Secure Lossy Transmission of Vector Gaussian Sources

Ersen Ekrem, *Student Member, IEEE*, and Sennur Ulukus, *Member, IEEE*

Abstract—We study the secure lossy transmission of a vector Gaussian source to a legitimate user in the presence of an eavesdropper, where both the legitimate user and the eavesdropper have vector Gaussian side information. The aim of the transmitter is to describe the source to the legitimate user in a way that the legitimate user can reconstruct the source within a certain distortion level while the eavesdropper is kept ignorant of the source as much as possible as measured by the equivocation. 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. This characterization of the maximum equivocation involves two auxiliary random variables. We show that a nontrivial selection for both random variables may be necessary in general. The necessity of two auxiliary random variables also implies that, in general, Wyner–Ziv coding is suboptimal in the presence of an eavesdropper. In addition, we show that, even when there is no rate constraint on the legitimate link, uncoded transmission (deterministic or stochastic) is suboptimal; the presence of an eavesdropper necessitates the use of a coded scheme to attain the maximum equivocation.

Index Terms—Secure lossy source coding, vector Gaussian source, Wyner–Ziv coding.

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, in other words, secure transmission of uniformly distributed messages is studied.

Secure source coding problem has been studied for both lossless and lossy reconstruction cases in [3]–[16]. Secure *lossless*

source coding problem is studied in [3]–[9]. The common theme of these works is that the legitimate receiver wants to reconstruct the source in a lossless fashion by using the information it gets from the transmitter in conjunction with its side information, while the eavesdropper is being kept ignorant of the source as much as possible. Secure lossy source coding problem is studied in [10]–[16]. 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 [15], [16]. In [15], 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 [15], in addition to the degradedness that the wiretap channel exhibits, the source and side information 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 [15], 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 [16], the setting of [15] is partially generalized such that in [16], the source and side information do not have any degradedness structure. On the other hand, as opposed to the *noisy* wiretap channel of [15], in [16], the channel between the transmitter and receivers is assumed to be *noiseless*. For this setting, in [16], a single-letter characterization of the rate, equivocation, and distortion region is provided.

Here, we consider the setting of [16] for jointly Gaussian source and side information. In particular, we consider the model where the transmitter has a vector Gaussian source which is jointly Gaussian with the vector Gaussian side information 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 as measured by the equivocation. A single-letter characterization of the rate, equivocation, and distortion region for this setting exists due to [16]. Although we are unable to evaluate this single-letter characterization for the vector Gaussian source and side information 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
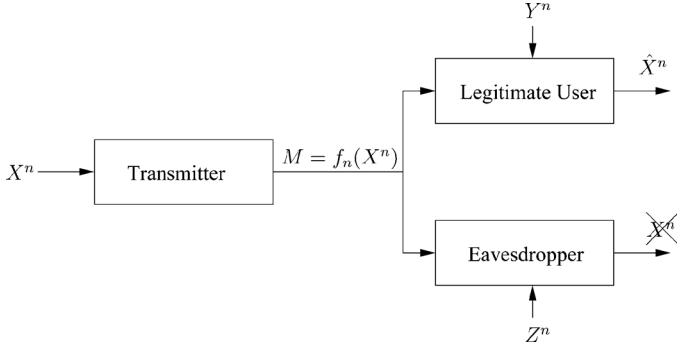
Fig. 1. Secure lossy source coding with side information.

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. We show that this outer bound is tight when we remove the rate constraint at the transmitter. In other words, we obtain the maximum achievable equivocation at the eavesdropper when the legitimate user needs to reconstruct the vector Gaussian source within a fixed distortion while there is no constraint on the transmission rate.

We note some implications of this result. First, we note that since there is no rate constraint on the transmitter, it can use an uncoded scheme to describe the source to the legitimate user, and, indeed, it can use any instantaneous (deterministic or stochastic) encoding scheme for this purpose. However, we show through an example that even when there is no rate constraint on the transmitter, to attain the maximum equivocation at the eavesdropper, in general, the transmitter needs to use a coded scheme. Hence, the presence of an eavesdropper necessitates the use of a coded scheme even in the absence of a rate constraint on the transmitter. Second, we note that the maximum equivocation expression has two different covariance matrices originating from the presence of two auxiliary random variables in the single-letter expression. We show through another example that both of these covariance matrices, in other words, both of these two auxiliary random variables, are needed in general to attain the maximum equivocation at the eavesdropper. The necessity of two covariance matrices, and hence two auxiliary random variables, implies that, in general, Wyner–Ziv coding scheme [17] is not sufficient to attain the maximum equivocation at the eavesdropper.

II. SECURE LOSSY SOURCE CODING

Here, we describe the secure lossy source coding problem (see Fig. 1) 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, the 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 ignorant of the source X^n as much as possible as measured by the equivocation. We note that if there was no eavesdropper, this setting would reduce to the Wyner–Ziv problem [17], for which a single-letter characterization for the minimum transmission rate of the transmitter for each distortion level exists.

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 the function $d^n(X^n, \hat{X}^n)$ that has the following form:

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

where $d(a, b)$ is a nonnegative finite-valued function. The confusion of the eavesdropper is measured by the following equivocation term:

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

where $M \in \mathcal{M}$, which 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 $f_n : \mathcal{X}^n \to \mathcal{M} = \{1, \dots, 2^{nR}\}$ 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, equivocation, and distortion tuple (R, R_e, D) is achievable if there exists an (n, R) code satisfying

$$\lim_{n \to \infty} \frac{1}{n} H(X^n | Z^n, M) \geq R_e \qquad (3)$$

$$\lim_{n \to \infty} E[d(X^n, \hat{X}^n)] \leq D. \qquad (4)$$

The set of all achievable (R, R_e, D) tuples is denoted by $\mathcal{R}^*$ which is given by the following theorem.

Theorem 1 ([16, Theorem 1]): $(R, R_e, D) \in \mathcal{R}^*$ iff

$$R \geq I(V; X | Y) \qquad (5)$$
$$R_e \leq H(X | V, Y) + I(X; Y | U) - I(X; Z | U) \qquad (6)$$
$$D \geq E[d(X, \hat{X}(V, Y))] \qquad (7)$$

for some U, V satisfying the following Markov chain:

$$U \to V \to X \to Y, Z \qquad (8)$$

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

The achievable scheme that attains the region $\mathcal{R}^*$ has the same spirit as the Wyner–Ziv scheme [17] in the sense that both achievable schemes use binning to exploit the side information at the legitimate user, and consequently, to reduce the rate requirement. The difference of the achievable scheme that attains $\mathcal{R}^*$ comes from the additional binning necessitated by the presence of an eavesdropper. In particular, the transmitter generates sequences (U^n, V^n) and bins both sequences. The transmitter sends these two bin indices. 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 (6)[1]. Indeed, this achievable scheme can be viewed as if it is using a rate-splitting technique to send the message M, since M has two coordinates, one for

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

the bin index of U^n, and one for the bin index of V^n. This perspective reveals the similarity of the achievable scheme that attains $\mathcal{R}^*$ and the one that attains the capacity-equivocation region of the wiretap channel [2] where also rate-splitting is used. In particular, in the latter case, the message W is divided into two parts W_{ne}, W_e such that W_{ne} is sent by the sequence U^n and W_e is sent by the sequence V^n. The eavesdropper decodes W_{ne} whereas the other message W_e contributes to the secrecy.

