Secure Lossy Transmission of Vector Gaussian Sources

Ersen Ekrem Sennur Ulukus
Department of Electrical and Computer Engineering
University of Maryland, College Park, MD 20742
ersen@umd.edu *ulukus@umd.edu*

***Abstract*— We study the secure lossy transmission of a Gaussian vector source to a legitimate user in the presence of an eavesdropper, where both the legitimate user and the eavesdropper have Gaussian vector side information. The transmitter describes the source to the legitimate user in a way that the legitimate user can reconstruct the source within a certain distortion while the eavesdropper is kept ignorant of the source as much as possible. We obtain an outer bound for the rate, equivocation and distortion region of this secure lossy transmission problem. This outer bound is tight when the transmission rate constraint is removed. In other words, we obtain the maximum equivocation at the eavesdropper when the legitimate user needs to reconstruct the source within a fixed distortion level while there is no constraint on the transmission rate.**

I. Introduction

Information theoretic secrecy was initiated by Wyner in [1], where he studied the secure lossless transmission of a source over a degraded wiretap channel, and obtained the necessary and sufficient conditions. Later, his result was generalized to arbitrary, i.e., *not necessarily degraded*, wiretap channels in [2]. In recent years, information theoretic secrecy has gathered a renewed interest, where mostly channel coding aspects of secure transmission is considered.

Secure source coding problem is studied for both lossless and lossy reconstruction cases, where the former case can be viewed as a special case of the latter case. In this work, we consider the secure lossy source coding problem, which was studied in [3]–[9]. In these works, unlike the ones focusing on secure lossless source coding, the legitimate receiver does not want to reconstruct the source in a lossless fashion, but within a distortion level. The most relevant works to our work here are [8], [9]. In [8], the author considers the secure lossy transmission of a source over a degraded wiretap channel while both the legitimate receiver and the eavesdropper have side information about the source. In [8], in addition to the degradedness that the wiretap channel exhibits, the source and side informations also have a degradedness structure such that given the legitimate user's side information, the source and the eavesdropper's side information are independent. For this setting, in [8], a single-letter characterization of the distortion and equivocation region is provided. In particular, the optimality of a separation-based approach, i.e., the optimality of a code that concatenates a rate-distortion code and a wiretap channel code, is shown. In [9], the setting of [8] is partially generalized such that in [9], the source and side informations do not have any degradedness structure. On the other hand, as opposed to the *noisy* wiretap channel of [8], in [9], the channel between the transmitter and receivers is assumed to be *noiseless*. For this setting, in [9], a single-letter characterization of the rate, equivocation, and distortion region is provided.

Here, we consider the setting of [9] for the jointly Gaussian source and side informations. In particular, we consider the model where the transmitter has a Gaussian vector source which is jointly Gaussian with the Gaussian vector side informations of both the legitimate receiver and the eavesdropper. In this model, the transmitter wants to convey information to the legitimate user in a way that the legitimate user can reconstruct the source within a distortion level while the eavesdropper is being kept ignorant of the source as much as possible. A single-letter characterization of the rate, equivocation, and distortion region for this setting exists due to [9]. Although we are unable to evaluate this single-letter characterization for the Gaussian vector source and side informations case to obtain the corresponding rate, equivocation, distortion region explicitly, we obtain an outer bound for this region. We obtain this outer bound by optimizing the rate and equivocation constraints separately. We note that a joint optimization of the rate and equivocation constraints for a fixed distortion level would yield the exact achievable rate and equivocation region for this fixed distortion level. Thus, optimizing the rate and equivocation constraints separately yields a larger region, i.e., an outer bound. Moreover, we show that this outer bound is tight when we remove the transmission rate constraint. In other words, we obtain the maximum achievable equivocation at the eavesdropper when the legitimate user needs to reconstruct the Gaussian vector source within a fixed distortion while there is no constraint on the transmission rate.

II. Secure Lossy Source Coding

Here, we describe the secure lossy source coding problem and state the existing results. Let $\{(X_i, Y_i, Z_i)\}_{i=1}^n$ denote i.i.d. tuples drawn from a distribution $p(x, y, z)$. The transmitter, legitimate user and the eavesdropper observe $X^n \in \mathcal{X}^n, Y^n \in \mathcal{Y}^n$, and $Z^n \in \mathcal{Z}^n$, respectively. The transmitter wants to convey information to the legitimate user in a way that the legitimate user can reconstruct the source X^n within a certain distortion, and meanwhile the eavesdropper is kept

This work was supported by NSF Grants CCF 07-29127, CNS 09-64632, CCF 09-64645 and CCF 10-18185.

ignorant of the source X^n as much as possible. We note that in the absence of an eavesdropper, this setting reduces to the Wyner-Ziv problem [10].

