Secure Lossy Source Coding with Side Information

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 problem of secure lossy source coding with side information. In all works on this problem, either the equivocation of the source at the eavesdropper or the equivocation of the legitimate user's reconstruction of the source at the eavesdropper is used as the measure of secrecy. In this work, we propose a new secrecy measure, namely, the *relative equivocation* of the source at the eavesdropper with respect to the legitimate user. We argue that this new secrecy measure is the one that corresponds to the natural generalization of the equivocation in a wiretap channel to the context of secure lossy source coding, and discuss its advantages over the other two secrecy measures. Once we adopt the relative equivocation as the measure of secrecy, we provide a single-letter description of the rate, relative equivocation and distortion region. We specialize this single-letter description to the degraded and reversely degraded cases. Moreover, we investigate the relationships between the optimal scheme that attains this region and the Wyner-Ziv scheme.**

I. Introduction

Secure source coding problem has been studied for both lossless and lossy reconstruction cases in [1]–[16]. Secure *lossless* source coding problem is studied in [1]–[7]. These works, despite the differences in their models, share a common framework, in which the legitimate user wants to reconstruct the source in a lossless fashion by using the information it gets from the transmitter in conjunction with its own side information, while the eavesdropper is kept ignorant of the source as much as possible. Secure *lossy* source coding problem is studied in [8]–[16]. In these works, unlike the ones focusing on secure lossless source coding, the legitimate receiver wants to reconstruct the source in a lossy fashion, to within a distortion level.

Here, similar to [13]–[16], we also study the problem of secure lossy source coding with side information. In this problem, the transmitter wants to describe the source to the legitimate user within a distortion level, where the legitimate user has a side information. Meanwhile, this communication between the transmitter and the legitimate user needs to be kept secret from the eavesdropper, who also has a side information, to the extent possible. In [13]–[16], the security of this communication is measured by the equivocation of the source at the eavesdropper. Indeed, this measure of secrecy corresponds to a direct generalization of the one used for the wiretap channel in [17], [18], where secrecy is measured by the equivocation of the message at the eavesdropper. However, in a wiretap channel, the equivocation of the message at the eavesdropper measures not only the confusion of the eavesdropper about the message but also the *relative* confusion of the eavesdropper about the message with respect to the legitimate user. This comes from the fact that the legitimate user is able to decode the message, and hence the equivocation of the message at the legitimate user is asymptotically zero, making the relative equivocation and the equivocation asymptotically the same. On the other hand, in the context of secure *lossy* source coding, there is no such asymptotical equivalence between the equivocation of the source at the eavesdropper and the relative equivocation of the source at the eavesdropper with respect to the legitimate user. The lack of an asymptotical equivalence comes from the fact that the legitimate user does not reconstruct the source in a lossless fashion, but within a distortion, and hence, the legitimate user has an equivocation about the source sequence as well. Based on this observation, we argue that, indeed, the use of relative equivocation of the source as the secrecy measure provides the natural generalization of the equivocation in a wiretap channel to a secure *lossy* source coding context.

Before adopting the relative equivocation as the secrecy measure, we next discuss another possible secrecy measure which is the equivocation of the legitimate user's reconstruction of the source at the eavesdropper [19]. We argue that although the equivocation of the reconstructed source is useful to measure the confusion of the eavesdropper about the legitimate user's reconstruction, from a secrecy point of view, it provides inconsistent results. This inconsistency results from the fact that although the correlation between the side information of the legitimate user and the eavesdropper does not affect the quality of the legitimate user's reconstruction or the quality of the eavesdropper's reconstruction, it affects the equivocation of the legitimate user's reconstruction of the source at the eavesdropper. Hence, for two models differing only in the correlation between the side information of the legitimate user and the eavesdropper, the qualities of the legitimate user's and the eavesdropper's reconstructions in both models would be the same. Hence, the capability of the legitimate user and the capability of the eavesdropper to reproduce the source will be the same in both cases. Consequently, both models should have the same *amount* of secrecy. However, the equivocations of the legitimate user's reconstructions of the source at the eavesdropper in these two models might be different since they depend on the

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

correlation between the side information of the legitimate user and the eavesdropper. Thus, the equivocation of the legitimate user's reconstruction at the eavesdropper is an inconsistent measure of secrecy.

Once we adopt the relative equivocation as the secrecy measure, we obtain the single-letter description of the rate, relative equivocation and distortion region for the secure lossy source coding problem. To this end, we show that the coding scheme proposed in [14], where the same problem is studied when the equivocation of the source at the eavesdropper is used as the secrecy measure, attains the rate, relative equivocation and distortion region. This result implies that the coding scheme in [14] maximizes not only the equivocation of the source at the eavesdropper but also the relative equivocation of the source.

Next, we specialize the single-letter description we obtain to the degraded and reversely degraded cases. Although the single-letter description of the rate, relative equivocation and distortion region involves two auxiliary random variables, when it is specialized to either degraded or reversely degraded cases, a single auxiliary random variable is sufficient for the single-letter description. The latter fact implies that Wyner-Ziv scheme [20] is optimal for both degraded and reversely degraded cases, though it might not be optimal for the general case. In the final part of the paper, we address this issue, and provide a model for which two auxiliary random variables are needed; implying that Wyner-Ziv scheme is not optimal in general.

II. The Secrecy Measure

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 while keeping the source from the eavesdropper as secret as possible (see Figure 1). We note that if there was no eavesdropper, this setting would reduce to the Wyner-Ziv problem [20].

The distortion of the reconstructed sequence at the legitimate user is measured by the function $d^n(X^n, \hat{X}^n)$ where $\hat{X}^n \in \hat{\mathcal{X}}^n$ denotes the legitimate user's reconstruction of the source X^n. We consider functions $d^n(X^n, \hat{X}^n)$ that have 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.