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 I_e defined by

$$\lim_{n \to \infty} \frac{1}{n} I(X^n; Z^n, M). \tag{9}$$

Once we are interested in the mutual information leakage to the eavesdropper, 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

$$\lim_{n \to \infty} \frac{1}{n} I(X^n; Z^n, M) \leq I_e \tag{10}$$

$$\lim_{n \to \infty} E[d(X^n, \hat{X}^n)] \leq D. \tag{11}$$

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 ([16]): $(R, I_e, D) \in \mathcal{R}$ iff

$$R \geq I(V; X|Y) \tag{12}$$

$$I_e \geq I(V; X) - I(V; Y|U) + I(X; Z|U) \tag{13}$$

$$D \geq E[d(X, \hat{X}(V, Y))] \tag{14}$$

for some U, V satisfying the following Markov chain:

$$U \to V \to X \to Y, Z \tag{15}$$

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

III. VECTOR GAUSSIAN SOURCES

Now we study the secure lossy source coding problem for jointly Gaussian $\{(\mathbf{X}_i, \mathbf{Y}_i, \mathbf{Z}_i)\}_{i=1}^n$ (see Fig. 2) 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 other words, we consider the case where $\mathbf{X}_i$ is a zero-mean Gaussian random vector with covariance matrix $\mathbf{K}_X \succ \mathbf{0}$,[2] and the side information at the legitimate user $\mathbf{Y}_i$ and the eavesdropper $\mathbf{Z}_i$ are jointly Gaussian with the source $\mathbf{X}_i$. In particular, we assume that $\mathbf{Y}_i, \mathbf{Z}_i$ have the following form:

$$\mathbf{Y}_i = \mathbf{X}_i + \mathbf{N}_{Y,i} \tag{16}$$

$$\mathbf{Z}_i = \mathbf{X}_i + \mathbf{N}_{Z,i} \tag{17}$$

---

[2]$\mathbf{A} \succ \mathbf{B}$ means that the difference between the matrices $\mathbf{A}$ and $\mathbf{B}$, i.e., $\mathbf{A} - \mathbf{B}$, is strictly positive definite; and $\mathbf{A} \succeq \mathbf{B}$ means that the difference between the matrices $\mathbf{A}$ and $\mathbf{B}$, i.e., $\mathbf{A} - \mathbf{B}$, is positive semidefinite.
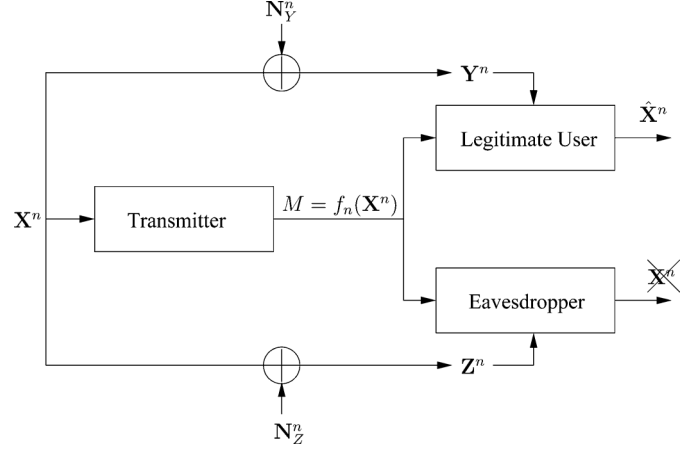

Fig. 2. Secure lossy source coding with side information for jointly Gaussian source and side information.

where $\mathbf{N}_{Y,i}$ and $\mathbf{N}_{Z,i}$ are independent zero-mean Gaussian random vectors with covariance matrices $\mathbf{\Sigma}_Y \succ \mathbf{0}$ and $\mathbf{\Sigma}_Z \succ \mathbf{0}$, respectively, and $(\mathbf{N}_{Y,i}, \mathbf{N}_{Z,i})$ and $\mathbf{X}_i$ are independent. We note that the side information given by (16)–(17) are not in the most general form. In the most general case, we have

$$\mathbf{Y}_i = \mathbf{H}_Y \mathbf{X}_i + \mathbf{N}_{Y,i} \tag{18}$$

$$\mathbf{Z}_i = \mathbf{H}_Z \mathbf{X}_i + \mathbf{N}_{Z,i} \tag{19}$$

for some $\mathbf{H}_Y, \mathbf{H}_Z$ matrices. However, until Section V, we consider the form of side information given by (16)–(17), and obtain our results for this model. In Section V, we generalize our results to the most general case given by (18)–(19). We note that since the rate, information leakage, and distortion region is invariant with respect to the correlation between $\mathbf{N}_{Y,i}$ and $\mathbf{N}_{Z,i}$, the correlation between $\mathbf{N}_{Y,i}$ and $\mathbf{N}_{Z,i}$ is immaterial.

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

$$E\left[\left(\mathbf{X}_i - \hat{\mathbf{X}}_i\right)\left(\mathbf{X}_i - \hat{\mathbf{X}}_i\right)^\top\right]. \tag{20}$$

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

$$\frac{1}{n} \sum_{i=1}^n E\left[\left(\mathbf{X}_i - \hat{\mathbf{X}}_i\right)\left(\mathbf{X}_i - \hat{\mathbf{X}}_i\right)^\top\right] \preceq \mathbf{D}. \tag{21}$$

Throughout the paper, we assume that $\mathbf{0} \preceq \mathbf{D} \preceq \mathbf{K}_{X|Y}$ where $\mathbf{K}_{X|Y}$ is the conditional covariance matrix of $\mathbf{X}$ conditioned on $\mathbf{Y}$:

$$\mathbf{K}_{X|Y} = E\left[\left(\mathbf{X} - E\left[\mathbf{X}|\mathbf{Y}\right]\right)\left(\mathbf{X} - E\left[\mathbf{X}|\mathbf{Y}\right]\right)^\top\right]. \tag{22}$$

Since the mean square error is minimized by the minimum mean square error (MMSE) estimator which is given by the conditional mean, we assume that the legitimate user applies this optimal estimator, i.e., the legitimate user selects its reconstruction function $\{\hat{\mathbf{X}}_i\}_{i=1}^n$ as

$$\hat{\mathbf{X}}_i = E\left[\mathbf{X}_i|\mathbf{Y}^n, f_n(\mathbf{X}^n)\right]. \tag{23}$$

Once the estimator of the legitimate user is set as (23), 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

$$R \geq I(V; \mathbf{X} | \mathbf{Y}) \tag{24}$$

$$I_e \geq I(V; \mathbf{X}) - I(V; \mathbf{Y} | U) + I(\mathbf{X}; \mathbf{Z} | U) \tag{25}$$

$$\mathbf{D} \succeq \mathbf{K}_{X|VY} \tag{26}$$

for some U, V satisfying the following Markov chain:

$$U \to V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z}. \tag{27}$$

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 $\mathcal{R}$.

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

$$\mathcal{R}(\mathbf{D}) \subseteq \mathcal{R}^o(\mathbf{D}) \tag{28}$$

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

$$R \geq \frac{1}{2} \log \frac{|\mathbf{K}_{X|Y}|}{|\mathbf{D}|} = \frac{1}{2} \log \frac{|\mathbf{K}_X|}{|\mathbf{F}(\mathbf{D})|} - \frac{1}{2} \log \frac{|\mathbf{K}_X + \mathbf{\Sigma}_Y|}{|\mathbf{F}(\mathbf{D}) + \mathbf{\Sigma}_Y|} \tag{29}$$

$$\begin{aligned} I_e \geq \min_{\substack{0 \preceq \mathbf{K}_{X|V} \preceq \mathbf{K}_{X|U} \preceq \mathbf{K}_X \\ \mathbf{K}_{X|V} \preceq \mathbf{F}(\mathbf{D})}} &\frac{1}{2} \log \frac{|\mathbf{K}_X|}{|\mathbf{K}_{X|V}|} - \frac{1}{2} \log \frac{|\mathbf{K}_{X|U} + \mathbf{\Sigma}_Y|}{|\mathbf{K}_{X|V} + \mathbf{\Sigma}_Y|} \\ &+ \frac{1}{2} \log \frac{|\mathbf{K}_{X|U} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \end{aligned} \tag{30}$$

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

We will prove Theorem 4 in Section IV. In the remainder of this section, we provide interpretations and discuss some implications of Theorem 4.