We denote the legitimate user's reconstruction of the source X^n by $\hat{X}^n \in \hat{\mathcal{X}}^n$. The distortion of the reconstructed sequence $\hat{X}^n$ is measured by $d^n(X^n, \hat{X}^n)$ which has the following form

$$d^n(X^n, \hat{X}^n) = \frac{1}{n}\sum_{i=1}^{n} d(X_i, \hat{X}_i) \tag{1}$$

where $d(a,b)$ is a non-negative finite-valued function. The ignorance of the eavesdropper is measured by the equivocation $(1/n)H(X^n|Z^n, M)$, where $M \in \mathcal{M}$, is a function of the source X^n, denotes the signal sent by the transmitter.

An (n, R) code for secure lossy source coding consists of an encoding function $f_n : \mathcal{X}^n \to \mathcal{M} = \{1, \ldots, 2^{nR}\}$ at the transmitter and a decoding function at the legitimate user $g_n : \mathcal{M} \times \mathcal{Y}^n \to \hat{\mathcal{X}}^n$. A rate, equivocation and distortion tuple (R, R_e, D) is attainable if there exists an (n, R) code satisfying

$$\lim_{n\to\infty} \frac{1}{n} H(X^n|Z^n, M) \geq R_e \tag{2}$$

$$\lim_{n\to\infty} E[d(X^n, \hat{X}^n)] \leq D \tag{3}$$

where $M = f_n(X^n)$. The set of all achievable (R, R_e, D) tuples is denoted by $\mathcal{R}^*$ which is given as follows.

Theorem 1 ([9, Theorem 1]) $(R, R_e, D) \in \mathcal{R}^*$ *iff*

$$R \geq I(V; X|Y) \tag{4}$$

$$R_e \leq H(X|V, Y) + I(X; Y|U) - I(X; Z|U) \tag{5}$$

$$D \geq E[d(X, \hat{X}(V, Y))] \tag{6}$$

for some U, V satisfying the following Markov chain

$$U \to V \to X \to Y, Z \tag{7}$$

and a function $\hat{X}(V, Y)$.

Both the achievable scheme that attains the region $\mathcal{R}^*$ in Theorem 1 and the Wyner-Ziv scheme in [10] use binning to exploit the side information at the legitimate user, and hence, to reduce the rate requirement. The difference of the scheme that attains $\mathcal{R}^*$ comes from the extra binning necessitated by the presence of an eavesdropper. In particular, the transmitter generates sequences (U^n, V^n) and bins both U^n and V^n. The transmitter sends these two bin indices. Using the bin indices, the legitimate user identifies the right (U^n, V^n), and reconstructs X^n. However, using the bin indices of (U^n, V^n), the eavesdropper identifies only the right U^n. Hence, U does not contribute to the equivocation, see (5)[1].

We note that Theorem 1 holds for continuous (X^n, Y^n, Z^n) by replacing the discrete entropy term $H(X|V, Y)$ with the differential entropy term $h(X|V, Y)$. To avoid the negative equivocation that might arise because of the use of differential entropy, we replace equivocation with the mutual information leakage to the eavesdropper, where this leakage is measured by $\lim_{n\to\infty}(1/n)I(X^n; Z^n, M)$. In this alternative setting, a rate, mutual information leakage, and distortion (R, I_e, D) tuple is said to be achievable if there exists an (n, R) code such that

$$\lim_{n\to\infty} \frac{1}{n} I(X^n; Z^n, M) \leq I_e \tag{8}$$

$$\lim_{n\to\infty} E[d(X^n, \hat{X}^n)] \leq D \tag{9}$$

The set of all achievable (R, I_e, D) tuples is denoted by $\mathcal{R}$. Using Theorem 1, the region $\mathcal{R}$ can be stated as follows.

Theorem 2 ([9]) $(R, I_e, D) \in \mathcal{R}$ *iff*

$$R \geq I(V; X|Y) \tag{10}$$

$$I_e \geq I(V; X) - I(V; Y|U) + I(X; Z|U) \tag{11}$$

$$D \geq E[d(X, \hat{X}(V, Y))] \tag{12}$$

for some U, V satisfying the following Markov chain

$$U \to V \to X \to Y, Z \tag{13}$$

and a function $\hat{X}(V, Y)$.