In the previous works [13]–[16] on secure lossy source coding with side information, the objective was to maximize the uncertainty of the eavesdropper about the source X^n, and consequently, the equivocation of the source at the eavesdropper was chosen as the measure of secrecy:

$$\frac{1}{n} H(X^n | M, Z^n) \tag{2}$$

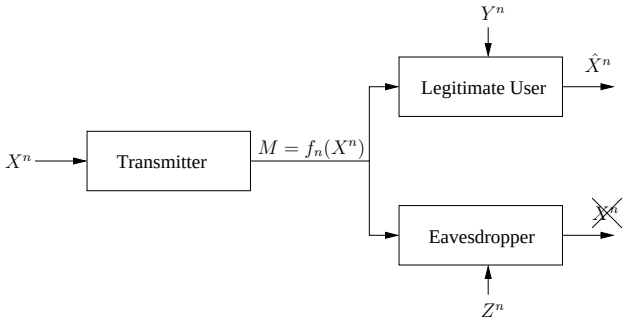

Fig. 1. Secure lossy source coding with side information.

where $M \in \mathcal{M}$, which is a function of the source X^n, denotes the signal sent by the transmitter. In this paper, we propose to use *relative equivocation* of the source at the eavesdropper with respect to the legitimate user

$$\frac{1}{n} \big[H(X^n | M, Z^n) - H(X^n | M, Y^n) \big] \tag{3}$$

To measure secrecy by using the equivocation of the source at the eavesdropper given by (2) is indeed inspired by the secure transmission of uniformly distributed messages over a wiretap channel (see Figure 2), where secrecy is measured by the equivocation of the message at the eavesdropper

$$\frac{1}{n} H(W | Z^n) \tag{4}$$

We note that in the wiretap channel, the legitimate user correctly decodes the message W, and hence due to Fano's lemma, we have $\lim_{n\to\infty} (1/n) H(W|Y^n) = 0$. Thus, the equivocation of the message at the eavesdropper for the wiretap channel given by (4) is equivalent to

$$\frac{1}{n} \left[H(W | Z^n) - H(W | Y^n) \right] \tag{5}$$

as $n \to \infty$. In other words, as $n \to \infty$, the equivocation of the message at the eavesdropper given by (4) is equivalent to the relative equivocation of the message at the eavesdropper with respect to the legitimate user given by (5).

In our case, since the legitimate user does not reconstruct the source in a lossless manner, the legitimate user will have some confusion about the source. In other words, as long as the distortion between the source and its reconstruction at the legitimate user is non-zero, the legitimate user will have a non-zero equivocation, i.e., we have $\lim_{n\to\infty} (1/n) H(X^n | M, Y^n) \neq 0$. Hence, as opposed to the wiretap channel, in our case, if we use the equivocation of the source at the eavesdropper given by (2) as the secrecy measure, we do not have an equivalence between (2) and the relative equivocation of the source at the eavesdropper with respect to the legitimate user given by (3). In other words, although in the wiretap channel, the equivocation at the eavesdropper tells us not only how much the eavesdropper is confused about the message but also the relative confusion of the eavesdropper with respect to the legitimate user, in the secure lossy source coding problem, the equivocation at

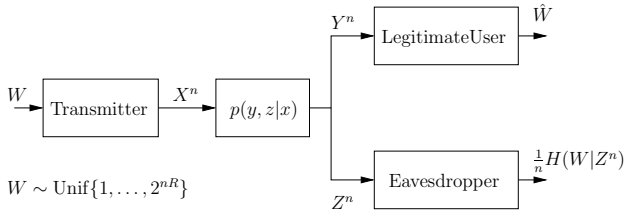

Fig. 2. Wiretap channel.

the eavesdropper tells us just how much the eavesdropper is confused about the source, but not the relative confusion of the eavesdropper with respect to the legitimate user.

Moreover, although the equivocation of the source at the eavesdropper given by (2) cannot indicate whether the eavesdropper has a better reconstruction of the source or not, *for some models of source and side information*, the relative equivocation of the source at the eavesdropper with respect to the legitimate user given by (3) would indicate whether the eavesdropper has a better reconstruction of the source than the legitimate user. The following example identifies some models of source and side information where this claim holds.

Example 1: In this example, we consider the degraded and reversely degraded models. For the degraded model, we have the following Markov chain

$$X_i \to Y_i \to Z_i, \quad i = 1, \ldots, n \tag{6}$$

and for the reversely degraded model, we have the following Markov chain

$$X_i \to Z_i \to Y_i, \quad i = 1, \ldots, n \tag{7}$$

We assume that in both models, both the legitimate user and the eavesdropper have the same reconstruction alphabet $\hat{\mathcal{X}}^n$ and use the same distortion metric $d^n(x^n, \hat{x}^n) = (1/n)\sum_{i=1}^n d(x_i, \hat{x}_i)$. We denote the minimum achievable distortion by the legitimate user and the eavesdropper by d_Y and d_Z, respectively. We have the following order between d_Y and d_Z for the models under consideration in this example.

Lemma 1: When both the legitimate user and the eavesdropper use the same reconstruction alphabet and the same distortion metric, the following orders hold.

- If $X_i \to Y_i \to Z_i,\ i = 1, \ldots, n$, we have $d_Y \leq d_Z$.
- If $X_i \to Z_i \to Y_i,\ i = 1, \ldots, n$, we have $d_Y \geq d_Z$.

The proof of Lemma 1 as well as the proofs of upcoming results are omitted due to space limitations here. Corresponding proofs can be found in [21].

