

Joint Source-Channel Secrecy Using Hybrid Coding

Eva C. Song Paul Cuff H. Vincent Poor
Dept. of Electrical Eng., Princeton University, NJ 08544
{csong, cuff, poor}@princeton.edu

Abstract—The secrecy performance of a source-channel model is studied in the context of lossy source compression over a noisy broadcast channel. The source is causally revealed to the eavesdropper during decoding. The fidelity of the transmission to the legitimate receiver and the secrecy performance at the eavesdropper are both measured by a distortion metric. Two achievability schemes using the technique of hybrid coding are analyzed and compared with an operationally separate source-channel coding scheme. A numerical example is provided and the comparison results show that the hybrid coding schemes outperform the operationally separate scheme.

Index Terms—hybrid coding, likelihood encoder, joint source-channel coding, secrecy, wiretap channel

I. INTRODUCTION

The secrecy properties of the wiretap channel have been studied under a variety of formulations. Shannon [1] considered the model of a noiseless wiretap channel where the transmitter and the legitimate receiver share a secret key. Other works [2] [3] consider the case of a noisy wiretap channel where the physical structure of the channel is exploited instead of using a secret key.

The most frequently adopted measure for information theoretic secrecy in the literature by far is equivocation, or normalized equivocation to be more precise. Wyner [2] introduced the notion of (normalized) equivocation for the study of secrecy capacity of a wiretap channel. This secrecy metric uses the conditional entropy of the source given what the eavesdropper observes $H(S|E)$, where E here can be a noisy channel output or an ciphered text protected by a secret key depending on the setup. When the source is a sequence, this quantity is typically normalized over the blocklength, $\frac{1}{n}H(S^n|E)$. Such a metric can be intuitively interpreted as the average statistical independence between the source and what the eavesdropper observes.

Inspired by [4], other works [5] [6] [7] [8] [9] have taken a rate-distortion approach to secrecy in communication systems. Instead of using equivocation, the secrecy is measured by the average distortion between the source and the eavesdropper's reconstruction of the source by allowing the eavesdropper to optimize its estimation. There the goal is to design an encoding and decoding scheme such that the source can be delivered reliably (lossless or lossy) to the legitimate receiver while a high distortion can be forced on the eavesdropper.

It may not have been straightforward to draw any connection between these two secrecy metrics until recent work [10] which has shown that equivocation is a special case of the distortion secrecy metric if the source sequence realization is causally disclosed to the eavesdropper during decoding.

Specifically, the distortion secrecy formulation with causal source disclosure fully recovers the equivocation secrecy formulation by choosing the distortion function to be a log-loss function.

In this work, we investigate the secrecy performance of a source-channel communication system composed of an independent and identically distributed (i.i.d.) source sequence and a noisy memoryless wiretap channel. By causally disclosing the source to the eavesdropper and using the distortion secrecy metric, it grants us the freedom of considering the general formulation of a secrecy problem, which can be particularized to the equivocation formulation if needed. A variation of this source-channel secrecy model was considered in [8] without causal source disclosure. Despite an important game-theoretic setting, such formulation does not render a strong enough secrecy criterion.

Previous work [11] considers the same source-channel model with causal source disclosure. However, only an operationally separate source-channel coding scheme was considered. Recent work on hybrid coding [12] and the likelihood encoder [13] [14] suggests a new way of approaching this problem.

II. PRELIMINARIES

A. Notation

A sequence X_1, \dots, X_n is denoted by X^n . Limits taken with respect to " $n \rightarrow \infty$ " are abbreviated as " \rightarrow_n ". Inequalities of the forms $\limsup_{n \rightarrow \infty} h_n \leq h$ and $\liminf_{n \rightarrow \infty} h_n \geq h$ are abbreviated as $h_n \leq_n h$ and $h_n \geq_n h$, respectively. When X denotes a random variable, x is used to denote a realization, and \mathcal{X} is used to denote the support of that random variable. A Markov relation is denoted by the symbol $-$. We use \mathbb{E}_P , \mathbb{P}_P , and $I_P(X; Y)$ to indicate expectation, probability, and mutual information taken with respect to a distribution P ; however, when the distribution is clear from the context, the subscript will be omitted. We use a bold capital letter \mathbf{P} to denote that a distribution P is random.