III. Vector Gaussian Sources

Now we study the secure lossy source coding problem for jointly Gaussian $\{(\mathbf{X}_i, \mathbf{Y}_i, \mathbf{Z}_i)\}_{i=1}^n$ where the tuples $\{(\mathbf{X}_i, \mathbf{Y}_i, \mathbf{Z}_i)\}_{i=1}^n$ are independent across time, i.e., across the index i, and each tuple is drawn from the same jointly Gaussian distribution $p(\mathbf{X}, \mathbf{Y}, \mathbf{Z})$. In particular, we consider the case where $\mathbf{X}_i$ is a zero-mean Gaussian random vector with covariance matrix $\mathbf{K}_X \succ \mathbf{0}$, and the side information at the legitimate user $\mathbf{Y}_i$ and the eavesdropper $\mathbf{Z}_i$ are given by

$$\mathbf{Y}_i = \mathbf{X}_i + \mathbf{N}_{Y,i} \tag{14}$$

$$\mathbf{Z}_i = \mathbf{X}_i + \mathbf{N}_{Z,i} \tag{15}$$

where $\mathbf{N}_{Y,i}$ and $\mathbf{N}_{Z,i}$ are zero-mean Gaussian random vectors with covariance matrices $\mathbf{\Sigma}_Y \succ \mathbf{0}$ and $\mathbf{\Sigma}_Z \succ \mathbf{0}$, respectively. $(\mathbf{N}_{Y,i}, \mathbf{N}_{Z,i})$ is assumed to be independent of $\mathbf{X}_i$.

The distortion of the reconstructed sequence $\{\hat{\mathbf{X}}_i\}_{i=1}^n$ is measured by the mean square error matrix:

$$E\left[\left(\mathbf{X}_i - \hat{\mathbf{X}}_i\right)\left(\mathbf{X}_i - \hat{\mathbf{X}}_i\right)^\top\right] \tag{16}$$

Hence, distortion constraint is imposed by a positive definite matrix $\mathbf{D}$, which is achievable if there is an (n, R) code such that

$$\frac{1}{n}\sum_{i=1}^{n} E\left[\left(\mathbf{X}_i - \hat{\mathbf{X}}_i\right)\left(\mathbf{X}_i - \hat{\mathbf{X}}_i\right)^\top\right] \preceq \mathbf{D} \tag{17}$$

Throughout the paper, we assume that $\mathbf{0} \prec \mathbf{D} \preceq \mathbf{K}_{X|Y}$. Since the mean square error is minimized by setting the conditional mean as the estimator, we assume that the legitimate user applies this optimal estimator, i.e., $\{\hat{\mathbf{X}}_i\}_{i=1}^n$ are selected as

$$\hat{\mathbf{X}}_i = E\left[\mathbf{X}_i|\mathbf{Y}^n, f_n(\mathbf{X}^n)\right] \tag{18}$$

[1]The fact that the eavesdropper can decode U^n sequence can be obtained by observing that for a (U, V) selection, if $I(U; Y) \geq I(U; Z)$, there is no loss of optimality in setting $U = \phi$ which will yield a larger region.

Once the estimator of the legitimate user is set as (18), using Theorem 2, a single-letter description of the region $\mathcal{R}$ for a vector Gaussian source can be given as follows.

Theorem 3 $(R, I_e, \mathbf{D}) \in \mathcal{R}$ *iff*

$$R \geq I(V;\mathbf{X}|\mathbf{Y}) \tag{19}$$

$$I_e \geq I(V;\mathbf{X}) - I(V;\mathbf{Y}|U) + I(\mathbf{X};\mathbf{Z}|U) \tag{20}$$

$$\mathbf{D} \succeq \mathbf{K}_{X|VY} \tag{21}$$

for some U, V *satisfying the following Markov chain*

$$U \rightarrow V \rightarrow \mathbf{X} \rightarrow \mathbf{Y}, \mathbf{Z} \tag{22}$$

We also define the region $\mathcal{R}(\mathbf{D})$ as the union of the (R, I_e) pairs that are achievable when the distortion constraint matrix is set to $\mathbf{D}$. Our main result is an outer bound for the region $\mathcal{R}(\mathbf{D})$, hence for the region $\mathcal{R}$. Before presenting this result, we introduce the notation $\mathbf{K}_{A|B}$ which denotes the conditional covariance matrix of the random vector $\mathbf{A}$ conditioned on the random vector $\mathbf{B}$. Our main result is as follows.

Theorem 4 *When* $\mathbf{D} \preceq \mathbf{K}_{X|Y}$*, we have*

$$\mathcal{R}(\mathbf{D}) \subseteq \mathcal{R}^o(\mathbf{D}) \tag{23}$$

where $\mathcal{R}^o(\mathbf{D})$ *is given by the union of* (R, I_e) *that satisfy*

$$R \geq \frac{1}{2}\log\frac{|\mathbf{K}_{X|Y}|}{|\mathbf{D}|} = \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{F}(\mathbf{D})|} - \frac{1}{2}\log\frac{|\mathbf{K}_X + \mathbf{\Sigma}_Y|}{|\mathbf{F}(\mathbf{D}) + \mathbf{\Sigma}_Y|} \tag{24}$$

$$I_e \geq \min_{\substack{0 \preceq \mathbf{K}_1 \preceq \mathbf{K}_2 \preceq \mathbf{K}_X \\ \mathbf{K}_1 \preceq \mathbf{F}(\mathbf{D})}} \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{K}_1|} - \frac{1}{2}\log\frac{|\mathbf{K}_2 + \mathbf{\Sigma}_Y|}{|\mathbf{K}_1 + \mathbf{\Sigma}_Y|} + \frac{1}{2}\log\frac{|\mathbf{K}_2 + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{25}$$

and $\mathbf{F}(\mathbf{D}) = \mathbf{\Sigma}_Y(\mathbf{\Sigma}_Y - \mathbf{D})^{-1}\mathbf{\Sigma}_Y - \mathbf{\Sigma}_Y$.