Now, we consider the degraded model. For the degraded model, as Lemma 1 states, the minimum achievable distortion by the legitimate user is less than the minimum achievable distortion by the eavesdropper, i.e., $d_Y \leq d_Z$. Consequently, we expect that the eavesdropper is more confused about the source than the legitimate user, i.e., the relative equivocation of the source at the eavesdropper with respect to the legitimate user is positive. Indeed, this expectation is right as seen through

$$\begin{aligned} &H(X^n|M, Z^n) - H(X^n|M, Y^n) \\ &\quad = H(X^n|M, Z^n) - H(X^n|M, Y^n, Z^n) && (8) \\ &\quad = I(X^n; Y^n|M, Z^n) && (9) \\ &\quad \geq 0 && (10) \end{aligned}$$

where (8) is due to the Markov chain $M \to X^n \to Y^n \to Z^n$.

Similarly, for the reversely degraded model, as Lemma 1 states, the minimum achievable distortion by the eavesdropper is less than the minimum achievable distortion by the legitimate user, i.e., $d_Z \leq d_Y$, and consequently, the legitimate user is more confused about the source than the legitimate user, i.e., the relative equivocation at the eavesdropper with respect to the legitimate user is negative:

$$\begin{aligned} &H(X^n|M, Z^n) - H(X^n|M, Y^n) \\ &\quad = H(X^n|M, Z^n, Y^n) - H(X^n|M, Y^n) && (11) \\ &\quad = -I(X^n; Z^n|M, Y^n) && (12) \\ &\quad \leq 0 && (13) \end{aligned}$$

where (11) is due to the Markov chain $M \to X^n \to Z^n \to Y^n$.

We note that although this example shows that *for some models of source and side information*, the relative equivocation of the source at the eavesdropper with respect to the legitimate user given by (3) indicates whether the eavesdropper will have a better reconstruction of the source than the legitimate user, we do not expect it to hold for all source and side information models. For example, if there is a model with vector source and side information, and the model is neither degraded nor reversely degraded, then using the relative equivocation, we might not understand whether the legitimate user or the eavesdropper is able to reconstruct a specific component of the source in a better way. Indeed, to understand the relative qualities of the reconstructions of the source at the legitimate user and the eavesdropper, the most appropriate secrecy metric to use is the minimum attainable distortion of the eavesdropper's reconstruction of the source. However, this formulation does not seem to be tractable for now, especially, if one considers the fact that even for the degraded case, this problem is still open [11].

Before adopting the relative equivocation given by (3) as the secrecy metric to formulate the problem of secure lossy source coding with side information, we discuss another possible secrecy metric [19] which considers the equivocation of the reconstructed sequence at the eavesdropper:

$$\frac{1}{n} H(\hat{X}^n|M, Z^n) \tag{14}$$

Although this secrecy measure is useful in the sense that it can tell us how much information the eavesdropper has about the legitimate user's reconstruction, and hence to what extent, the eavesdropper can reproduce the legitimate user's reconstruction, this secrecy measure also has some shortcomings. First, we note that although the equivocation

of the reconstructed source at the eavesdropper measures the capability of the eavesdropper to reproduce the legitimate user's reconstruction, it does not measure the capability of the eavesdropper to reproduce the source itself. Hence, the use of the equivocation of the legitimate user's reconstruction as the measure of secrecy might be misleading, because the equivocation of the reconstructed source might have a non-zero value indicating that the eavesdropper cannot duplicate the legitimate user's reconstruction, while the eavesdropper has a better reconstruction of the source than the legitimate user. The following example demonstrates this observation.

Example 2: In this example, we consider the reversely degraded model introduced in Example 1. In the reversely degraded model, the eavesdropper has a better side information than the legitimate user, and consequently, is less confused than the legitimate user. Moreover, as Lemma 1 states, for the reversely degraded model, we have $d_Z \leq d_Y$, i.e., the eavesdropper has a better reconstruction of the source than the legitimate user. On the other hand, due to the non-negativity of the entropy, we have $H(\hat{X}^n|M,Z^n) \geq 0$ indicating that the eavesdropper might not be able to reproduce the legitimate user's reconstruction of the source. This results from the fact that the reconstructed sequence $\hat{X}^n$ depends on Y^n, where this dependence cannot be resolved by conditioning on Z^n. Hence, the use of equivocation of legitimate user's reconstruction might be misleading.

Another point about the equivocation of the reconstructed sequence at the eavesdropper given by (14) is that it depends on the entire joint distribution of the source X^n and side information Y^n and Z^n, i.e., $p(x^n,y^n,z^n)$. It is well-known that the minimum achievable distortions by the legitimate user and the eavesdropper, i.e., d_Y and d_Z, depend only on the distributions $p(x^n,y^n)$ and $p(x^n,z^n)$, respectively, but not on the joint distribution $p(x^n,y^n,z^n)$. Hence, by using the equivocation of the reconstructed sequence at the eavesdropper given by (14), we might get different equivocations for models that have identical distortion pairs (d_Y,d_Z). In particular, consider two models with joint distributions $p_1(x^n,y^n,z^n)$ and $p_2(x^n,y^n,z^n)$, for which although the joint distributions $p_1(x^n,y^n,z^n)$ and $p_2(x^n,y^n,z^n)$ are not identical, we have $p_1(x^n,y^n) = p_2(x^n,y^n)$ and $p_1(x^n,z^n) = p_2(x^n,z^n)$. Let d_Y^i be the minimum achievable distortion by the legitimate user in the model described by $p_i(x^n,y^n,z^n)$, and similarly, let d_Z^i be the minimum achievable distortion by the eavesdropper in the model described by $p_i(x^n,y^n,z^n)$. Due to the equalities $p_1(x^n,y^n) = p_2(x^n,y^n)$ and $p_1(x^n,z^n) = p_2(x^n,z^n)$, we have $d_Y^1 = d_Y^2$ and $d_Z^1 = d_Z^2$. On the other hand, in general, we have $H_1(\hat{X}^n|M,Z^n) \neq H_2(\hat{X}^n|M,Z^n)$[1] because the equivocation of the reconstructed sequence at the eavesdropper given by (14) depends on the joint distribution, and the joint distributions for these models are not identical, i.e., $p_1(x^n,y^n,z^n) \neq p_2(x^n,y^n,z^n)$. Hence, the equivocation of the reconstructed sequence at the eavesdropper might be regarded as an inconsistent measure of secrecy because although the relative qualities of the reconstructions of the legitimate user and the eavesdropper do not change from one model to the other, the equivocation of the reconstructed sequence at the eavesdropper might change.