For a distortion measure $d : \mathcal{X} \times \mathcal{Y} \mapsto \mathbb{R}^+$, we use $\mathbb{E}[d(X, Y)]$ to measure the distortion of X incurred by reconstructing it as Y . The maximum distortion is defined as

$$d_{max} = \max_{(x, y) \in \mathcal{X} \times \mathcal{Y}} d(x, y).$$

The distortion between two sequences is defined to be the per-letter average distortion

$$d(x^n, y^n) = \frac{1}{n} \sum_{t=1}^n d(x_t, y_t).$$

B. Total Variation Distance

The total variation distance between two probability measures P and Q on the same σ -algebra \mathcal{F} of subsets of the sample space \mathcal{X} is defined as

$$\|P - Q\|_{TV} \triangleq \sup_{\mathcal{A} \in \mathcal{F}} |P(\mathcal{A}) - Q(\mathcal{A})|.$$

Some basic properties of total variation distance are given as Property 2 in [15].

C. Soft-covering Lemma

We now introduce the soft-covering lemma, which will be used in the achievability proof of the joint source-channel coding scheme.

Lemma 1. (Soft-covering, [16]) Given a joint distribution $\bar{P}_{U^k X^k Z^k}$, let $\mathcal{C}^{(n)}$ be a random codebook of sequences $U^n(m)$, with $m = 1, \dots, 2^{nR}$, each drawn independently and i.i.d. according to \bar{P}_U . Let

$$\mathbf{P}_{M X^n Z^k}(m, x^n, z^k)$$

$$\triangleq \frac{1}{2^{nR}} \prod_{t=1}^n \bar{P}_{X|U}(x_t | U_t(m)) \prod_{t=1}^k \bar{P}_{Z|XU}(z_t | x_t, U_t(m))$$

and

$$\bar{P}_{X^n Z^k} \triangleq \prod_{t=1}^n \bar{P}_X(x_t) \prod_{t=1}^k \bar{P}_{Z|X}(z_t | x_t). \quad (2)$$

If $R > I(X; U)$, then

$$\mathbb{E}_{\mathcal{C}^n} [\|\mathbf{P}_{X^n Z^k} - \bar{P}_{X^n Z^k}\|_{TV}] \leq \exp(-\gamma n) \rightarrow_n 0,$$

for any $\beta < \frac{R - I(X; U)}{I(Z; U|X)}$, $k \leq \beta n$, where $\gamma > 0$ depends on the gap $\frac{R - I(X; U)}{I(Z; U|X)} - \beta$.

III. PROBLEM SETUP AND PREVIOUS WORK

A. Problem Setup

Given a memoryless source and broadcast channel, we want to maximize the distortion forced on the eavesdropper (for estimating the source) while communicating the source reliably within a distortion constraint to the legitimate receiver. The input of the system is an i.i.d. source sequence S^n distributed according to $\prod_{t=1}^n \bar{P}_S(s_t)$ and the channel is a memoryless broadcast channel $\prod_{t=1}^n \bar{P}_{YZ|X}(y_t, z_t | x_t)$. The source realization is causally disclosed to the eavesdropper during decoding. The source-channel coding model satisfies the following constraints:

- Encoder $f_n : \mathcal{S}^n \mapsto \mathcal{X}^n$ (possibly stochastic);
- Legitimate receiver decoder $g_n : \mathcal{Y}^n \mapsto \hat{\mathcal{S}}^n$ (possibly stochastic);
- Eavesdropper decoders $\{P_{\hat{S}_t | Z^n, S^{t-1}}\}_{t=1}^n$.

The system performance is measured by a distortion metric $d(\cdot, \cdot)$ as follows:

- Average distortion for the legitimate receiver:

$$\mathbb{E} [d(S^n, \hat{S}^n)] \leq_n D_b$$

- Minimum average distortion for the eavesdropper:

$$\min_{\{P_{\hat{S}_t | Z^n, S^{t-1}}\}_{t=1}^n} \mathbb{E} [d(S^n, \check{S}^n)] \geq_n D_e$$

Definition 1. A distortion pair (D_b, D_e) is achievable if there exists a sequence of source-channel encoders and decoders (f_n, g_n) such that

$$\mathbb{E} [d(S^n, \hat{S}^n)] \leq_n D_b$$

and

$$\min_{\{P_{\hat{S}_t | Z^n, S^{t-1}}\}_{t=1}^n} \mathbb{E} [d(S^n, \check{S}^n)] \geq_n D_e.$$

The above mathematical formulation is illustrated in Fig. 1.