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 (29) is obtained by minimizing the rate constraint in (24) and the mutual information leakage lower bound in (30) is obtained by minimizing the mutual information leakage constraint in (25) separately. However, to characterize the rate and mutual information leakage region $\mathcal{R}(\mathbf{D})$, one needs to minimize the rate constraint in (24) and the mutual leakage information constraint in (25) jointly, not separately. In particular, since the region $\mathcal{R}(\mathbf{D})$ is convex in the pairs (R, I_e) as per a time-sharing argument, joint optimization of the rate constraint in (24) and the mutual information leakage constraint in (25) can be carried out by considering the tangent lines to the region $\mathcal{R}(\mathbf{D})$, i.e., by solving the following optimization problem:

$$\begin{aligned} L(\mu_1, \mu_2) &= \min_{(R, I_e) \in \mathcal{R}(\mathbf{D})} \mu_1 R + \mu_2 I_e \tag{31} \\ &= \min_{\substack{U \to V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z} \\ \mathbf{K}_{X|VY} \preceq \mathbf{D}}} \mu_1 \left[I(V; \mathbf{X}) - I(V; \mathbf{Y}) \right] \\ &\quad + \mu_2 \left[I(V; \mathbf{X}) - I(V; \mathbf{Y}|U) + I(\mathbf{X}; \mathbf{Z}|U) \right] \end{aligned} \tag{32}$$

for all values of μ_1, μ_2, where $\mu_j \in [0, \infty)$, $j = 1, 2$. As of now, we have been unable to 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:

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

$$I_e \geq L(0, 1). \tag{34}$$

We note that the constraint in (29), and hence $L(1, 0)$, gives us the Wyner–Ziv rate distortion function [17] for the vector Gaussian sources. Moreover, we note that $L(0, 1)$ gives us 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 $I_e^{\min}(\mathbf{D})$, the corresponding result can be stated as follows.

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

$$\begin{aligned} I_e^{\min}(\mathbf{D}) = \min_{\substack{0 \preceq \mathbf{K}_{X|V} \preceq \mathbf{K}_{X|U} \preceq \mathbf{K}_X \\ \mathbf{K}_{X|V} \preceq \mathbf{F}(\mathbf{D})}} &\frac{1}{2} \log \frac{|\mathbf{K}_X|}{|\mathbf{K}_{X|V}|} \\ - \frac{1}{2} \log \frac{|\mathbf{K}_{X|U} + \mathbf{\Sigma}_Y|}{|\mathbf{K}_{X|V} + \mathbf{\Sigma}_Y|} &+ \frac{1}{2} \log \frac{|\mathbf{K}_{X|U} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \end{aligned} \tag{35}$$

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 receiver is able to reconstruct the source within a distortion constraint $\mathbf{D}$, the use of jointly Gaussian $(U, V, \mathbf{X})$ is optimal. Since in Theorem 5, there is no rate constraint, one natural question to ask is whether $I_e^{\min}(\mathbf{D})$ can be achieved by an uncoded transmission scheme. Now, we address this question in a broader context by letting the encoder use any *instantaneous* encoding function in the form of $g_i(\mathbf{X}_i)$ where $g_i(\cdot)$ can be a deterministic or a stochastic mapping. When $g_i(\cdot)$ is chosen to be stochastic, we assume it to be independent across time. We note that the uncoded transmission can be obtained from instantaneous encoding by selecting $g_i(\cdot)$ to be a linear function. Similarly, uncoded transmission with artificial noise can be obtained from instantaneous encoding by selecting $g_i(x) = \alpha x + N$, where N denotes the noise. Hence, if the encoder uses an instantaneous encoding scheme, the transmitted signal is given by $M = [g_1(\mathbf{X}_1), \dots, g_n(\mathbf{X}_n)]$. Let $I_e^{\mathrm{ins}}(\mathbf{D})$ be the minimum information leakage to the eavesdropper when the legitimate user is able to reconstruct the source with a distortion constraint $\mathbf{D}$ while the encoder uses an instantaneous encoding. The following example demonstrates that, in general, $I_e^{\min}(\mathbf{D})$ cannot be achieved by instantaneous encoding.

Example 1: Consider the scalar case, where the side information at the legitimate user and the eavesdropper are given as follows:

$$Y_i = X_i + N_{y,i} \tag{36}$$

$$Z_i = X_i + N_{z,i} \tag{37}$$

where $X_i, N_{y,i}$, and $N_{z,i}$ are zero-mean Gaussian random variables with variances σ_x^2, σ_y^2, and σ_z^2, respectively. $\{X_i\}_{i=1}^n, \{N_{y,i}\}_{i=1}^n$, and $\{N_{z,i}\}_{i=1}^n$ are independent. We assume that $\sigma_y^2 < \sigma_z^2$, which implies that we can assume $X \rightarrow Y \rightarrow Z$ since the scalar model in (36)–(37) is statistically degraded, or in other words, the correlation between $N_{y,i}$ and $N_{z,i}$ does not affect the achievable (R, I_e, D) region. Using Theorem 3, $I_e^{\min}(D)$ for the scalar Gaussian channel under consideration can be found as follows:

$$I_e^{\min}(D) = \min_{\substack{U \rightarrow V \rightarrow X \rightarrow Y \rightarrow Z \\ \sigma_{x|vy}^2 \leq D}} I(V;X) - I(V;Y|U)$$

$$+ I(X;Z|U) \qquad (38)$$

$$= \min_{\substack{V \rightarrow X \rightarrow Y \rightarrow Z \\ \sigma_{x|vy}^2 \leq D}} I(V;X) - I(V;Y) + I(X;Z)$$

$$(39)$$

where in (39), we used the Markov chain $U \rightarrow V \rightarrow X \rightarrow Y \rightarrow Z$.

As shown in Appendix A, the information leakage to the eavesdropper when the encoder uses an instantaneous mapping is given by

$$I_e^{\text{ins}}(D) = \min_{\substack{V \rightarrow X \rightarrow Y \rightarrow Z \\ \sigma_{x|vy}^2 \leq D}} I(X;V,Z) \qquad (40)$$

$$= \min_{\substack{V \rightarrow X \rightarrow Y \rightarrow Z \\ \sigma_{x|vy}^2 \leq D}} I(V;X) - I(V;Z) + I(X;Z)$$

$$(41)$$

where (41) is obtained by using the Markov chain $V \rightarrow X \rightarrow Z$.

Using (39) and (41), we have

$$I_e^{\text{ins}}(D) - I_e^{\min}(D)$$

$$= \min_{\substack{V \rightarrow X \rightarrow Y \rightarrow Z \\ \sigma_{x|vy}^2 \leq D}} I(V;X) - I(V;Z) + I(X;Z)$$

$$- \min_{\substack{V \rightarrow X \rightarrow Y \rightarrow Z \\ \sigma_{x|vy}^2 \leq D}} I(V;X) - I(V;Y) + I(X;Z) \quad (42)$$

$$\geq \min_{\substack{V \rightarrow X \rightarrow Y \rightarrow Z \\ \sigma_{x|vy}^2 \leq D}} I(V;Y) - I(V;Z) \qquad (43)$$

$$= \min_{\substack{V \rightarrow X \rightarrow Y \rightarrow Z \\ \sigma_{x|vy}^2 \leq D}} I(V;Y|Z) \qquad (44)$$

where (44) comes from the Markov chain $V \rightarrow Y \rightarrow Z$. Next, we note the following lemma.

Lemma 1: For jointly Gaussian (X, Y, Z) satisfying the Markov chain $X \rightarrow Y \rightarrow Z$ and $\Pr[Y = Z] \neq 1$, if $D < \sigma_{x|y}^2$, we have

$$\min_{\substack{V \rightarrow X \rightarrow Y \rightarrow Z \\ \sigma_{x|vy}^2 \leq D}} I(V;Y|Z) > 0. \qquad (45)$$

The proof of Lemma 1 can be found in Appendix B. The proof of Lemma 1 starts with the observation that (45) is zero iff we have the Markov chain $V \rightarrow Z \rightarrow Y$. On the other hand, since we already have the Markov chain $V \rightarrow X \rightarrow Y \rightarrow Z$, and Y

and Z are not identical, we show in Appendix B that the Markov chain $V \rightarrow Z \rightarrow Y$ is possible iff V and X are independent. However, if $D < \sigma_{x|y}^2$, any V that is independent of X is not feasible. Hence, Lemma 1 follows. Lemma 1 implies that in general, we have $I_e^{\text{ins}}(D) \neq I_e^{\min}(D)$, i.e., $I_e^{\min}(\mathbf{D})$ cannot be achieved by instantaneous encoding.