[1] $H_i(\hat{X}^n|M,Z^n)$ denotes the conditional entropy term that is computed according to the distribution $p_i(m,x^n,y^n,z^n,\hat{x}^n)$.

III. Single-Letter Characterization

Now, we formulate the secure lossy source coding problem when the relative equivocation of the source at the eavesdropper with respect to the legitimate user given by (3) is used as the merit of secrecy. An (n,R) code for secure lossy source coding consists of an encoding function $f_n : \mathcal{X}^n \to \mathcal{M} = \{1,\dots,2^{nR}\}$ 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, relative equivocation and distortion tuple (R,Δ,D) is achievable if there exists an (n,R) code satisfying

$$\lim_{n\to\infty}\frac{1}{n}\big[H(X^n|M,Z^n) - H(X^n|M,Y^n)\big] \geq \Delta \qquad (15)$$

$$\lim_{n\to\infty} E[d^n(X^n,\hat{X}^n)] \leq D \qquad (16)$$

where $M = f_n(X^n) \in \mathcal{M}$. The set of all achievable (R,Δ,D) tuples is denoted by $\mathcal{R}^*$. We obtain a single-letter characterization of the region $\mathcal{R}^*$ as stated in the following theorem.

Theorem 1: $(R,\Delta,D) \in \mathcal{R}^*$ iff

$$R \geq I(V;X) - I(V;Y) \qquad (17)$$

$$\Delta \leq I(X;Y|U) - I(X;Z|U) \qquad (18)$$

$$D \geq E[d(X,\hat{X}(V,Y))] \qquad (19)$$

for some U,V satisfying the following Markov chain

$$U \to V \to X \to Y,Z \qquad (20)$$

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

We show the achievability of the region $\mathcal{R}^*$ by using the coding scheme proposed in [14], where the problem of secure lossy source coding with side information was studied when the secrecy of the source is measured by its equivocation at the eavesdropper given in (2). We note that the two problems, the one that we consider by using the relative equivocation of the source at the eavesdropper with respect to the legitimate user given by (3) as the secrecy measure and the other one studied in [14] that uses the equivocation of the source at the eavesdropper given by (2) as the secrecy measure, are not identical, and hence, having the optimum coding scheme for the latter problem does not imply that it will be an optimum solution for our problem that uses the relative equivocation given by (3) as the secrecy measure. Since here we show that the coding scheme in [14] can also achieve the region $\mathcal{R}^*$, our result implies that maximizing the equivocation at the eavesdropper given by (2) is equivalent to maximizing the difference between the equivocations of the legitimate user and the eavesdropper given by (3).

The coding scheme achieving the region $\mathcal{R}^*$ is similar to the Wyner-Ziv scheme [20] in the sense that both schemes, by means of binning, make use of the side information at the legitimate user to reduce the transmission rate. The difference

between these two schemes is that although the Wyner-Ziv scheme uses a single-binning, the coding scheme achieving the region $\mathcal{R}^*$ uses a double-binning, where the additional binning is necessary due to the secrecy consideration in our problem. In particular, in our problem, the transmitter generates sequences (U^n, V^n) and bins both sequences. The bin indices of these two sequences are delivered to the legitimate user. Using these bin indices, the legitimate user identifies the right (U^n, V^n) sequences, and reconstructs X^n within the required distortion. On the other hand, using the bin indices of (U^n, V^n), the eavesdropper identifies only the right U^n sequence, and consequently, U does not contribute to the equivocation, see (18)[2].

IV. Degraded and Reversely Degraded Cases

We now consider the degraded and reversely degraded cases. In the degraded case, the source and side information satisfy the Markov chain in (6) and in the reversely degraded case, they satisfy the Markov chain in (7).

For the degraded case, Theorem 1 can be specialized into the following form.

Corollary 1: In the degraded case, $(R, \Delta, D) \in \mathcal{R}^*$ iff

$$R \geq I(V;X) - I(V;Y) \tag{21}$$

$$\Delta \leq I(X;Y) - I(X;Z) \tag{22}$$

$$D \geq E[d(X, \hat{X}(V,Y))] \tag{23}$$

for some V satisfying the following Markov chain $V \rightarrow X \rightarrow Y \rightarrow Z$ and a function $\hat{X}(V,Y)$.

This corollary can be obtained from Theorem 1 by noting the fact that $I(X;Y|U) - I(X;Z|U) \leq I(X;Y) - I(X;Z)$ in view of the Markov chain in (6), where the equality can be attained by setting $U = \phi$. Corollary 1 implies that in the degraded case, the relative equivocation is not affected by the choice of V, and hence, there is no tension between the achievable rate and the achievable relative equivocation originating from the choice of V. This also implies that the use of optimal compression rate for the given distortion level is optimal. In other words, the use of Wyner-Ziv coding [20] is optimal, and the region $\mathcal{R}^*$ for a fixed distortion D can be expressed as the union of rate and relative equivocation pairs (R, Δ)

$$R \geq R_{WZ}(D) \tag{24}$$

$$\Delta \leq I(X;Y) - I(X;Z) \tag{25}$$

where $R_{WZ}(D)$ is the Wyner-Ziv rate distortion function given by

$$R_{WZ}(D) = \min_{\substack{V \rightarrow X \rightarrow Y \\ E\left[d(X,\hat{X}(V,Y))\right] \leq D}} I(V;X) - I(V;Y) \tag{26}$$

The following example obtains the rate and relative equivocation region for the degraded scalar Gaussian model.