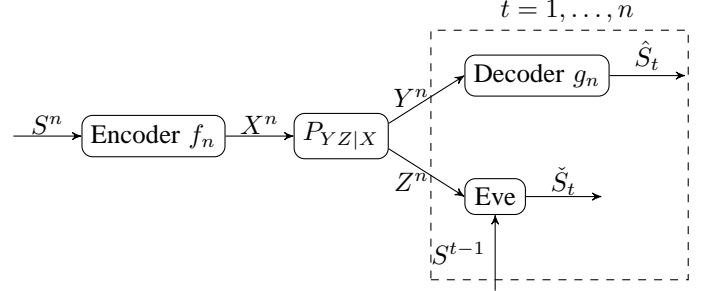


Fig. 1: Joint source-channel secrecy system setup with causal source disclosure at the eavesdropper

B. Previous Result

Before introducing the new joint source-channel coding schemes, we first review the achievability result from previous work [11] of the same problem formulation with an operationally separate source-channel coding scheme. Although the problem was only studied for the case of lossless reconstruction at the legitimate receiver in [11], the result can be readily generalized to the case of lossy compression as was formulated in Section III-A.

Theorem 1. (Generalized Theorem 2 of [11]) A distortion pair (D_b, D_e) is achievable if

$$I(S; U_1) < I(U_2; Y) \quad (3)$$

$$I(S; \hat{S} | U_1) < I(V_2; Y | U_2) - I(V_2; Z | U_2) \quad (4)$$

$$D_b \geq \mathbb{E} [d(S, \hat{S})] \quad (5)$$

$$D_e \leq \eta \min_{a \in \mathcal{S}} \mathbb{E} [d(S, a)] + (1 - \eta) \min_{t(u_1)} \mathbb{E} [d(S, t(U_1))] \quad (6)$$

for some distribution $\bar{P}_S \bar{P}_{\hat{S} | S} \bar{P}_{U_1 | \hat{S}} \bar{P}_{U_2} \bar{P}_{V_2 | U_2} \bar{P}_{X | V_2} \bar{P}_{Y Z | X}$, where

$$\eta = \frac{[I(U_2; Y) - I(U_2; Z)]^+}{I(S; U_1)}. \quad (7)$$

Since the source coding and channel coding parts of the above scheme are almost independent (with some technical details), we refer to it as the operationally separate source-channel coding scheme – Scheme O.

IV. MAIN RESULTS

This section is organized as follows. We first introduce the idea of secure hybrid coding. We then state the result of using basic hybrid coding (Scheme I) followed by its proof. We next state and briefly discuss the result using superposition hybrid coding (Scheme II). Finally, we analytically compare Scheme O, I and II, and give a trivial outer bound for completeness.

A. Secure Hybrid Coding

Hybrid coding is a joint source-channel coding technique [12] where 1) the encoder generates a digital codeword from the analog source and selects the channel input as a symbol-by-symbol function of the codeword and the source; and 2) the decoder recovers the digital codeword from the analog channel output and selects the source estimate as a symbol-by-symbol function of the codeword and the channel output. It has been shown that this joint source-channel code is at least optimal for point-to-point communication. For the purpose of achieving secrecy, the symbol-by-symbol mapping (deterministic) to the channel input in the encoding stage is modified to be stochastic.

B. Scheme 1 – Basic Hybrid Coding

An achievability region using basic secure hybrid coding is given in the following theorem.

Theorem 2. A distortion pair (D_b, D_e) is achievable if

$$I(U; S) < I(U; Y) \quad (8)$$

$$D_b \geq \mathbb{E}[d(S, \phi(U, Y))] \quad (9)$$

$$D_e \leq \beta \min_{\psi_0(z)} \mathbb{E}[d(S, \psi_0(Z))] + (1 - \beta) \min_{\psi_1(u, z)} \mathbb{E}[d(S, \psi_1(U, Z))] \quad (10)$$

where

$$\beta = \min \left\{ \frac{[I(U; Y) - I(U; Z)]^+}{I(S; U|Z)}, 1 \right\} \quad (11)$$

for some distribution $\bar{P}_S \bar{P}_{U|S} \bar{P}_{X|SU} \bar{P}_{YZ|X}$ and function $\phi(\cdot, \cdot)$.