The outer bound in Theorem 4 is obtained by minimizing the constraints on R and I_e individually, i.e., the rate lower bound in (24) is obtained by minimizing the rate constraint in (19) and the mutual information leakage lower bound in (25) is obtained by minimizing the mutual information leakage constraint in (20) separately. However, to characterize the rate and mutual information leakage region $\mathcal{R}(\mathbf{D})$, one needs to minimize the rate constraint in (19) and the mutual information leakage constraint in (20) jointly, not separately. In particular, since the region $\mathcal{R}(\mathbf{D})$ is convex in the pair (R, I_e) as per a time-sharing argument, joint optimization of the rate constraint in (19) and the mutual information leakage constraint in (20) can be carried out by considering the tangent lines to the region $\mathcal{R}(\mathbf{D})$, i.e., by solving the following optimization problem

$$L(\mu_1, \mu_2) = \min_{(R, I_e) \in \mathcal{R}(\mathbf{D})} \mu_1 R + \mu_2 I_e \tag{26}$$

$$= \min_{\substack{U \rightarrow V \rightarrow \mathbf{X} \rightarrow \mathbf{Y}, \mathbf{Z} \\ \mathbf{K}_{X|VY} \preceq \mathbf{D}}} \mu_1 \left[I(V;\mathbf{X}) - I(V;\mathbf{Y})\right] + \mu_2 \left[I(V;\mathbf{X}) - I(V;\mathbf{Y}|U) + I(\mathbf{X};\mathbf{Z}|U)\right] \tag{27}$$

for all values of μ_1, μ_2, where $\mu_j \in [0, \infty),\ j = 1, 2$. As of now, we could not solve the optimization problem $L(\mu_1, \mu_2)$ for all values of (μ_1, μ_2). However, as stated in Theorem 4, we solve the optimization problems $L(0, \mu_2)$ and $L(\mu_1, 0)$ by showing the optimality of jointly Gaussian $(U, V, \mathbf{X})$ to evaluate the corresponding cost functions. In other words, our outer bound in Theorem 4 can be written as follows.

$$R \geq L(1, 0) \tag{28}$$

$$I_e \geq L(0, 1) \tag{29}$$

We note that the constraint in (24), and hence $L(1, 0)$, gives us the Wyner-Ziv rate distortion function [10] for the vector Gaussian sources. Moreover, we note that $L(0, 1)$ gives us the the minimum mutual information leakage to the eavesdropper when the legitimate user wants to reconstruct the source within a fixed distortion constraint $\mathbf{D}$ while there is no concern on the transmission rate R. Denoting the minimum mutual information leakage to the eavesdropper when the legitimate user needs to reconstruct the source within a fixed distortion constraint $\mathbf{D}$ by $I_e^{\min}(\mathbf{D})$, $I_e^{\min}(\mathbf{D})$ is given as follows.

Theorem 5 *When* $\mathbf{D} \preceq \mathbf{K}_{X|Y}$*, we have*

$$I_e^{\min}(\mathbf{D}) = \min_{\substack{0 \preceq \mathbf{K}_1 \preceq \mathbf{K}_2 \preceq \mathbf{K}_X \\ \mathbf{K}_{X|V} \preceq \mathbf{F}(\mathbf{D})}} \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{K}_1|} - \frac{1}{2}\log\frac{|\mathbf{K}_2 + \mathbf{\Sigma}_Y|}{|\mathbf{K}_1 + \mathbf{\Sigma}_Y|} + \frac{1}{2}\log\frac{|\mathbf{K}_2 + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{30}$$

where $\mathbf{F}(\mathbf{D}) = \mathbf{\Sigma}_Y(\mathbf{\Sigma}_Y - \mathbf{D})^{-1}\mathbf{\Sigma}_Y - \mathbf{\Sigma}_Y$.

Theorem 5 implies that, if the transmitter's aim is to minimize the mutual information leakage to the eavesdropper without concerning itself with the rate it costs as long as the legitimate user is able to reconstruct the source within a distortion constraint $\mathbf{D}$, the use of jointly Gaussian $(U, V, \mathbf{X})$ is optimal.