This example shows that an uncoded transmission is not optimal even when there is no rate constraint. This is due to the presence of an eavesdropper; the presence of an eavesdropper necessitates the use of a coded scheme.

Another question that Theorem 5 brings about is whether the minimum in (35) is achieved by a nontrivial $\mathbf{K}_{X|U}$. By a trivial selection for $\mathbf{K}_{X|U}$, we mean either $\mathbf{K}_{X|U} = \mathbf{K}_X$ or $\mathbf{K}_{X|U} = \mathbf{K}_{X|V}$. The former corresponds to the selection $U = \phi$ and the latter corresponds to the selection $U = V$. We note that although (35) is monotonically decreasing in $\mathbf{K}_{X|V}$ in the positive semidefinite sense, (35) is neither monotonically increasing nor monotonically decreasing in $\mathbf{K}_{X|U}$ in the positive semidefinite sense. Hence, due to this lack of monotonicity of (35) in $\mathbf{K}_{X|U}$, in general, we expect that both $U \neq \phi$ and $U \neq V$ may be necessary to attain the minimum in (35). The following example demonstrates that in general $U \neq \phi$ and $U \neq V$ may be necessary.

Example 2: Consider the Gaussian source $\mathbf{X} = [X_1 X_2]^\top$ where X_1 and X_2 are independent. The side information at the legitimate receiver and the eavesdropper are given by

$$Y_\ell = X_\ell + N_{Y,\ell}, \quad \ell = 1, 2 \qquad (46)$$

$$Z_\ell = X_\ell + N_{Z,\ell}, \quad \ell = 1, 2 \qquad (47)$$

where $N_{Y,\ell}$ and $N_{Z,\ell}$ are zero-mean Gaussian random variables with variances $\sigma_{Y,\ell}^2$ and $\sigma_{Z,\ell}^2$, respectively. Moreover, $N_{Y,1}$ and $N_{Y,2}$ are independent, and also so are $N_{Z,1}$ and $N_{Z,2}$. We assume that noise variances satisfy

$$\sigma_{Y,1}^2 < \sigma_{Z,1}^2 \qquad (48)$$

$$\sigma_{Z,2}^2 < \sigma_{Y,2}^2 \qquad (49)$$

which, in view of the fact that correlation between the noise at the legitimate receiver and the noise at the eavesdropper does not affect the rate, distortion, and information leakage region, lets us assume the following Markov chains:

$$X_1 \rightarrow Y_1 \rightarrow Z_1 \qquad (50)$$

$$X_2 \rightarrow Z_2 \rightarrow Y_2. \qquad (51)$$

Moreover, we assume that the distortion constraint $\mathbf{D}$ is a diagonal matrix with diagonal entries D_1 and D_2. In this case, the minimum information leakage is given by

$$I_e^{\min}(D_1, D_2)$$

$$= \min_{\substack{V_1 \rightarrow X_1 \rightarrow Y_1 \rightarrow Z_1 \\ \sigma_{X_1|V_1 Y_1}^2 \leq D_1}} I(V_1; X_1) - I(V_1; Y_1) + I(X_1; Z_1)$$

$$+ \min_{\substack{V_2 \rightarrow X_2 \rightarrow Z_2 \rightarrow Y_2 \\ \sigma_{X_2|V_2 Y_2}^2 \leq D_2}} I(V_2; X_2) + I(X_2; Z_2|V_2) \quad (52)$$

whose proof can be found in Appendix C. The minimum information leakage in (52) corresponds the selections $U = (\phi, V_2)$

and $V = (V_1, V_2)$, where (U_1, V_1) and (U_2, V_2) are independent. This selection of (U, V) corresponds to neither $U = \phi$ nor $U = V$.

Next, we obtain the minimum information leakage that arises when we set either $U = \phi$ or $U = V$, and show that the minimum information leakage arising from these selections are strictly larger than the minimum information leakage in (52), which will imply the suboptimality of $U = \phi$ and $U = V$. When we set $U = \phi$, the minimum information leakage is given by

$$
\begin{aligned}
& I_e^{\min-\phi}(D_1, D_2) \\
& = \min_{\substack{V_1 \to X_1 \to Y_1 \to Z_1 \\ \sigma^2_{X_1|V_1 Y_1} \leq D_1}} I(V_1; X_1) - I(V_1; Y_1) + I(X_1; Z_1) \\
& \quad + \min_{\substack{V_2 \to X_2 \to Z_2 \to Y_2 \\ \sigma^2_{X_2|V_2 Y_2} \leq D_2}} I(V_2; X_2) - I(V_2; Y_2) + I(X_2; Z_2)
\end{aligned}
\tag{53}
$$

whose proof is given in Appendix D. When we set $U = V$, the minimum information leakage is given by

$$
\begin{aligned}
& I_e^{\min-S}(D_1, D_2) \\
& = \min_{\substack{V_1 \to X_1 \to Y_1 \to Z_1 \\ \sigma^2_{X_1|V_1 Y_1} \leq D_1}} I(V_1; X_1) + I(X_1; Z_1|V_1) \\
& \quad + \min_{\substack{V_2 \to X_2 \to Z_2 \to Y_2 \\ \sigma^2_{X_2|V_2 Y_2} \leq D_2}} I(V_2; X_2) + I(X_2; Z_2|V_2)
\end{aligned}
\tag{54}
$$

whose proof can be found in Appendix D.

Now, we compare the minimum information leakage in (52) with (53) and (54) to show that the selections $U = \phi$ and $U = V$ are suboptimal in general. Using (52) and (53), we obtain

$$
\begin{aligned}
& I_e^{\min-\phi}(D_1, D_2) - I_e^{\min}(D_1, D_2) \\
& = \min_{\substack{V_2 \to X_2 \to Z_2 \to Y_2 \\ \sigma^2_{X_2|V_2 Y_2} \leq D_2}} I(V_2; X_2) - I(V_2; Y_2) + I(X_2; Z_2) \\
& \quad - \min_{\substack{V_2 \to X_2 \to Z_2 \to Y_2 \\ \sigma^2_{X_2|V_2 Y_2} \leq D_2}} I(V_2; X_2) + I(X_2; Z_2|V_2)
\end{aligned}
\tag{55}
$$

$$
\geq \min_{\substack{V_2 \to X_2 \to Z_2 \to Y_2 \\ \sigma^2_{X_2|V_2 Y_2} \leq D_2}} I(X_2; Z_2) - I(X_2; Z_2|V_2) - I(V_2; Y_2)
\tag{56}
$$

$$
= \min_{\substack{V_2 \to X_2 \to Z_2 \to Y_2 \\ \sigma^2_{X_2|V_2 Y_2} \leq D_2}} I(V_2; Z_2) - I(V_2; Y_2)
\tag{57}
$$

$$
= \min_{\substack{V_2 \to X_2 \to Z_2 \to Y_2 \\ \sigma^2_{X_2|V_2 Y_2} \leq D_2}} I(V_2; Z_2|Y_2)
\tag{58}
$$

$$
> 0
\tag{59}
$$

where (57)–(58) follow from the Markov chain:

$$
V_2 \to X_2 \to Z_2 \to Y_2
\tag{60}
$$

and (59) comes from Lemma 1. Thus, in general, we have $I_e^{\min-\phi}(D_1, D_2) \neq I_e^{\min}(D_1, D_2)$, or in other words, in general, $U = \phi$ is suboptimal.