The proof of Theorem 2 to be presented next uses hybrid coding combined with the likelihood encoder. The general idea is that under our choice of the encoder and decoder, the system induced distribution \mathbf{P} is close in total variation distance to an idealized distribution \mathbf{Q} by our construction. Therefore, by properties of total variation, we can approximate the performance of the system under \mathbf{P} by that under \mathbf{Q} .

C. Proof Outline of Scheme 1

The source and channel distributions \bar{P}_S and $\bar{P}_{YZ|X}$ are given by the problem statement. Fix a joint distribution $\bar{P}_S \bar{P}_{U|S} \bar{P}_{X|SU} \bar{P}_{YZ|X}$. We will use \bar{P}_{S^n} to denote $\prod_{t=1}^n \bar{P}_S$.

Codebook generation: We independently generate 2^{nR} sequences in \mathcal{U}^n according to $\prod_{t=1}^n \bar{P}_U(u_t)$ and index by $m \in [1 : 2^{nR}]$. We use $\mathcal{C}^{(n)}$ to denote this random codebook.

Encoder: Encoding has two steps. In the first step, a likelihood encoder $\mathbf{P}_{LE}(m|s^n)$ is used. It chooses M stochastically according to the following probability:

$$\mathbf{P}_{LE}(m|s^n) = \frac{\mathcal{L}(m|s^n)}{\sum_{\bar{m} \in \mathcal{M}} \mathcal{L}(\bar{m}|s^n)} \quad (12)$$

where $\mathcal{M} = [1 : 2^{nR}]$, and

$$\mathcal{L}(m|s^n) = \bar{P}_{S^n|U^n}(s^n|u^n(m)). \quad (13)$$

In the second step, the encoder produces the channel input through a random transformation given by $\prod_{t=1}^n \bar{P}_{X|SU}(x_t|s_t, U_t(m))$.

Decoder: Decoding also has two steps. In the first step, let $\mathbf{P}_{D1}(\hat{m}|y^n)$ be a good channel decoder with respect to the codebook $\{u^n(a)\}_a$ and memoryless channel $\bar{P}_{Y|U}$. In the second step, fix a function $\phi(\cdot, \cdot)$. Define $\phi^n(u^n, y^n)$ as the concatenation $\{\phi(u_t, y_t)\}_{t=1}^n$ and set the decoder \mathbf{P}_{D2} to be the deterministic function

$$\mathbf{P}_{D2}(\hat{s}^n|\hat{m}, y^n) \triangleq \mathbb{1}\{\hat{s}^n = \phi^n(u^n(\hat{m}), y^n)\}. \quad (14)$$

Analysis: We can write the system induced distribution in the following form:

$$\begin{aligned} & \mathbf{P}_{MU^n S^n X^n Y^n Z^n \hat{M} \hat{S}^n}(m, u^n, s^n, x^n, y^n, z^n, \hat{m}, \hat{s}^n) \\ & \triangleq \bar{P}_{S^n}(s^n) \mathbf{P}_{LE}(m|s^n) \mathbb{1}\{u^n = U^n(m)\} \\ & \prod_{t=1}^n \bar{P}_{X|SU}(x_t|s_t, u_t) \prod_{t=1}^n \bar{P}_{YZ|X}(y_t, z_t|x_t) \\ & \mathbf{P}_{D1}(\hat{m}|y^n) \mathbf{P}_{D2}(\hat{s}^n|\hat{m}, y^n). \end{aligned} \quad (15)$$

An idealized distribution \mathbf{Q} is defined as follows to help with the analysis:

$$\begin{aligned} & \mathbf{Q}_{MU^n S^n X^n Y^n Z^n}(m, u^n, s^n, x^n, y^n, z^n) \\ & \triangleq \frac{1}{2^{nR}} \mathbb{1}\{u^n = U^n(m)\} \prod_{t=1}^n \bar{P}_{S|U}(s_t|u_t) \\ & \prod_{t=1}^n \bar{P}_{X|SU}(x_t|s_t, u_t) \prod_{t=1}^n \bar{P}_{YZ|X}(y_t, z_t|x_t). \end{aligned} \quad (16)$$