IV. Proof of Theorem 4

We now provide the proof of Theorem 4. As mentioned in the previous section, this outer bound is obtained by minimizing the rate constraint in (19) and the mutual information leakage constraint in (20) separately. We first consider the rate constraint in (19) as follows

$$R \geq L(1, 0) = \min_{\substack{V \rightarrow \mathbf{X} \rightarrow \mathbf{Y}, \mathbf{Z} \\ \mathbf{K}_{X|VY} \preceq \mathbf{D}}} I(V;\mathbf{X}|\mathbf{Y}) = \frac{1}{2}\log\frac{|\mathbf{K}_{X|Y}|}{|\mathbf{D}|} \tag{31}$$

where the second equality of (31) is shown in [11]. Now we introduce the following lemma.

Lemma 1

$$\frac{1}{2}\log\frac{|\mathbf{K}_{X|Y}|}{|\mathbf{D}|} = \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{F}(\mathbf{D})|} - \frac{1}{2}\log\frac{|\mathbf{K}_X + \mathbf{\Sigma}_Y|}{|\mathbf{F}(\mathbf{D}) + \mathbf{\Sigma}_Y|} \tag{32}$$

The proof of Lemma 1 as well as the proofs of upcoming lemmas are omitted due to the space limitations. Lemma 1 and (31) imply (24).

Next, we consider the mutual information leakage constraint in (20) as follows.

$$I_e \geq L(0,1) \tag{33}$$

$$= \min_{\substack{U\to V\to \mathbf{X}\to \mathbf{Y},\mathbf{Z} \\ \mathbf{K}_{X|VY}\preceq \mathbf{D}}} I(V;\mathbf{X}) - I(V;\mathbf{Y}|U) + I(\mathbf{X};\mathbf{Z}|U) \tag{34}$$

We note that the cost function of $L(0,1)$ can be rewritten as follows.

$$C(L) = I(V;\mathbf{X}) - I(V;\mathbf{Y}) + I(U;\mathbf{Y}) + I(\mathbf{X};\mathbf{Z}|U) \tag{35}$$

$$= I(V;\mathbf{X}|\mathbf{Y}) + [I(U;\mathbf{Y}) + I(\mathbf{X};\mathbf{Z}|U)] \tag{36}$$

where (36) comes from the Markov chain $V \to \mathbf{X} \to \mathbf{Y}$. We note that the first term in (36) is minimized by a jointly Gaussian $(V,\mathbf{X})$ as we already showed in obtaining the lower bound for the rate. On the other hand, the remaining term of (36) in the bracket is maximized by a jointly Gaussian $(U,\mathbf{X})$ as it is shown in [12]. Thus, a tension between these two terms arises if $(U,V,\mathbf{X})$ is selected to be jointly Gaussian. In spite of this tension, we can still show that a jointly Gaussian $(U,V,\mathbf{X})$ is the minimizer of $L(0,1)$. Instead of directly showing this, we first characterize the minimum mutual information leakage when $(U,V,\mathbf{X})$ is restricted to be jointly Gaussian, and show that this cannot be attained by any other distribution of $(U,V,\mathbf{X})$. We note that any jointly Gaussian $(U,V,\mathbf{X})$ can be written as

$$V = \mathbf{A}_V\mathbf{X} + \mathbf{N}_V \tag{37}$$

$$U = \mathbf{A}_U\mathbf{X} + \mathbf{N}_U \tag{38}$$

where $\mathbf{N}_V, \mathbf{N}_U$ are zero-mean Gaussian random vectors with covariance matrices $\mathbf{\Sigma}_V, \mathbf{\Sigma}_U$, respectively. Moreover, $\mathbf{N}_V, \mathbf{N}_U$ are independent of each other, and also of $\mathbf{X}, \mathbf{Y}, \mathbf{Z}$. Before characterizing the minimum mutual information leakage when $(U,V,\mathbf{X})$ is restricted to be jointly Gaussian, we introduce the following lemma.

Lemma 2 *When $\mathbf{D} \preceq \mathbf{K}_{X|Y}$ and V is Gaussian, we have the following facts.*

- *$\mathbf{\Sigma}_Y - \mathbf{D} \succ \mathbf{0}$, i.e., $\mathbf{\Sigma}_Y - \mathbf{D}$ is positive definite, and hence, non-singular.*
- *Let $\mathbf{F}(\mathbf{D}) = \mathbf{\Sigma}_Y(\mathbf{\Sigma}_Y - \mathbf{D})^{-1}\mathbf{\Sigma}_Y - \mathbf{\Sigma}_Y$. Then, we have the following equivalence.*

$$\mathbf{K}_{X|VY} \preceq \mathbf{D} \quad \Leftrightarrow \quad \mathbf{K}_{X|V} \preceq \mathbf{F}(\mathbf{D}) \tag{39}$$