Next, we consider the selection $U = V$. Using (52) and (54), we have

$$
\begin{aligned}
& I_e^{\min-S}(D_1, D_2) - I_e^{\min}(D_1, D_2) \\
& = \min_{\substack{V_1 \to X_1 \to Y_1 \to Z_1 \\ \sigma^2_{X_1|V_1 Y_1} \leq D_1}} I(V_1; X_1) + I(X_1; Z_1|V_1) \\
& \quad - \min_{\substack{V_1 \to X_1 \to Y_1 \to Z_1 \\ \sigma^2_{X_1|V_1 Y_1} \leq D_1}} I(V_1; X_1) - I(V_1; Y_1) + I(X_1; Z_1)
\end{aligned}
\tag{61}
$$

$$
\geq \min_{\substack{V_1 \to X_1 \to Y_1 \to Z_1 \\ \sigma^2_{X_1|V_1 Y_1} \leq D_1}} I(X_1; Z_1|V_1) + I(V_1; Y_1) - I(X_1; Z_1)
\tag{62}
$$

$$
= \min_{\substack{V_1 \to X_1 \to Y_1 \to Z_1 \\ \sigma^2_{X_1|V_1 Y_1} \leq D_1}} I(V_1; Y_1) - I(V_1; Z_1)
\tag{63}
$$

$$
= \min_{\substack{V_1 \to X_1 \to Y_1 \to Z_1 \\ \sigma^2_{X_1|V_1 Y_1} \leq D_1}} I(V_1; Y_1|Z_1)
\tag{64}
$$

$$
> 0
\tag{65}
$$

where (63)–(64) follow from the Markov chain

$$
V_1 \to X_1 \to Y_1 \to Z_1
\tag{66}
$$

and (65) comes from Lemma 1. Thus, in general, we have $I_e^{\min-S}(D_1, D_2) \neq I_e^{\min}(D_1, D_2)$, or in other words, in general, $U = V$ is suboptimal.

Example 2 shows that, in general, we might need two covariance matrices, and hence two different auxiliary random variables, to attain the minimum information leakage. Indeed, if we have either $U = V$ or $U = \phi$, the corresponding achievable scheme is identical to the Wyner–Ziv scheme [17]. Hence, the necessity of two different auxiliary random variables implies that, in general, Wyner–Ziv scheme [17] is suboptimal.

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 (24) and the mutual information leakage constraint in (25) separately. We first consider the rate constraint in (24) as follows:

$$
R \geq L(1, 0) = \min_{\substack{V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z} \\ \mathbf{K}_{X|VY} \preceq \mathbf{D}}} I(V; \mathbf{X}|\mathbf{Y})
\tag{67}
$$

$$
= \min_{\substack{V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z} \\ \mathbf{K}_{X|VY} \preceq \mathbf{D}}} h(\mathbf{X}|\mathbf{Y}) - h(\mathbf{X}|V, \mathbf{Y})
\tag{68}
$$

$$
= \min_{\substack{V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z} \\ \mathbf{K}_{X|VY} \preceq \mathbf{D}}} \frac{1}{2} \log |(2\pi e)\mathbf{K}_{X|Y}| - h(\mathbf{X}|V, \mathbf{Y})
\tag{69}
$$

$$
= \min_{\mathbf{K}_{X|VY} \preceq \mathbf{D}} \frac{1}{2} \log \frac{|\mathbf{K}_{X|Y}|}{|\mathbf{K}_{X|VY}|}
\tag{70}
$$

$$
= \frac{1}{2} \log \frac{|\mathbf{K}_{X|Y}|}{|\mathbf{D}|}
\tag{71}
$$

where (70) comes from the fact that $h(\mathbf{X}|V, \mathbf{Y})$ is maximized by jointly Gaussian $(V, \mathbf{X}, \mathbf{Y})$, and (71) comes from the monotonicity of $|\cdot|$ in positive semidefinite matrices. Now we introduce the following lemma.

Lemma 2:

$$\frac{1}{2}\log\frac{|\mathbf{K}_{X|Y}|}{|\mathbf{D}|} = \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{F(D)}|} - \frac{1}{2}\log\frac{|\mathbf{K}_X + \boldsymbol{\Sigma}_Y|}{|\mathbf{F(D)} + \boldsymbol{\Sigma}_Y|}. \quad (72)$$

The proof of Lemma 2 is given in Appendix E. Lemma 2 and (71) imply (29).

Next, we consider the mutual information leakage constraint in (25) as follows:

$$I_e \geq L(0,1) \quad (73)$$

$$= \min_{\substack{U \to V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z} \\ \mathbf{K}_{X|VY} \preceq \mathbf{D}}} I(V;\mathbf{X}) - I(V;\mathbf{Y}|U) + I(\mathbf{X};\mathbf{Z}|U). \quad (74)$$

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

$$C(L) = I(V;\mathbf{X}) - I(V;\mathbf{Y}) + I(U;\mathbf{Y}) + I(\mathbf{X};\mathbf{Z}|U) \quad (75)$$

$$= I(V;\mathbf{X}|\mathbf{Y}) + [I(U;\mathbf{Y}) + I(\mathbf{X};\mathbf{Z}|U)] \quad (76)$$

where (75) comes from the Markov chain $U \to V \to \mathbf{Y}$ and (76) comes from the Markov chain $V \to \mathbf{X} \to \mathbf{Y}$. We note that the first term in (76) is minimized by a jointly Gaussian $(V,\mathbf{X})$ as we already showed in obtaining the lower bound for the rate given by (29) above in (67)–(71). On the other hand, the remaining term of (76) in the bracket is maximized by a jointly Gaussian $(U,\mathbf{X})$ as shown in [18]. 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 will 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 for $(U,V,\mathbf{X})$. We note that any jointly Gaussian $(U,V,\mathbf{X})$ can be written as

$$V = \mathbf{A}_V \mathbf{X} + \mathbf{N}_V \quad (77)$$

$$U = \mathbf{A}_U \mathbf{X} + \mathbf{N}_U \quad (78)$$

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

Lemma 3: When $\mathbf{D} \preceq \mathbf{K}_{X|Y}$ and V is Gaussian, we have the following facts:
1) $\boldsymbol{\Sigma}_Y - \mathbf{D} \succ \mathbf{0}$, i.e., $\boldsymbol{\Sigma}_Y - \mathbf{D}$ is positive definite, and hence, nonsingular.
2) We have the following equivalence:

$$\mathbf{K}_{X|VY} \preceq \mathbf{D} \iff \mathbf{K}_{X|V} \preceq \mathbf{F(D)}. \quad (79)$$

The proof of Lemma 3 is given in Appendix F. Using Lemma 3, the minimum mutual information leakage to the

eavesdropper when $(U,V,\mathbf{X})$ is restricted to be jointly Gaussian can be written as follows:

$$L^G = \min_{\substack{U \to V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z} \\ (U,V,\mathbf{X}) \text{ is jointly Gaussian} \\ \mathbf{K}_{X|V} \preceq \mathbf{F(D)}}} I(V;\mathbf{X}) - I(V;\mathbf{Y}|U) + I(\mathbf{X};\mathbf{Z}|U). \quad (80)$$

We note that the minimization in (80) can be written as a minimization of the cost function in (80) over all possible $\mathbf{A}_U, \mathbf{A}_V, \boldsymbol{\Sigma}_U, \boldsymbol{\Sigma}_V$ matrices by expressing $\mathbf{K}_{X|U}$ and $\mathbf{K}_{X|V}$ in terms of $\mathbf{A}_U, \mathbf{A}_V, \boldsymbol{\Sigma}_U, \boldsymbol{\Sigma}_V$. Instead of considering this tedious optimization problem, we consider the following one:

$$\bar{L}^G = \min_{\substack{\mathbf{0} \preceq \mathbf{K}_{X|V} \preceq \mathbf{K}_{X|U} \preceq \mathbf{K}_X \\ \mathbf{K}_{X|V} \preceq \mathbf{F(D)}}} \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{K}_{X|V}|} - \frac{1}{2}\log\frac{|\mathbf{K}_{X|U} + \boldsymbol{\Sigma}_Y|}{|\mathbf{K}_{X|V} + \boldsymbol{\Sigma}_Y|}$$
$$+ \frac{1}{2}\log\frac{|\mathbf{K}_{X|U} + \boldsymbol{\Sigma}_Z|}{|\boldsymbol{\Sigma}_Z|}. \quad (81)$$

We note that due to the Markov chain $U \to V \to \mathbf{X}$, we always have $\mathbf{K}_{X|V} \preceq \mathbf{K}_{X|U}$. A proof of this fact is given in Appendix G. Besides this inequality, $\mathbf{K}_{X|V}$ and $\mathbf{K}_{X|U}$ might have further interdependencies which are not considered in the optimization problem in (81). Since neglecting these further interdependencies among $\mathbf{K}_{X|U}$ and $\mathbf{K}_{X|V}$ enlarges the feasible set of the optimization problem in (80), we have, in general,

$$L^G \geq \bar{L}^G. \quad (82)$$

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 4:

$$L^G = \bar{L}^G. \quad (83)$$

The proof of Lemma 4 is given in Appendix H.

