=1$  channel use per source symbol. Under these assumptions, the inner bound of Theorem 1 is maximized by choosing  $V=A$  and a uniformly distributed binary auxiliary random variable  $U$  (resp.  $Q$ ), produced as the output of a BSC with crossover probability  $u \in [0, 1/2]$  (resp.  $q \in [0, 1/2]$ ), and input  $A$  (resp.  $X$ ), as stated by the following proposition (which proof is omitted due to the lack of space).

*Proposition 3:* In the case considered in this section, region  $\mathcal{R}_{\text{in}}$  reduces to the set of all tuples  $(k=1, D=0, \Delta)$  such that there exist  $u, q \in [0, 1/2]$  satisfying

$$\beta(1 - h_2(u)) \leq 1 - h_2(q),$$

$$\Delta \leq h_2(\epsilon) + h_2(u) - h_2(\epsilon \star u) - \left[ \beta h_2(u) - \left( h_2(\zeta) + h_2(q) - h_2(\zeta \star q) \right) \right]_+,$$

where  $a \star b = a(1-b) + (1-a)b$  for each  $a, b \in [0, 1]$ .

Notice that if  $\beta \leq 4\epsilon(1-\epsilon)$  then  $B \succeq_A E$ , and hence Proposition 1 holds *i.e.*, the above inner bound is optimal.

#### Counterexample for the optimality of Theorem 1

Let now assume that Bob does not have any side information *i.e.*,  $\beta=1$ , and let  $\epsilon = \zeta = 0.1$  so that  $A \leftrightarrow E \leftrightarrow B$  form a Markov chain, and neither Proposition 1, nor Proposition 2 applies. This setting provides a counterexample for the general optimality of the inner bound in Theorem 1. Numerical optimization over  $u$  and  $q$  in Proposition 3 indicates that the proposed scheme achieves an equivocation rate  $\Delta = 0.056$ , while a naive analogue scheme

consisting of directly plugging the source on the channel achieves  $\Delta = 0.258$ . Furthermore, the latter coincides with the outer bound of Theorem 2.

The above example shows that a naive *joint* source-channel scheme may achieve better performance in some cases. At first look, this is not surprising since it is well-known that *joint* source-channel coding/decoding is a must for broadcast channels without secrecy constraints [20], [18]. However, the *secure* setting is rather different because Alice only wants to help one receiver (Bob), while she wants to blur the other one (Eve). Therefore, the intuition indicates that the optimal strategy would be the opposite *i.e.*, separation between source and channel encoders, as in Propositions 1 and 2.

## REFERENCES

- [1] C. Shannon, "Communication theory of secrecy systems," *BSTJ*, vol. 28, pp. 656–715, 1949.
- [2] D. Slepian and J. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471–480, 1973.
- [3] A. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. 22, no. 1, pp. 1–10, 1976.
- [4] V. Prabhakaran and K. Ramchandran, "On secure distributed source coding," in *Proc. ITW*, 2007, pp. 442–447.
- [5] D. Gunduz, E. Erkip, and H. Poor, "Secure lossless compression with side information," in *Proc. ITW*, 2008, pp. 169–173.
- [6] —, "Lossless compression with security constraints," in *Proc. ISIT*, 2008, pp. 111–115.
- [7] R. Tandon, S. Ulukus, and K. Ramchandran, "Secure source coding with a helper," in *Proc. Allerton*, 2009, pp. 1061–1068.
- [8] J. Villard and P. Piantanida, "Secure lossy source coding with side information at the decoders," in *Proc. Allerton*, 2010.
- [9] H. Yamamoto, "Coding theorems for Shannon's cipher system with correlated source outputs, and common information," *IEEE Trans. Inf. Theory*, vol. 40, no. 1, pp. 85–95, 1994.
- [10] —, "Rate-distortion theory for the Shannon cipher system," *IEEE Trans. Inf. Theory*, vol. 43, no. 3, pp. 827–835, 1997.
- [11] R. Liu and W. Trappe, *Securing wireless communications at the physical layer*. Springer, 2010.
- [12] N. Merhav, "On the Shannon cipher system with a capacity-limited key-distribution channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 1269–1273, 2006.
- [13] A. Wyner, "The wire-tap channel," *BSTJ*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [14] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.
- [15] N. Merhav, "Shannon's secrecy system with informed receivers and its application to systematic coding for wiretapped channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2723–2734, 2008.
- [16] "Special issue on information theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2405–2818, 2008.
- [17] Y. Liang, H. Poor, and S. Shamai, *Information theoretic security*. Now Publishers, 2009.
- [18] E. Tuncel, "Slepian-Wolf coding over broadcast channels," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1469–1482, 2006.
- [19] C. Nair, "Capacity regions of two new classes of 2-receiver broadcast channels," in *Proc. ISIT*, 2009, pp. 1839–1843.
- [20] M. Gastpar, B. Rimoldi, and M. Vetterli, "To code, or not to code: lossy source-channel communication revisited," *Information Theory, IEEE Transactions on*, vol. 49, no. 5, pp. 1147 – 1158, May 2003.