Example 3: In this example, we consider the degraded scalar Gaussian model. In this model, there is an i.i.d. Gaussian source $\{X_i\}_{i=1}^n$ with zero-mean and variance σ_X^2. The side information are given by

$$Y_i = X_i + N_{Y,i} \tag{27}$$

$$Z_i = X_i + N_{Z,i} \tag{28}$$

where $\{N_{Y,i}\}_{i=1}^n$ and $\{N_{Z,i}\}_{i=1}^n$ are i.i.d. Gaussian random variables with zero-mean and variance σ_Y^2 and σ_Z^2, respectively. X_i and $(N_{Y,i}, N_{Z,i})$ are independent for each i. We assume that $\sigma_Y^2 < \sigma_Z^2$. Thus, without loss of generality, we can assume that the Markov chain

$$X_i \rightarrow Y_i \rightarrow Z_i \tag{29}$$

holds, since the correlation between $N_{Y,i}$ and $N_{Z,i}$ does not change the rate, relative equivocation and distortion region. Hence, in view of the Markov chain in (29), the rate, relative equivocation and distortion region of this model follows from Corollary 1.

Before evaluating the region in Corollary 1 for the degraded scalar Gaussian model, we specify the distortion metric. For this model, the distortion of the reconstructed sequence is measured by its mean square error, i.e., $d(x, \hat{x}) = (x - \hat{x})^2$. Since the mean square error is minimized by the conditional mean, the legitimate user selects its reconstruction function as

$$\hat{X}_i = E\left[X_i | Y^n, f_n(X^n)\right] \tag{30}$$

which implies that the distortion constraint in Corollary 1 can be expressed as

$$\sigma_{X|VY}^2 \leq D \tag{31}$$

Hence, we can obtain the rate and relative equivocation region of the degraded scalar Gaussian model by evaluating the region defined by (21)-(22) and (31), which results in the region stated in the following corollary.

Corollary 2: In the degraded scalar Gaussian model, $(R, \Delta) \in \mathcal{R}^*(D)$ iff

$$R \geq R_{\mathrm{WZ}}(D) = \frac{1}{2} \log \frac{\sigma_X^2 \sigma_Y^2}{D(\sigma_X^2 + \sigma_Y^2)} \tag{32}$$

$$\Delta \leq \frac{1}{2} \log \frac{\sigma_X^2 + \sigma_Y^2}{\sigma_Y^2} - \frac{1}{2} \log \frac{\sigma_X^2 + \sigma_Z^2}{\sigma_Z^2} \tag{33}$$

We note that in Corollary 2, the relative equivocation is constant, i.e., does not interact with the rate. This also implies that we can always transmit at the Wyner-Ziv rate.

Next, we specialize Theorem 1 for the reversely degraded model as follows.

Corollary 3: In the reversely degraded case, $(R, \Delta, D) \in \mathcal{R}^*$ iff

$$R \geq I(V;X) - I(V;Y) \tag{34}$$

$$\Delta \leq I(X;Y|V) - I(X;Z|V) \tag{35}$$

$$D \geq E[d(X, \hat{X}(V,Y))] \tag{36}$$

for some V satisfying the following Markov chain $V \rightarrow X \rightarrow Z \rightarrow Y$ and a function $\hat{X}(V,Y)$.

This corollary can be obtained from Theorem 1 by noting the fact that $I(X;Y|U) - I(X;Z|U) \leq I(X;Y|V) -$

[2]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 of setting $U = \phi$ which will yield a larger region.

$I(X;Z|V)$ in view of the Markov chain in (7), where the equality can be attained by setting $U = V$. Corollary 3 implies that unlike the degraded case, in the reversely degraded case, there might be a tension between the achievable rate and the achievable relative equivocation originating from the choice of V, since both the achievable rate and the achievable relative equivocation depend on the choice of V. However, similar to the degraded case, in the reversely degraded case also, we need only one auxiliary random variable to attain the rate, relative equivocation and distortion region $\mathcal{R}^*$. Thus, similar to the degraded case, in the reversely degraded case also, Wyner-Ziv coding [20] is sufficient to attain the entire region $\mathcal{R}^*$. The difference between the degraded and the reversely degraded cases is that in the degraded case, we can always transmit at the minimum rate determined by the Wyner-Ziv rate distortion function in (24), however, in the reversely degraded case, we might need to transmit at higher rates to obtain a higher relative equivocation, since in this case, both the achievable rate and the achievable relative equivocation depend on the choice of the auxiliary random variable V. In other words, the choice of V that minimizes the rate, i.e., the minimizer for the optimization problem in (24), might not be the maximizer of the relative equivocation term in (35). The following example demonstrates this point.

Example 4: In this example, we consider the reversely degraded scalar Gaussian model which is identical to the degraded scalar Gaussian model in Example 3 with the only exception that here, we have $\sigma_Z^2 < \sigma_Y^2$. Thus, without loss of generality, we can assume that the Markov chain

$$X_i \to Z_i \to Y_i \tag{37}$$

holds, since the correlation between $N_{Y,i}$ and $N_{Z,i}$ does not change the rate, relative equivocation and distortion region. Hence, in view of the Markov chain in (37), the rate, relative equivocation and distortion region of this model follows from Corollary 3.