Now we study the optimization problem $\bar{L}^G$ in (81) 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 5: If $\mathbf{K}^*_{X|V}$ and $\mathbf{K}^*_{X|U}$ are the minimizers for the optimization problem $\bar{L}^G$, they need to satisfy

$$(\mathbf{K}^*_{X|V} + \boldsymbol{\Sigma}_Y)^{-1} + \mathbf{M}_U + \mathbf{M}_D = (\mathbf{K}^*_{X|V})^{-1} \quad (84)$$

$$(\mathbf{K}^*_{X|U} + \boldsymbol{\Sigma}_Z)^{-1} + \mathbf{M}_X = (\mathbf{K}^*_{X|U} + \boldsymbol{\Sigma}_Y)^{-1} + \mathbf{M}_U \quad (85)$$

$$\mathbf{M}_U(\mathbf{K}^*_{X|U} - \mathbf{K}^*_{X|V}) = (\mathbf{K}^*_{X|U} - \mathbf{K}^*_{X|V})\mathbf{M}_U = \mathbf{0} \quad (86)$$

$$\mathbf{M}_D(\mathbf{F(D)} - \mathbf{K}^*_{X|V}) = (\mathbf{F(D)} - \mathbf{K}^*_{X|V})\mathbf{M}_D = \mathbf{0} \quad (87)$$

$$\mathbf{M}_X(\mathbf{K}_X - \mathbf{K}^*_{X|U}) = (\mathbf{K}_X - \mathbf{K}^*_{X|U})\mathbf{M}_X = \mathbf{0} \quad (88)$$

for some positive semidefinite matrices $\mathbf{M}_U, \mathbf{M}_D, \mathbf{M}_X$.

The proof of Lemma 5 is given in Appendix I.

Next, we use channel enhancement [19]. In particular, we enhance the legitimate user's side information as follows:

$$(\mathbf{K}_{X|U}^* + \tilde{\boldsymbol{\Sigma}}_Y)^{-1} = (\mathbf{K}_{X|U}^* + \boldsymbol{\Sigma}_Y)^{-1} + \mathbf{M}_U. \tag{89}$$

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

Lemma 6: We have the following facts.
1) $\mathbf{0} \preceq \tilde{\boldsymbol{\Sigma}}_Y$
2) $\tilde{\boldsymbol{\Sigma}}_Y \preceq \boldsymbol{\Sigma}_Y, \tilde{\boldsymbol{\Sigma}}_Y \preceq \boldsymbol{\Sigma}_Z$
3) $(\mathbf{K}_{X|V}^* + \tilde{\boldsymbol{\Sigma}}_Y)^{-1} = (\mathbf{K}_{X|V}^* + \boldsymbol{\Sigma}_Y)^{-1} + \mathbf{M}_U$
4) $(\mathbf{K}_{X|U}^* + \tilde{\boldsymbol{\Sigma}}_Y)^{-1}(\mathbf{K}_{X|V}^* + \tilde{\boldsymbol{\Sigma}}_Y) = (\mathbf{K}_{X|U}^* + \boldsymbol{\Sigma}_Y)^{-1}(\mathbf{K}_{X|V}^* + \boldsymbol{\Sigma}_Y)$
5) $(\mathbf{K}_{X|U}^* + \tilde{\boldsymbol{\Sigma}}_Y)^{-1}(\mathbf{K}_X + \tilde{\boldsymbol{\Sigma}}_Y) = (\mathbf{K}_{X|U}^* + \boldsymbol{\Sigma}_Z)^{-1}(\mathbf{K}_X + \boldsymbol{\Sigma}_Z)$
6) $(\mathbf{K}_{X|V}^* + \tilde{\boldsymbol{\Sigma}}_Y)^{-1}(\mathbf{F}(\mathbf{D}) + \tilde{\boldsymbol{\Sigma}}_Y) = (\mathbf{K}_{X|V}^*)^{-1}\mathbf{F}(\mathbf{D})$.

The proof of Lemma 6 is given in Appendix J. Using this new covariance $\tilde{\boldsymbol{\Sigma}}_Y$, we define the *enhanced* side information at the legitimate user $\tilde{\mathbf{Y}}$ as follows:

$$\tilde{\mathbf{Y}} = \mathbf{X} + \tilde{\mathbf{N}}_Y \tag{90}$$

where $\tilde{\mathbf{N}}_Y$ is a zero-mean Gaussian random vector with covariance matrix $\tilde{\boldsymbol{\Sigma}}_Y$. Since we have $\tilde{\boldsymbol{\Sigma}}_Y \preceq \boldsymbol{\Sigma}_Y$ and $\tilde{\boldsymbol{\Sigma}}_Y \preceq \boldsymbol{\Sigma}_Z$ as stated in the second statement of Lemma 6, without loss of generality, we can assume that the following Markov chain exists:

$$\mathbf{X} \to \tilde{\mathbf{Y}} \to \mathbf{Y}, \mathbf{Z}. \tag{91}$$

Assuming that the Markov chain in (91) 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:

$$\bar{L} = \min_{\substack{U \to V \to \mathbf{X} \to \tilde{\mathbf{Y}} \to \mathbf{Y}, \mathbf{Z} \\ \mathbf{K}_{X|VY} \preceq \mathbf{D}}} I(V; \mathbf{X}) - I(V; \tilde{\mathbf{Y}}|U) + I(\mathbf{X}; \mathbf{Z}|U). \tag{92}$$

We note that we have $I(V; \mathbf{Y}|U) \leq I(V; \tilde{\mathbf{Y}}|U)$ due to the Markov chain in (91), which leads to the following fact:

$$L^G = \bar{L}^G \geq L(0, 1) \geq \bar{L}. \tag{93}$$

Moreover, unlike the original optimization problem $L(0, 1)$ in (74), we can find the minimizer of the new optimization problem $\bar{L}$ explicitly, as stated in the following lemma.

Lemma 7:

$$\bar{L} = \frac{1}{2} \log \frac{|\mathbf{K}_X|}{|\mathbf{F}(\mathbf{D})|} - \frac{1}{2} \log \frac{|\mathbf{K}_X + \tilde{\boldsymbol{\Sigma}}_Y|}{|\mathbf{F}(\mathbf{D}) + \tilde{\boldsymbol{\Sigma}}_Y|} + \frac{1}{2} \log \frac{|\mathbf{K}_X + \boldsymbol{\Sigma}_Z|}{|\boldsymbol{\Sigma}_Z|}. \tag{94}$$

We note that Lemma 7 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 $\bar{L}$. The proof of Lemma 7 is given in Appendix K.