Using Lemma 2, the minimum mutual information leakage to the eavesdropper when $(U,V,\mathbf{X})$ is restricted to be jointly Gaussian can be written as follows.

$$L^G = \min_{\substack{U\to V\to \mathbf{X}\to \mathbf{Y},\mathbf{Z} \\ (U,V,\mathbf{X}) \text{ is jointly Gaussian} \\ \mathbf{K}_{X|V}\preceq \mathbf{F}(\mathbf{D})}} I(V;\mathbf{X}) - I(V;\mathbf{Y}|U) + I(\mathbf{X};\mathbf{Z}|U) \tag{40}$$

We note that the minimization in (40) can be written as a minimization of the cost function in (40) over all possible $\mathbf{A}_U, \mathbf{A}_V, \mathbf{\Sigma}_U, \mathbf{\Sigma}_V$ matrices by expressing $\mathbf{K}_{X|U}$ and $\mathbf{K}_{X|V}$ in terms of $\mathbf{A}_U, \mathbf{A}_V, \mathbf{\Sigma}_U, \mathbf{\Sigma}_V$. Instead of considering this tedious optimization problem, we consider the following one.

$$\bar{L}^G = \min_{\substack{0\preceq \mathbf{K}_{X|V}\preceq \mathbf{K}_{X|U}\preceq \mathbf{K}_X \\ \mathbf{K}_{X|V}\preceq \mathbf{F}(\mathbf{D})}} \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{K}_{X|V}|} - \frac{1}{2}\log\frac{|\mathbf{K}_{X|U}+\mathbf{\Sigma}_Y|}{|\mathbf{K}_{X|V}+\mathbf{\Sigma}_Y|} + \frac{1}{2}\log\frac{|\mathbf{K}_{X|U}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{41}$$

We note that due to the Markov chain $U \to V \to \mathbf{X}$, we always have $\mathbf{K}_{X|V} \preceq \mathbf{K}_{X|U}$. Besides that inequality, $\mathbf{K}_{X|V}$ and $\mathbf{K}_{X|U}$ have further interdependency which is not considered in the optimization problem given by (41). Since neglecting this further interdependency among $\mathbf{K}_{X|U}$ and $\mathbf{K}_{X|V}$ enlarges the feasible set of the optimization problem in (40), we have

$$L^G \geq \bar{L}^G \tag{42}$$

On the other hand, it can be shown that the value of $\bar{L}^G$ can be obtained by some jointly Gaussian $(U,V,\mathbf{X})$ satisfying the Markov chain $U \to V \to \mathbf{X}$, as stated in the following lemma.

Lemma 3

$$L^G = \bar{L}^G \tag{43}$$

Now we study the optimization problem $\bar{L}^G$ in more detail. Let $\mathbf{K}^*_{X|V}$ and $\mathbf{K}^*_{X|U}$ be the minimizers for the optimization problem $\bar{L}^G$. They need to satisfy the following KKT conditions.

Lemma 4 *If $\mathbf{K}^*_{X|V}$ and $\mathbf{K}^*_{X|U}$ are the minimizers for the optimization problem $\bar{L}^G$, they need to satisfy*

$$(\mathbf{K}^*_{X|V}+\mathbf{\Sigma}_Y)^{-1} + \mathbf{M}_U + \mathbf{M}_D = (\mathbf{K}^*_{X|V})^{-1} \tag{44}$$

$$(\mathbf{K}^*_{X|U}+\mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_X = (\mathbf{K}^*_{X|U}+\mathbf{\Sigma}_Y)^{-1} + \mathbf{M}_U \tag{45}$$

for some positive semi-definite matrices $\mathbf{M}_U, \mathbf{M}_D, \mathbf{M}_X$ which also need to satisfy

$$\mathbf{M}_U(\mathbf{K}^*_{X|U} - \mathbf{K}^*_{X|V}) = (\mathbf{K}^*_{X|U} - \mathbf{K}^*_{X|V})\mathbf{M}_U = \mathbf{0} \tag{46}$$

$$\mathbf{M}_D(\mathbf{F}(\mathbf{D}) - \mathbf{K}^*_{X|V}) = (\mathbf{F}(\mathbf{D}) - \mathbf{K}^*_{X|V})\mathbf{M}_D = \mathbf{0} \tag{47}$$

$$\mathbf{M}_X(\mathbf{K}_X - \mathbf{K}^*_{X|U}) = (\mathbf{K}_X - \mathbf{K}^*_{X|U})\mathbf{M}_X = \mathbf{0} \tag{48}$$

Next, we use channel enhancement [13]. In particular, we enhance, i.e., improve, the legitimate user's side information as follows.

$$(\mathbf{K}^*_{X|U}+\tilde{\mathbf{\Sigma}}_Y)^{-1} = (\mathbf{K}^*_{X|U}+\mathbf{\Sigma}_Y)^{-1} + \mathbf{M}_U \tag{49}$$

This new covariance matrix $\tilde{\mathbf{\Sigma}}_Y$ has some useful properties which are listed in the following lemma.