1) *Distortion analysis at the legitimate receiver:* Applying Lemma 1 and properties of total variation distance, if

$$R > I(U; S), \quad (17)$$

then

$$\mathbb{E}_{\mathcal{C}^{(n)}} [\|\mathbf{P} - \mathbf{Q}\|_{TV}] \leq \exp(-\gamma_1 n) \triangleq \epsilon_{1n} \rightarrow_n 0, \quad (18)$$

where the distributions are over the random variables $MU^n S^n X^n Y^n Z^n$,

Using the same steps as was given in [14] for the analysis of the Wyner-Ziv setting, it can be verified that the following holds:

$$\begin{aligned} & \mathbb{E}_{\mathcal{C}^{(n)}} \left[\mathbb{E}_{\mathbf{P}} \left[d(S^n, \hat{S}^n) \right] \right] \\ & \leq \mathbb{E}_{\bar{P}}[d(S, \phi(U, Y))] + d_{max}(\epsilon_{1n} + \delta_n), \end{aligned} \quad (19)$$

if

$$R \leq I(U; Y), \quad (20)$$

where $\delta_n \rightarrow_n 0$.

2) *Distortion analysis at the eavesdropper:* On the eavesdropper side, we make the following observation. Define an auxiliary distribution

$$\check{\mathbf{Q}}_{S^i Z^n}^{(i)}(s^i, z^n) \triangleq \prod_{t=1}^n \bar{P}_Z(z_t) \prod_{j=1}^i \bar{P}_{S|Z}(s_j|z_j). \quad (21)$$

Under $\check{\mathbf{Q}}^{(i)}$,

$$S_i - Z_i - Z^n S^{i-1}. \quad (22)$$

Recall that

$$\begin{aligned} & \mathbf{Q}_{MZ^n S^i}(m, z^n, s^i) \\ &= \frac{1}{2^{nR}} \prod_{t=1}^n \bar{P}_{Z|U}(z_t | U_t(m)) \prod_{j=1}^i \bar{P}_{S|ZU}(s_j | z_j, U_j(m)) \end{aligned} \quad (23)$$

and under \mathbf{Q} , the following Markov relation holds:

$$S_i - Z_i U_i(M) - Z^n S^{i-1} M. \quad (24)$$

Applying Lemma 1, we have

$$\mathbb{E}_{\mathcal{C}^{(n)}} \left[\left\| \check{\mathbf{Q}}_{Z^n S^i}^{(i)} - \mathbf{Q}_{Z^n S^i} \right\|_{TV} \right] \leq \exp(-\gamma_2 n) \quad (25)$$

if

$$R > I(Z; U) \quad (26)$$

where i here can go up to βn , for any $\beta < \frac{R - I(U; Z)}{I(S; U|Z)}$. Consequently,

$$\mathbb{E}_{\mathcal{C}^{(n)}} \left[\left\| \check{\mathbf{Q}}_{Z^n S^i}^{(i)} - \mathbf{P}_{Z^n S^i} \right\|_{TV} \right] \leq \exp(-\gamma_1 n) + \exp(-\gamma_2 n). \quad (27)$$

Note that (26) is a degenerate statement if $R > I(Z; U)$.

Also note that since $R > 0$, we have

$$\mathbb{E}_{\mathcal{C}^{(n)}} \left[\left\| \mathbf{Q}_{u_i(M)} - \bar{P}_U \right\|_{TV} \right] \leq \exp(-\gamma_3 n). \quad (28)$$

Therefore, combining (18), (27), (28), and (19), there exists a codebook $\mathcal{C}^{(n)}$ such that

$$\sum_{i=1}^n \left\| P_{MZ^n S^i} - Q_{MZ^n S^i} \right\|_{TV} \leq \epsilon_n \quad (29)$$

$$\sum_{i=1}^n \left\| P_{Z^n S^i} - \check{Q}_{Z^n S^i}^{(i)} \right\|_{TV} \leq \epsilon_n \quad (30)$$

$$\sum_{i=1}^n \left\| Q_{u_i(M)} - \bar{P}_U \right\|_{TV} \leq \epsilon_n \quad (31)$$

$$\mathbb{E}_P \left[d(S^n, \hat{S}^n) \right] \leq \mathbb{E}_{\bar{P}} \left[d(S^n, \hat{S}^n) \right] + \epsilon_n \quad (32)$$

where $\epsilon_n = n(2\exp(-n\gamma_1) + \exp(-n\gamma_2) + \exp(-n\gamma_3)) + d_{max}(\epsilon_{1n} + \delta_n) \rightarrow_n 0$.