Next, we show that indeed $L^G = \bar{L}^G = \bar{L}$ which, in view of (93), will imply $L(0, 1) = \bar{L} = \bar{L}^G = L^G$. To this end, using Lemma 7, we have

$$\bar{L} = \frac{1}{2} \log \frac{|\mathbf{K}_X|}{|\mathbf{F}(\mathbf{D})|} - \frac{1}{2} \log \frac{|\mathbf{K}_X + \tilde{\boldsymbol{\Sigma}}_Y|}{|\mathbf{F}(\mathbf{D}) + \tilde{\boldsymbol{\Sigma}}_Y|} + \frac{1}{2} \log \frac{|\mathbf{K}_X + \boldsymbol{\Sigma}_Z|}{|\boldsymbol{\Sigma}_Z|} \tag{95}$$

$$= \frac{1}{2} \log \frac{|\mathbf{K}_X|}{|\mathbf{K}_{X|V}^*|} - \frac{1}{2} \log \frac{|\mathbf{K}_X + \tilde{\boldsymbol{\Sigma}}_Y|}{|\mathbf{K}_{X|V}^* + \tilde{\boldsymbol{\Sigma}}_Y|} + \frac{1}{2} \log \frac{|\mathbf{K}_X + \boldsymbol{\Sigma}_Z|}{|\boldsymbol{\Sigma}_Z|} \tag{96}$$

$$= \frac{1}{2} \log \frac{|\mathbf{K}_X|}{|\mathbf{K}_{X|V}^*|} - \frac{1}{2} \log \frac{|\mathbf{K}_{X|U}^* + \tilde{\boldsymbol{\Sigma}}_Y|}{|\mathbf{K}_{X|V}^* + \tilde{\boldsymbol{\Sigma}}_Y|} + \frac{1}{2} \log \frac{|\mathbf{K}_{X|U}^* + \boldsymbol{\Sigma}_Z|}{|\boldsymbol{\Sigma}_Z|} \tag{97}$$

$$= \frac{1}{2} \log \frac{|\mathbf{K}_X|}{|\mathbf{K}_{X|V}^*|} - \frac{1}{2} \log \frac{|\mathbf{K}_{X|U}^* + \boldsymbol{\Sigma}_Y|}{|\mathbf{K}_{X|V}^* + \boldsymbol{\Sigma}_Y|} + \frac{1}{2} \log \frac{|\mathbf{K}_{X|U}^* + \boldsymbol{\Sigma}_Z|}{|\boldsymbol{\Sigma}_Z|} \tag{98}$$

$$= \bar{L}^G \tag{99}$$

$$= L^G \tag{100}$$

where (96) comes from the last statement of Lemma 6, (97) follows from the fifth statement of Lemma 6, and (98) comes from the fourth statement of Lemma 6. In view of (93), (100) 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. GENERAL CASE

We now consider the general case where the side information are given by

$$\mathbf{Y} = \mathbf{H}_Y \mathbf{X} + \mathbf{N}_Y \tag{101}$$

$$\mathbf{Z} = \mathbf{H}_Z \mathbf{X} + \mathbf{N}_Z \tag{102}$$

where without loss of generality, we can assume that the covariance matrices of Gaussian vectors $\mathbf{N}_Y$ and $\mathbf{N}_Z$ are given by identity matrices. We denote the singular value decomposition of $\mathbf{H}_Y$ and $\mathbf{H}_Z$ by $\mathbf{H}_Y = \mathbf{Q}_Y \boldsymbol{\Lambda}_Y \mathbf{R}_Y^\top$ and $\mathbf{H}_Z = \mathbf{Q}_Z \boldsymbol{\Lambda}_Z \mathbf{R}_Z^\top$, respectively. Since any invertible transformation applied to the side information does not change the rate, information leakage, and distortion region, the side information given by (101)–(102) and the side information obtained by multiplying (101)–(102) by $\mathbf{Q}_Y^\top, \mathbf{Q}_Z^\top$, respectively, yield the same rate, information leakage, and distortion region. In other words, the side information given by (101)–(102) and the side information given by

$$\bar{\mathbf{Y}} = \boldsymbol{\Lambda}_Y \mathbf{R}_Y^\top \mathbf{X} + \bar{\mathbf{N}}_Y \tag{103}$$

$$\bar{\mathbf{Z}} = \boldsymbol{\Lambda}_Z \mathbf{R}_Z^\top \mathbf{X} + \bar{\mathbf{N}}_Z \tag{104}$$

yield the same rate, information leakage, and distortion region, where the covariance matrices of $\bar{\mathbf{N}}_Y, \bar{\mathbf{N}}_Z$ are given by identity matrices. Next, we claim that there is no loss of generality to assume that the side information $\bar{\mathbf{Y}}$ and $\bar{\mathbf{Z}}$ have the same length as

the source $\mathbf{X}$. To this end, assume that the length of $\bar{\mathbf{Y}}$ is smaller than the length of $\mathbf{X}$. In this case, simply, we can concatenate $\bar{\mathbf{Y}}$ with some zero vector to ensure that both $\bar{\mathbf{Y}}$ and $\mathbf{X}$ have the same length. Next, assume that the length of $\bar{\mathbf{Y}}$ is larger than the length of $\mathbf{X}$. In this case, $\mathbf{\Lambda}_Y$ will definitely have at least $\text{length}(\bar{\mathbf{Y}}) - \text{length}(\mathbf{X})$ diagonal elements which are zero, and hence the corresponding entries in $\bar{\mathbf{Y}}$ will come from only the noise. Since noise components are independent, dropping these elements of $\bar{\mathbf{Y}}$ does not change the rate, information leakage, and distortion region. Thus, without loss of generality, we can assume that $\text{length}(\bar{\mathbf{Y}}) = \text{length}(\mathbf{X})$, and hence without loss of generality, we can assume that $\mathbf{\Lambda}_Y$ is a square matrix. The same argument applies to the eavesdropper's side information, and hence, without loss of generality, we can also assume that $\mathbf{\Lambda}_Z$ is a square matrix. Next, we define the following side information:

$$\bar{\mathbf{Y}}_\alpha = (\mathbf{\Lambda}_Y + \alpha\mathbf{I})\mathbf{R}_Y^\top \mathbf{X} + \bar{\mathbf{N}}_Y \tag{105}$$

$$\bar{\mathbf{Z}}_\alpha = (\mathbf{\Lambda}_Z + \alpha\mathbf{I})\mathbf{R}_Z^\top \mathbf{X} + \bar{\mathbf{N}}_Z \tag{106}$$

where $\alpha > 0$. We note that $(\mathbf{\Lambda}_Y + \alpha\mathbf{I})$ and $(\mathbf{\Lambda}_Y + \alpha\mathbf{I})$ are invertible matrices. Since multiplying the side information in (105)–(102) by some invertible matrices does not change the rate, information leakage, and distortion region, the side information in (105)–(106) and the following side information:

$$\bar{\bar{\mathbf{Y}}}_\alpha = \mathbf{X} + \bar{\mathbf{N}}_{Y,\alpha} \tag{107}$$

$$\bar{\bar{\mathbf{Z}}}_\alpha = \mathbf{X} + \bar{\mathbf{N}}_{Z,\alpha} \tag{108}$$

have the same rate, information leakage, and distortion region, where the covariance matrices of $\bar{\mathbf{N}}_{Y,\alpha}$ and $\bar{\mathbf{N}}_{Z,\alpha}$ are given by

$$\mathbf{\Sigma}_{Y,\alpha} = \mathbf{R}_Y(\mathbf{\Lambda}_Y + \alpha\mathbf{I})^{-2}\mathbf{R}_Y^\top \tag{109}$$

$$\mathbf{\Sigma}_{Z,\alpha} = \mathbf{R}_Z(\mathbf{\Lambda}_Z + \alpha\mathbf{I})^{-2}\mathbf{R}_Z^\top \tag{110}$$

respectively. For a given distortion constraint $\mathbf{D}$, we denote the rate and information leakage region for the side information model given in (101)–(102) by $\mathcal{R}_o(\mathbf{D})$, where the subscript o stands for the "original system," and for the side information model given in (107)–(108) by $\mathcal{R}_\alpha(\mathbf{D})$. We have the following relationship between $\mathcal{R}_o(\mathbf{D})$ and $\mathcal{R}_\alpha(\mathbf{D})$.

Lemma 8:

$$\mathcal{R}_o(\mathbf{D}) \subseteq \lim_{\alpha \to 0} \mathcal{R}_\alpha(\mathbf{D}). \tag{111}$$

The proof of Lemma 8 is given in Appendix L. Next, using Theorem 4, we obtain an outer bound for the region $\lim_{\alpha \to 0} \mathcal{R}_\alpha(\mathbf{D})$, where this outer bound also serves as an outer bound for the region $\mathcal{R}_o(\mathbf{D})$ due to Lemma 8. The corresponding result is stated in the following theorem.