Before evaluating the region in Corollary 3, we specify the distortion metric. Similar to Example 3, here also, we use the mean square error as the distortion metric, i.e., $d(x,\hat{x}) = (x-\hat{x})^2$. Hence, the optimal reconstruction function for the legitimate user is given by the conditional mean in (30), which implies that the distortion constraint in Corollary 3 can be expressed as

$$\sigma_{X|VY}^2 \leq D \tag{38}$$

Hence, we can obtain the rate, relative equivocation and distortion region of the reversely degraded scalar Gaussian model by evaluating the region defined by (34)-(35) and (38), which results in the region stated in the following corollary.

Corollary 4: In the reversely degraded scalar Gaussian model, $(R,\Delta) \in \mathcal{R}^*(D)$ iff

$$R \geq \frac{1}{2}\log\frac{\sigma_X^2}{\sigma_{X|V}^2} - \frac{1}{2}\log\frac{\sigma_X^2+\sigma_Y^2}{\sigma_{X|V}^2+\sigma_Y^2} \tag{39}$$

$$\Delta \leq \frac{1}{2}\log\frac{\sigma_{X|V}^2+\sigma_Y^2}{\sigma_Y^2} - \frac{1}{2}\log\frac{\sigma_{X|V}^2+\sigma_Z^2}{\sigma_Z^2} \tag{40}$$

for some $\sigma_{X|V}^2$ satisfying

$$\sigma_{X|V}^2 \leq \frac{\sigma_Y^2 D}{\sigma_Y^2 - D} \tag{41}$$

We note that both rate and relative equivocation constraints in (39) and (40), respectively, are monotonically decreasing in $\sigma_{X|V}^2$. Hence, there is a tension between the rate and the relative equivocation, i.e., there is a trade-off between the achievable rate and the relative equivocation controlled by $\sigma_{X|V}^2$, and equivalently by the choice of V.

V. Maximum Relative Equivocation

In the previous section, we consider the degraded and reversely degraded cases where it turned out that either $(U=\phi,V)$ or $(U=V,V)$ is optimal for the evaluation of the region given in Theorem 1. Here, we address the question whether one of these two choices $(U=\phi,V)$ and $(U=V,V)$ is always optimal. To this end, we consider the maximum relative equivocation that is achievable when there is no rate constraint on the transmitter. In other words, we are interested in the maximum relative equivocation that we can obtain when the legitimate user needs to reconstruct the source within a distortion D while there is no concern on the transmission rate R. We denote the maximum relative equivocation by $\Delta_{\max}(D)$ which is given in the following theorem.

Theorem 2: The maximum relative equivocation $\Delta_{\max}(D)$ at the eavesdropper with respect to the legitimate user when the legitimate user needs to reconstruct the source within a distortion D while there is no concern on the transmission rate R is given by

$$\Delta_{\max}(D) = \max_{\substack{U\to V\to X\to Y,Z \\ E\left[d(X,\hat{X}(V,Y))\right]\leq D}} I(X;Y|U) - I(X;Z|U) \tag{42}$$

We note that in Theorem 2, there are two auxiliary random variables U and V over which optimization needs to be carried out. In the previous section, we observe that when the model is either degraded or reversely degraded, a single auxiliary random variable is sufficient. Now, we provide the following example which shows that there are models for which two auxiliary random variables are necessary, in other words, neither $(U=\phi,V)$ nor $(U=V,V)$ is sufficient to attain the maximum relative equivocation, and hence the entire rate, relative equivocation and distortion region.

Example 5: Consider the parallel Gaussian source $\mathbf{X}_i = [X_{1,i}\ X_{2,i}]^\top$ where $\{X_{1,i}\}_{i=1}^n$ and $\{X_{2,i}\}_{i=1}^n$ are i.i.d. zero-mean Gaussian random variables with variances $\sigma_{X,1}^2$ and $\sigma_{X,2}^2$, respectively. The side information at the legitimate receiver and the eavesdropper are given by

$$Y_{\ell,i} = X_{\ell,i} + N_{Y,\ell,i}, \quad \ell = 1,2 \tag{43}$$

$$Z_{\ell,i} = X_{\ell,i} + N_{Z,\ell,i}, \quad \ell = 1,2 \tag{44}$$

where $\{N_{Y,\ell,i}\}_{i=1}^n$ and $\{N_{Z,\ell,i}\}_{i=1}^n$ are zero-mean Gaussian random variables with variances $\sigma_{Y,\ell}^2$ and $\sigma_{Z,\ell}^2$, respectively, which are independent of $\{X_{\ell,i}\}_{i=1}^n$. Moreover, we assume that $N_{Y,1,i}$ and $N_{Y,2,i}$ are independent, and also so are $N_{Z,1,i}$

and $N_{Z,2,i}$. We assume that noise variances satisfy

$$\sigma_{Y,1}^2 < \sigma_{Z,1}^2 \tag{45}$$

$$\sigma_{Z,2}^2 < \sigma_{Y,2}^2 \tag{46}$$

Hence, without loss of generality, we can assume the following Markov chains

$$X_1 \to Y_1 \to Z_1 \tag{47}$$

$$X_2 \to Z_2 \to Y_2 \tag{48}$$

We impose a separate distortion constraint on each component of the source as follows

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} E\left[(X_{\ell,i} - \hat{X}_{\ell,i})^2\right] \le D_\ell, \quad \ell = 1, 2 \tag{49}$$

Using Theorem 2, the maximum relative equivocation $\Delta_{\max}(D_1, D_2)$ can be obtained as follows.

Corollary 5:

$$\Delta_{\max}(D_1, D_2) = I(X_1; Y_1) - I(X_1; Z_1) \tag{50}$$

if there exists V_1 satisfying $V_1 \to X_1 \to Y_1 \to Z_1$ and $\sigma^2_{X_1|V_1Y_1} \le D_1$.

We note that the maximum relative equivocation given in (50) corresponds to the choice $U = (\phi, X_2), V = (V_1, X_2)$ with independent V_1 and X_2 for the relative equivocation bound given in Theorem 2. It is clear that this optimal choice does not correspond to either $(U = \phi, V)$ or $(U = V, V)$.