Lemma 5 *We have the following facts.*

- $\mathbf{0} \preceq \tilde{\mathbf{\Sigma}}_Y, \tilde{\mathbf{\Sigma}}_Y \preceq \mathbf{\Sigma}_Y, \tilde{\mathbf{\Sigma}}_Y \preceq \mathbf{\Sigma}_Z$
- $(\mathbf{K}^*_{X|V}+\tilde{\mathbf{\Sigma}}_Y)^{-1} = (\mathbf{K}^*_{X|V}+\mathbf{\Sigma}_Y)^{-1} + \mathbf{M}_U$

- $(\mathbf{K}^*_{X|U}+\tilde{\mathbf{\Sigma}}_Y)^{-1}(\mathbf{K}^*_{X|V}+\tilde{\mathbf{\Sigma}}_Y)$
$= (\mathbf{K}^*_{X|U}+\mathbf{\Sigma}_Y)^{-1}(\mathbf{K}^*_{X|V}+\mathbf{\Sigma}_Y)$
- $(\mathbf{K}^*_{X|U}+\tilde{\mathbf{\Sigma}}_Y)^{-1}(\mathbf{K}_X+\tilde{\mathbf{\Sigma}}_Y)$
$= (\mathbf{K}^*_{X|U}+\mathbf{\Sigma}_Z)^{-1}(\mathbf{K}_X+\mathbf{\Sigma}_Z)$
- $(\mathbf{K}^*_{X|V}+\tilde{\mathbf{\Sigma}}_Y)^{-1}(\mathbf{F}(\mathbf{D})+\tilde{\mathbf{\Sigma}}_Y) = (\mathbf{K}^*_{X|V})^{-1}\mathbf{F}(\mathbf{D})$

Next, using this new covariance matrix $\tilde{\mathbf{\Sigma}}_Y$, we define the *enhanced* side information $\tilde{\mathbf{Y}}$ as follows.

$$\tilde{\mathbf{Y}} = \mathbf{X} + \tilde{\mathbf{N}}_Y \tag{50}$$

where $\tilde{\mathbf{N}}_Y$ is a zero-mean Gaussian random vector with covariance matrix $\tilde{\mathbf{\Sigma}}_Y$. Since we have $\tilde{\mathbf{\Sigma}}_Y \preceq \mathbf{\Sigma}_Y$ and $\tilde{\mathbf{\Sigma}}_Y \preceq \mathbf{\Sigma}_Z$ as stated in the first statement of Lemma 5, without loss of generality, we can assume that the following Markov chain exists.

$$\mathbf{X} \to \tilde{\mathbf{Y}} \to \mathbf{Y}, \mathbf{Z} \tag{51}$$

Assuming that the Markov chain in (51) exists does not incur any loss of generality because the rate, mutual information leakage and distortion region $\mathcal{R}$ depends only on the conditional marginal distributions $p(\mathbf{Y}|\mathbf{X}), p(\mathbf{Z}|\mathbf{X})$ but not on the conditional joint distribution $p(\mathbf{Y}, \mathbf{Z}|\mathbf{X})$. Now, we define the following optimization problem

$$\bar{L} = \min_{\substack{U\to V\to\mathbf{X}\to\tilde{\mathbf{Y}}\to\mathbf{Y},\mathbf{Z} \\ \mathbf{K}_{X|VY}\preceq\mathbf{D}}} I(V;\mathbf{X}) - I(V;\tilde{\mathbf{Y}}|U) + I(\mathbf{X};\mathbf{Z}|U) \tag{52}$$

We note that we have $I(V;\mathbf{Y}|U) \le I(V;\tilde{\mathbf{Y}}|U)$ due to the Markov chain in (51), which leads to the following fact:

$$L^G = \bar{L}^G \ge L(0,1) \ge \bar{L} \tag{53}$$

Moreover, unlike the original optimization problem $L(0,1)$ in (34), we can find the minimizer of the new optimization problem $\bar{L}$ explicitly, as stated in the following lemma.

Lemma 6

$$\bar{L} = \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{F}(\mathbf{D})|} - \frac{1}{2}\log\frac{|\mathbf{K}_X+\tilde{\mathbf{\Sigma}}_Y|}{|\mathbf{F}(\mathbf{D})+\tilde{\mathbf{\Sigma}}_Y|} + \frac{1}{2}\frac{|\mathbf{K}_X+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{54}$$

We note that Lemma 6 implies that $U=\phi$ and a Gaussian V leading to $\mathbf{K}_{X|V} = \mathbf{F}(\mathbf{D})$ is the minimizer of the optimization problem $\bar{L}$.