Now we can bound the distortion at the eavesdropper by breaking it down into two sections. The distortion after the time transition βn can be lower bounded by the following:

$$\begin{aligned} & \min_{\{\psi_{1_i}(s^{i-1}, z^n)\}} \mathbb{E}_P \left[\frac{1}{k} \sum_{i=j}^n d(S_i, \psi_{1_i}(S^{i-1}, Z^n)) \right] \\ &= \frac{1}{k} \sum_{i=j}^n \min_{\psi_{1_i}(s^{i-1}, z^n)} \mathbb{E}_P \left[d(S_i, \psi_{1_i}(S^{i-1}, Z^n)) \right] \end{aligned} \quad (33)$$

$$\geq \frac{1}{k} \sum_{i=j}^n \min_{\psi_{1_i}(s^{i-1}, z^n, m)} \mathbb{E}_P \left[d(S_i, \psi_{1_i}(S^{i-1}, Z^n, M)) \right] \quad (34)$$

$$\geq \frac{1}{k} \sum_{i=j}^n \min_{\psi_{1_i}(s^{i-1}, z^n, m)} \mathbb{E}_Q \left[d(S_i, \psi_{1_i}(S^{i-1}, Z^n, M)) \right] - \epsilon_n d_{max} \quad (35)$$

$$= \frac{1}{k} \sum_{i=j}^n \min_{\psi_{1_i}(u, z)} \mathbb{E}_Q \left[d(S_i, \psi_{1_i}(u_i(M), Z_i)) \right] - \epsilon_n d_{max} \quad (36)$$

$$\geq \frac{1}{k} \sum_{i=j}^n \min_{\psi_{1_i}(u, z)} \mathbb{E}_{\bar{P}} \left[d(S, \psi_{1_i}(U, Z)) \right] - 2\epsilon_n d_{max} \quad (37)$$

where $k = (1 - \beta)n$, $j = \beta n + 1$, (35) is from (29), (36) uses the Markov relation given in (24), and (37) uses (31) and the fact that

$$Q_{Z_i S_i | U_i}(z_i, s_i | u_i) = \bar{P}_{Z|U}(z_i | u_i) \bar{P}_{S|ZU}(s_i | z_i, u_i).$$

Similarly, by repeating the above process by replacing \mathbf{Q} with $\check{\mathbf{Q}}$ using (30), the Markov relation given in (22), and the definition of \mathbf{Q} given in (21), we can lower bound the distortion before time βn as

$$\begin{aligned} & \min_{\{\psi_{0_i}(s^{i-1}, z^n)\}_i} \mathbb{E}_P \left[\frac{1}{k} \sum_{i=1}^k d(S_i, \psi_{0_i}(S^{i-1}, Z^n)) \right] \\ & \geq \frac{1}{k} \sum_{i=1}^k \min_{\psi_{0_i}(z)} \mathbb{E}_{\bar{P}} \left[d(S, \psi_{0_i}(Z)) \right] - \epsilon_n d_{max}, \end{aligned} \quad (38)$$

where $k = \beta n$. Collecting (17), (20), and (32) and taking the average of the distortion at the eavesdropper over the entire blocklength n from (37) and (38) finishes the proof. \square

D. Scheme II – Superposition Hybrid Coding

An achievability region using superposition secure hybrid coding is given in the following theorem.