Next, we obtain the maximum relative equivocation arising from the choices $(U = \phi, V)$ and $(U = V, V)$. When $(U = \phi, V)$, the corresponding maximum relative equivocation $\Delta^{\phi}_{\max}(D_1, D_2)$ is stated in the following lemma.

Lemma 2:

$$\Delta^{\phi}_{\max}(D_1, D_2) = \sum_{i=1}^{2} I(X_i; Y_i) - I(X_i; Z_i) \tag{51}$$

if there exist (V_1, V_2) satisfying $V_i \to X_i \to Y_i, Z_i$ and $\sigma^2_{X_i|V_iY_i} \le D_i$.

Next, we obtain the maximum relative equivocation arising from the choice $U = V$, denoted by $\Delta^{\mathrm{S}}_{\max}(D_1, D_2)$, as stated in the following lemma.

Lemma 3:

$$\begin{aligned}&\Delta^{\mathrm{S}}_{\max}(D_1, D_2)\\ &= \max_{\substack{V_1 \to X_1 \to Y_1 \to Z_1\\ \sigma^2_{X_1|V_1Y_1} \le D_1}} I(X_1; Y_1|V_1) - I(X_1; Z_1|V_1)\end{aligned} \tag{52}$$

We note that (52) corresponds to the choice $U = V = (V_1, X_2)$ where V_1 and X_2 are independent.

Now, we compare the maximum relative equivocation with the ones arising from the choices $(U = \phi, V)$ and $U = V$. First, we compare $\Delta_{\max}(D_1, D_2)$ and $\Delta^{\phi}_{\max}(D_1, D_2)$ as follows

$$\begin{aligned}\Delta^{\phi}_{\max}(D_1, D_2) - \Delta_{\max}(D_1, D_2) &= I(X_2; Y_2) - I(X_2; Z_2)\\ &= -I(X_2; Z_2|Y_2) \qquad (53)\\ &< 0 \qquad (54)\end{aligned}$$

which implies that $(U = \phi, V)$ is, in general, a sub-optimal choice for the non-degraded parallel Gaussian model.

Next, we compare $\Delta_{\max}(D_1, D_2)$ and $\Delta^{\mathrm{S}}_{\max}(D_1, D_2)$. To this end, we introduce the following lemma which will be used in the sequel.

Lemma 4: **([16, Lem. 1])** For jointly Gaussian (X, Y, Z) satisfying the Markov chain $X \to Y \to Z$ and $\Pr[Y = Z] \ne 1$, if $D < \sigma^2_{X|Y}$, we have

$$\min_{\substack{V \to X \to Y \to Z\\ \sigma^2_{X|VY} \le D}} I(V; Y|Z) > 0 \tag{55}$$

Now, we are ready to compare $\Delta_{\max}(D_1, D_2)$ and $\Delta^{\mathrm{S}}_{\max}(D_1, D_2)$ as follows

$$\begin{aligned}&\Delta^{\mathrm{S}}_{\max}(D_1, D_2) - \Delta_{\max}(D_1, D_2)\\ &\quad= \max_{\substack{V_1 \to X_1 \to Y_1 \to Z_1\\ \sigma^2_{X_1|V_1Y_1} \le D_1}} I(X_1; Y_1|V_1) - I(X_1; Z_1|V_1)\\ &\qquad - [I(X_1; Y_1) - I(X_1; Z_1)] \qquad (56)\\ &\quad= \max_{\substack{V_1 \to X_1 \to Y_1 \to Z_1\\ \sigma^2_{X_1|V_1Y_1} \le D_1}} I(V_1; Z_1) - I(V_1; Y_1) \qquad (57)\\ &\quad= \max_{\substack{V_1 \to X_1 \to Y_1 \to Z_1\\ \sigma^2_{X_1|V_1Y_1} \le D_1}} -I(V_1; Y_1|Z_1) \qquad (58)\\ &\quad= -\min_{\substack{V_1 \to X_1 \to Y_1 \to Z_1\\ \sigma^2_{X_1|V_1Y_1} \le D_1}} I(V_1; Y_1|Z_1) \qquad (59)\\ &\quad< 0 \qquad (60)\end{aligned}$$

where (58) is due to the Markov chain $V_1 \to X_1 \to Y_1 \to Z_1$ and (60) comes from Lemma 4. Hence, (60) implies that $U = V$ is, in general, a sub-optimal choice for the non-degraded parallel Gaussian model.

This example shows that in general, we might need two different auxiliary random variables to evaluate the region $\mathcal{R}^*$ in Theorem 1 for non-degraded models. Hence, we conclude that, in general, the Wyner-Ziv coding scheme [20] is not sufficient to attain the region $\mathcal{R}^*$ for general non-degraded models.

VI. Uncoded Transmission

We note that in Theorem 2, there is no concern about the transmission rate R. Hence, the encoder can use any uncoded scheme that requires an infinite rate. We would like to understand whether the maximum relative equivocation $\Delta_{\max}(D)$ can be attained by an uncoded scheme. To this end, we consider a slightly more general scenario, where the encoder is allowed to use any *instantaneous* encoding function in the form of $g_i(X_i)$ where $g_i(\cdot)$ can be a deterministic or a stochastic mapping. When $g_i(\cdot)$ is chosen to be a stochastic function, we assume that it is independent across time. We note that since any uncoded scheme can be obtained from an instantaneous encoding scheme by choosing $g_i(\cdot)$ to be a linear function, the instantaneous encoding scheme encompasses any uncoded scheme. Moreover, uncoded transmission with artificial noise can also be obtained from an instantaneous encoding scheme by selecting $g_i(x) = \alpha x + N$, where N denotes the noise. When

the encoder uses an instantaneous encoding scheme, the transmitted signal is given by $M = [g_1(X_1), \ldots, g_n(X_n)]$. We denote the maximum relative equivocation when the encoder uses an instantaneous scheme by $\Delta_{\rm ins}(D)$, where, as usual, D denotes the distortion level within which the legitimate user needs to reconstruct the source. The following example shows that, in general, $\Delta_{\max}(D)$ cannot be achieved by an instantaneous encoding scheme, i.e., there are models where the maximum relative equivocation $\Delta_{\max}(D)$ is strictly larger than $\Delta_{\rm ins}(D)$, i.e., $\Delta_{\max}(D) > \Delta_{\rm ins}(D)$.