Next, we show that indeed $L^G = \bar{L}^G = \bar{L}$ which, in view of (53), will imply $L(0,1) = \bar{L} = \bar{L}^G = L^G$. To this end, using Lemma 6, we have

$$\bar{L} = \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{F}(\mathbf{D})|} - \frac{1}{2}\log\frac{|\mathbf{K}_X+\tilde{\mathbf{\Sigma}}_Y|}{|\mathbf{F}(\mathbf{D})+\tilde{\mathbf{\Sigma}}_Y|} + \frac{1}{2}\frac{|\mathbf{K}_X+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{55}$$

$$= \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{K}^*_{X|V}|} - \frac{1}{2}\log\frac{|\mathbf{K}_X+\tilde{\mathbf{\Sigma}}_Y|}{|\mathbf{K}^*_{X|V}+\tilde{\mathbf{\Sigma}}_Y|} + \frac{1}{2}\frac{|\mathbf{K}_X+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{56}$$

$$= \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{K}^*_{X|V}|} - \frac{1}{2}\log\frac{|\mathbf{K}^*_{X|U}+\tilde{\mathbf{\Sigma}}_Y|}{|\mathbf{K}^*_{X|V}+\tilde{\mathbf{\Sigma}}_Y|} + \frac{1}{2}\frac{|\mathbf{K}^*_{X|U}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{57}$$

$$= \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{K}^*_{X|V}|} - \frac{1}{2}\log\frac{|\mathbf{K}^*_{X|U}+\mathbf{\Sigma}_Y|}{|\mathbf{K}^*_{X|V}+\mathbf{\Sigma}_Y|} + \frac{1}{2}\frac{|\mathbf{K}^*_{X|U}+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{58}$$

$$= \bar{L}^G \tag{59}$$

$$= L^G \tag{60}$$

where (56), (57) and (58) come from the fifth, fourth, and third statements of Lemma 5, respectively, (59) follows from the definition of $\bar{L}^G$ in (41), and (60) is due to Lemma 3. In view of (53), (60) implies that $L(0,1) = L^G$; completing the proof of Theorem 4 as well as the proof of Theorem 5 due to the fact that $I_e^{\min} = L(0,1)$.

V. Conclusions

In this paper, we study the secure lossy source coding problem for vector Gaussian source and side informations. For this problem, a single-letter description of the achievable rate, mutual information leakage, and distortion region exists [9]. We obtain an outer bound for this region by optimizing the corresponding rate and mutual information leakage constraints separately. Moreover, we obtain the minimum mutual information leakage to the eavesdropper when the legitimate user needs to reconstruct the source within a certain distortion while there is no constraint on the transmission rate.

References

[1] A. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, Jan. 1975.

[2] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, IT-24(3):339–348, May 1978.

[3] P. Cuff. A framework for partial secrecy. In *IEEE Globecom*, 2010.

[4] H. Yamamoto. A source coding problem for sources with additional outputs to keep secret from the receiver or wiretappers. *IEEE Trans. Inf. Theory*, 29(6):918–923, Nov. 1983.

[5] H. Yamamoto. A rate-distortion problem for a communication system with a secondary decoder to be hindered. *IEEE Trans. Inf. Theory*, 34(4):835–842, Jul. 1988.

[6] H. Yamamoto. Rate-distortion theory for the Shannon cipher system. *IEEE Trans. Inf. Theory*, 43(3):827–835, May 1997.

[7] N. Merhav. On the Shannon cipher system with a capacity-limited key-distribution channel. *IEEE Trans. Inf. Theory*, 52(3):1269–1273, Mar. 2006.

[8] N. Merhav. Shannon's secrecy system with informed receivers and its applications to systematic coding for wiretapped channels. *IEEE Trans. Inf. Theory*, 54(6):2723–2734, Jun. 2008.

[9] J. Villard and P. Piantanida. Secure lossy source coding with side information at the decoders. In *Allerton Conference on Commun., Contr. and Comput.*, Sep. 2010. Also available at [arXiv: 1009.3891].

[10] A. Wyner and J. Ziv. The rate-distortion function for source coding with side information at the decoder. *IEEE Trans. Inf. Theory*, 22(1):1–10, Jan. 1976.

[11] Md. S. Rahman and A. B. Wagner. Rate region of the Gaussian scalar-help-vector source-coding problem. Submitted to *IEEE Trans. Inf. Theory*. Also available at [arXiv:1001.4739].

[12] T. Liu and P. Viswanath. An extremal inequality motivated by multiterminal information theoretic problems. *IEEE Trans. Inf. Theory*, 53(5):1839–1851, May 2007.

[13] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz). The capacity region of the Gaussian multiple-input multiple-output broadcast channel. *IEEE Trans. Inf. Theory*, 52(9):3936–3964, Sep. 2006.