Theorem 3. A distortion pair (D_b, D_e) is achievable if

$$I(V; S) < I(UV; Y) \quad (39)$$

$$D_b \geq \mathbb{E} [d(S, \phi(V, Y))] \quad (40)$$

$$\begin{aligned} D_e & \leq \min\{\beta, \alpha\} \min_{\psi_0(z)} \mathbb{E} [d(S, \psi_0(Z))] \\ & \quad + (\alpha - \min\{\beta, \alpha\}) \min_{\psi_1(u, z)} \mathbb{E} [d(S, \psi_1(U, Z))] \\ & \quad + (1 - \alpha) \min_{\psi_2(v, z)} \mathbb{E} [d(S, \psi_2(V, Z))] \end{aligned} \quad (41)$$

where

$$\beta = \min \left\{ \frac{[I(U; Y) - I(U; Z)]^+}{I(S; U|Z)}, 1 \right\} \quad (42)$$

$$\alpha = \min \left\{ \frac{[r_s - I(Z; V|U)]^+}{I(S; V|ZU)}, 1 \right\} \quad (43)$$

$$r_s = \min\{I(V; Y|U), I(UV; Y) - I(S; U)\} \quad (44)$$

for some distribution $\bar{P}_S \bar{P}_{V|S} \bar{P}_{U|V} \bar{P}_{X|SUV} \bar{P}_{Y|ZX}$ and function $\phi(\cdot, \cdot)$.

The proof of Theorem 3 follows the same line as the proof of Theorem 2 with the modification of using a superposition codebook and the superposition version of the soft-covering lemma which was discussed in Corollary VII.8 of [16].

Under Scheme II, the distortion at the eavesdropper can potentially experience two transitions at βn and αn due to the superposition structure of the code.

E. Scheme Comparison

The relationships among Scheme O, I and II can be summarized in the following corollaries.

Corollary 1. Scheme II generalizes Scheme I.

To see this, notice that we can let $U = \emptyset$ in Theorem 3. In fact, Scheme II simplifies to Scheme I if $\beta \geq \alpha$.

Corollary 2. *Scheme O is a special case of Scheme II.*

This can be verified by using the following assignment of random variables from Theorem 1 to 3:

$$U \leftarrow U_1U_2 \text{ and } V \leftarrow \hat{S}V_2$$

to show that the inequalities (3) and (4) satisfy the inequality (39), $\beta = \eta$, and $\alpha = 1$. The equivalence of (5) and (6) to (40) and (41) can be obtained by using the statistical independence of $S\hat{S}U_1$ and U_2V_2YZ .

F. The Perfect Secrecy Outer Bound

Theorem 4. *If (D_b, D_e) is achievable, then*

$$I(S; U) \leq I(U; Y) \quad (45)$$

$$D_b \geq \mathbb{E}[d(S, \phi(U, Y))] \quad (46)$$

$$D_e \leq \min_{a \in \hat{S}} \mathbb{E}[d(S, a)] \quad (47)$$

for some distribution $\bar{P}_S \bar{P}_{U|S} \bar{P}_{X|SU} \bar{P}_{YZ|X}$ and function $\phi(\cdot, \cdot)$.

This trivial outer bound can be verified by using the optimality of hybrid coding for point-to-point communication and the fact that the estimation by the eavesdropper cannot be worse than the a-priori estimation of the source.

V. NUMERICAL EXAMPLE

We use the same example that was considered in [11]. The source is distributed i.i.d. according to $Bern(p)$ and the channels are binary symmetric channels with crossover probabilities $p_1 = 0$ and $p_2 = 0.3$. For simplicity, we require lossless decoding at the legitimate receiver. Hamming distance is considered for distortion at the eavesdropper.

A numerical comparison of Scheme I with Scheme O is demonstrated in Fig. 2. The choice of auxiliary random variable U in Scheme I is SX , which may not necessarily be the optimum choice but is good enough to outperform Scheme O. Scheme II is not numerically evaluated. However, because of Corollary 1 and 2, we know analytically that Scheme II is no worse than O or I.

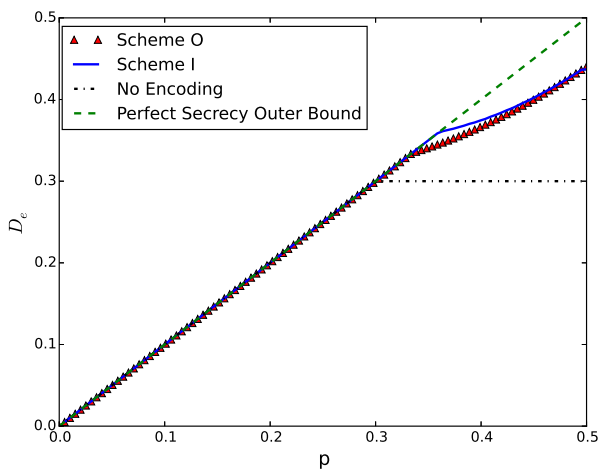


Fig. 2: Distortion at the eavesdropper as a function of source distribution p with $p_1 = 0$, $p_2 = 0.3$.