Example 6: In this example, we consider the degraded scalar Gaussian source and side information model which is defined in Example 3. Consequently, here, we have the Markov chain

$$X_i \to Y_i \to Z_i, \quad i = 1, \ldots, n \tag{61}$$

Using Theorem 2 and Corollary 1, the maximum relative equivocation $\Delta_{\max}(D)$ for the degraded scalar Gaussian model can be written as

$$\Delta_{\max}(D) = I(X;Y) - I(X;Z) \tag{62}$$

as long as there is a V satisfying $\sigma^2_{X|VY} \leq D$.

Next, we obtain $\Delta_{\rm ins}(D)$ for the degraded scalar Gaussian source and side information model.

Lemma 5:

$$\Delta_{\rm ins}(D) = \max_{\substack{V \to X \to Y \to Z \\ \sigma^2_{X|VY} \leq D}} I(X;Y|V) - I(X;Z|V) \tag{63}$$

We now compare $\Delta_{\max}(D)$ and $\Delta_{\rm ins}(D)$ as follows

$$\begin{aligned}
&\Delta_{\rm ins}(D) - \Delta_{\max}(D) \\
&\quad = \max_{\substack{V \to X \to Y \to Z \\ \sigma^2_{X|VY} \leq D}} I(X;Y|V) - I(X;Z|V) \\
&\qquad\qquad - [I(X;Y) - I(X;Z)] && (64)\\
&\quad = \max_{\substack{V \to X \to Y \to Z \\ \sigma^2_{X|VY} \leq D}} I(V;Z) - I(V;Y) && (65)\\
&\quad = \max_{\substack{V \to X \to Y \to Z \\ \sigma^2_{X|VY} \leq D}} - I(V;Y|Z) && (66)\\
&\quad = - \min_{\substack{V \to X \to Y \to Z \\ \sigma^2_{X|VY} \leq D}} I(V;Y|Z) && (67)\\
&\quad < 0 && (68)
\end{aligned}$$

where (66) follows from the Markov chain $V \to Y \to Z$ and (68) is due to Lemma 4. Hence, (68) implies that for the degraded scalar Gaussian source and side information model, the maximum relative equivocation cannot be achieved by an uncoded scheme, i.e., $\Delta_{\max}(D) > \Delta_{\rm ins}(D)$.

Example 6 shows that in general, the maximum relative equivocation cannot be achieved by an uncoded scheme. In other words, even when there is no concern on the transmission rate R that encoder uses, we still need to use a coded scheme to achieve the maximum relative equivocation at the eavesdropper.

VII. Conclusions

Here, we study the problem of secure lossy source coding with side information. Unlike the earlier works [13]–[16] using the equivocation of the source at the eavesdropper as the secrecy measure, we formulate this problem under a new secrecy measure, namely the relative equivocation of the source at the eavesdropper with respect to the legitimate user. We argue that this new secrecy measure corresponds to the natural generalization of the equivocation in a wiretap channel to the context of secure lossy source coding. We obtain a single-letter description of the rate, relative equivocation and distortion region for the problem of secure lossy source coding with side information under this new secrecy measure. We specialize this single-letter expression to the degraded and reversely degraded cases. We also discuss the relationships between the optimal scheme attaining this region and the Wyner-Ziv scheme.

References

[1] D. Gunduz, E. Erkip, and H. V. Poor. Secure lossless compression with side information. In *IEEE Information Theory Workshop*, 2008.

[2] D. Gunduz, E. Erkip, and H. V. Poor. Lossless compression with security constraints. In *ISIT*, 2008.

[3] V. Prabhakaran and K. Ramchandran. On secure distributed source coding. In *IEEE Information Theory Workshop*, 2007.

[4] R. Tandon, S. Ulukus, and K. Ramchandran. Secure source coding with a helper. In *Allerton Conf. Commun., Contr. and Comput.*, Oct. 2009. Also available at [arXiv:0910.5759].

[5] R. Tandon, S. Ulukus, and K. Ramchandran. Secure source coding with a helper. Submitted to *IEEE Trans. Inf. Theory*, Oct. 2009.

[6] W. Luh and D. Kundur. Distributed keyless secret sharing over noiseless channels. In *IEEE Globecom*, 2007.

[7] L. Grokop, A. Sahai, and M. Gastpar. Discriminatory source coding for a noiseless broadcast channel. In *IEEE ISIT*, 2005.

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

[9] 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.

[10] 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.

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

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

[13] 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.

[14] 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: 1009.3891v1].

[15] E. Ekrem and S. Ulukus. Secure lossy transmission of vector Gaussian sources. In *IEEE ISIT*, Aug. 2011.

[16] E. Ekrem and S. Ulukus. Secure lossy transmission of vector Gaussian sources. Submitted to *IEEE Trans. Inf. Theory*, Aug. 2011. Also available at [arXiv:1108.3544].

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

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

[19] N. Merhav. On joint coding for watermarking and encryption. *IEEE Trans. Inf. Theory*, 52(1):190–205, Jan. 2006.

[20] 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.

[21] E. Ekrem and S. Ulukus. Secure lossy source coding with side information under relative equivocation. In preparation.