VI. CONCLUSION

This work has investigated secure joint source-channel coding under a general information-theoretic secrecy formulation. By using hybrid coding, we achieve better performance than a previously considered operationally separate source-channel coding scheme (O). Although a simple numerical example shows that a basic hybrid coding scheme (I) can potentially outperform Scheme O, we have only managed to prove analytically a superposition hybrid coding scheme (II) can fully generalize both Scheme O and I. The direct relation between Scheme O and I, and whether Scheme II is strictly better than I are still open for further investigation. Non-trivial outer bounds are yet to be explored.

VII. ACKNOWLEDGEMENT

This research was supported in part by the Air Force Office of Scientific Research under Grant FA9550-12-1-0196 and MURI Grant FA9550-09-05086, in part by the Army Research Office under MURI Grant W911NF-11-1-0036, and in part by the National Science Foundation under Grants CCF-1116013, CCF-1350595, CNS-09-05086 and ECCS-1343210.

REFERENCES

- [1] C. E. Shannon, "Communication theory of secrecy systems," *Bell system technical journal*, vol. 28, no. 4, pp. 656–715, 1949.
- [2] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, pp. 339–348, May 1978.
- [4] H. Yamamoto, "Rate-distortion theory for the Shannon cipher system," *IEEE Transactions on Information Theory*, vol. 43, pp. 827–835, 1997.
- [5] P. Cuff, "Using a secret key to foil an eavesdropper," in *Proc. 48th Annual Allerton Conference on Communication, Control, and Computing*, pp. 1405–1411, Sept 2010.
- [6] P. Cuff, "A framework for partial secrecy," in *Proc. IEEE Global Communications Conference (GLOBECOM)*, pp. 1–5, Dec 2010.
- [7] C. Schieler and P. Cuff, "Secrecy is cheap if the adversary must reconstruct," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, pp. 66–70, July 2012.
- [8] E. C. Song, E. Soljanin, P. Cuff, H. V. Poor, and K. Guan, "Rate-distortion-based physical layer secrecy with applications to multimode fiber," *IEEE Transactions on Communications*, vol. 62, pp. 1080–1090, March 2014.
- [9] E. C. Song, P. Cuff, and H. V. Poor, "A rate-distortion based secrecy system with side information at the decoders," in *Proc. 52th Annual Allerton Conference on Communication, Control, and Computing*, Oct 2014.
- [10] C. Schieler and P. Cuff, "Rate-distortion theory for secrecy systems," *IEEE Transactions on Information Theory*, vol. 60, pp. 7584–7605, Dec 2014.
- [11] C. Schieler, E. C. Song, P. Cuff, and H. V. Poor, "Source-channel secrecy with causal disclosure," in *Proc. 50th Annual Allerton Conference on Communication, Control, and Computing*, pp. 968–973, Oct 2012.
- [12] P. Minero, S. H. Lim, and Y.-H. Kim, "Hybrid coding: An interface for joint source-channel coding and network communication," *arXiv preprint arXiv:1306.0530*, 2013.
- [13] P. Cuff and E. C. Song, "The likelihood encoder for source coding," in *Proc. IEEE Information Theory Workshop (ITW)*, pp. 1–2, Sept 2013.
- [14] E. C. Song, P. Cuff, and H. V. Poor, "The likelihood encoder for lossy source compression," in *Proc. IEEE International Symposium on Information Theory (ISIT)*, Sept 2014.
- [15] C. Schieler and P. Cuff, "Rate-distortion theory for secrecy systems," *IEEE Transactions on Information Theory*, vol. 60, pp. 7584–7605, Dec 2014.
- [16] P. Cuff, "Distributed channel synthesis," *IEEE Transactions on Information Theory*, vol. 59, no. 11, pp. 7071–7096, 2013.