Theorem 6: If $\mathbf{D} \preceq \mathbf{K}_{X|Y}$, any $(R, I_e) \in \mathcal{R}_o(\mathbf{D})$ satisfies

$$R \geq \frac{1}{2}\log\frac{|\mathbf{K}_{X|Y}|}{|\mathbf{D}|}$$

$$= \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{F}_o(\mathbf{D})|} - \frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{K}_X\mathbf{H}_Y^\top + \mathbf{I}|}{|\mathbf{H}_Y\mathbf{F}_o(\mathbf{D})\mathbf{H}_Y^\top + \mathbf{I}|} \tag{112}$$

$$I_e \geq \min_{\substack{0 \preceq \mathbf{K}_{X|V} \preceq \mathbf{K}_{X|U} \preceq \mathbf{K}_X \\ \mathbf{K}_{X|V} \preceq \mathbf{F}_o(\mathbf{D})}} \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{K}_{X|V}|}$$

$$- \frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{K}_{X|U}\mathbf{H}_Y^\top + \mathbf{I}|}{|\mathbf{H}_Y\mathbf{K}_{X|V}\mathbf{H}_Y^\top + \mathbf{I}|} + \frac{1}{2}\log|\mathbf{H}_Y\mathbf{K}_{X|U}\mathbf{H}_Y^\top + \mathbf{I}| \tag{113}$$

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

The proof of Theorem 6 is given in Appendix M. We prove Theorem 6 in two steps. In the first step, by using Theorem 4, we obtain an outer bound for the region $\mathcal{R}_\alpha(\mathbf{D})$, and in the second step, we obtain the limit of this outer bound as $\alpha \to 0$. As the outer bound in Theorem 6 basically comes from the outer bound in Theorem 4, all our previous comments and remarks about Theorem 4 are also valid for the outer bound in Theorem 6. Similar to Theorem 4, Theorem 6 also provides the minimum information leakage to the eavesdropper when the rate constraint on the transmitter is removed. Denoting the corresponding minimum information leakage by $I_e^{\min}(\mathbf{D})$, we have the following theorem.

Theorem 7: If $\mathbf{D} \preceq \mathbf{K}_{X|Y}$, we have

$$I_e^{\min}(\mathbf{D}) \geq \min_{\substack{0 \preceq \mathbf{K}_{X|V} \preceq \mathbf{K}_{X|U} \preceq \mathbf{K}_X \\ \mathbf{K}_{X|V} \preceq \mathbf{F}_o(\mathbf{D})}} \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{K}_{X|V}|}$$

$$- \frac{1}{2}\log\frac{|\mathbf{H}_Y\mathbf{K}_{X|U}\mathbf{H}_Y^\top + \mathbf{I}|}{|\mathbf{H}_Y\mathbf{K}_{X|V}\mathbf{H}_Y^\top + \mathbf{I}|} + \frac{1}{2}\log|\mathbf{H}_Y\mathbf{K}_{X|U}\mathbf{H}_Y^\top + \mathbf{I}| \tag{114}$$

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

As Theorem 7 basically comes from Theorem 5, all our previous comments and remarks about Theorem 5 are also valid for Theorem 7.

VI. Conclusion

In this paper, we study secure lossy source coding for vector Gaussian sources, where the transmitter sends information about the source in a way that the legitimate user can reconstruct the source within a distortion level by using its side information. Meanwhile, the transmitter wants to keep the mutual information leakage to the eavesdropper to a minimum, where the eavesdropper also has a side information about the source. We obtain an outer bound for the achievable rate, mutual information leakage, and distortion region. 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.

APPENDIX A
PROOF OF (40)

We first define the following function:

$$R(D) = \min_{\substack{V \to X \to Y,Z \\ \sigma^2_{X|VY} \leq D}} I(X; V, Z) \tag{115}$$

which is monotonically decreasing, continuous, and convex in D. Next, we note that when an instantaneous encoding scheme is used, the minimum-mean-square-error estimator is given by

$$\hat{X}_i = E[X_i | g_1(X_1), \ldots, g_n(X_n), Y^n] \tag{116}$$
$$= E[X_i | g_i(X_i), Y_i] \tag{117}$$

where (117) comes from the independence of $(X_i, g_i(X_i), Y_i)$ across time. Consequently, when an instantaneous encoding scheme is used, the minimum-mean-square-error is given by

$$\sigma^2_{X_i | g_i(X_i) Y_i} = E\left[(X_i - E[X_i | g_i(X_i), Y_i])^2 \right]. \tag{118}$$

Assume that there exists an instantaneous encoding scheme that achieves the distortion level D:

$$\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} \sigma^2_{X_i | g_i(X_i) Y_i} \leq D. \tag{119}$$

We now obtain a lower bound for the minimum information leakage for this instantaneous encoding scheme as follows:

$$\lim_{n \to \infty} \frac{1}{n} I(X^n; M, Z^n)$$
$$= \lim_{n \to \infty} \frac{1}{n} I(X^n; g_1(X_1), \ldots, g_n(X_n), Z^n) \tag{120}$$
$$= \lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} I(X_i; g_i(X_i), Z_i) \tag{121}$$
$$= \lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} I(X_i; V_i, Z_i) \tag{122}$$
$$\geq \lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} R\left(\sigma^2_{X_i | V_i Y_i} \right) \tag{123}$$
$$\geq \lim_{n \to \infty} R\left(\frac{1}{n} \sum_{i=1}^{n} \sigma^2_{X_i | V_i Y_i} \right) \tag{124}$$
$$= R\left(\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} \sigma^2_{X_i | V_i Y_i} \right) \tag{125}$$
$$\geq R(D) \tag{126}$$

where (121) comes from the independence of $(X_i, g_i(X_i), Z_i)$ across time, (122) follows by setting $V_i = g_i(X_i)$, (123) comes from the definition of $R(D)$, (124) is due to the convexity of $R(D)$ in D, (125) follows from the fact that $R(D)$ is continuous in D, and (126) comes from (119) and the fact that $R(D)$ is monotonically decreasing in D.

APPENDIX B
PROOF OF LEMMA 1

We first introduce two lemmas that will be used in the proof of Lemma 1. In this appendix, we use notation $A \perp\!\!\!\perp B$ to denote "A and B are independent" to shorten the presentation.

Lemma 9: Let Q, T, W be arbitrary random variables. If we have the Markov chain $Q \to T \to T + W$ and $T \perp\!\!\!\perp W$. Then, we have $(Q, T) \perp\!\!\!\perp W$.

Proof: Since a set of random variables is independent iff their joint characteristic function is the product of their individual characteristic functions, to prove Lemma 9, it is sufficient to show the following:

$$E\left[e^{s_1 Q + s_2 T + s_3 W} \right] = E\left[e^{s_1 Q + s_2 T} \right] E\left[e^{s_3 W} \right] \forall (s_1, s_2, s_3). \tag{127}$$

We can show this as follows:

$$E\left[e^{s_1 Q + s_2 T + s_3 W} \right] = E\left[E\left[e^{s_1 Q + s_2 T + s_3 W} | T \right] \right] \tag{128}$$
$$= E\left[e^{(s_2 - s_3)T} E\left[e^{s_1 Q + s_3(T + W)} | T \right] \right] \tag{129}$$
$$= E\left[e^{(s_2 - s_3)T} E\left[e^{s_1 Q} | T \right] E\left[e^{s_3(T + W)} | T \right] \right] \tag{130}$$
$$= E\left[e^{s_2 T} E\left[e^{s_1 Q} | T \right] E\left[e^{s_3 W} | T \right] \right] \tag{131}$$
$$= E\left[e^{s_2 T} E\left[e^{s_1 Q} | T \right] E\left[e^{s_3 W} \right] \right] \tag{132}$$
$$= E\left[e^{s_2 T} E\left[e^{s_1 Q} | T \right] \right] E\left[e^{s_3 W} \right] \tag{133}$$
$$= E\left[e^{s_1 Q + s_2 T} \right] E\left[e^{s_3 W} \right] \tag{134}$$

where (130) comes from the Markov chain $Q \to T \to T + W$ and (132) follows from the fact that $T \perp\!\!\!\perp W$. Equation (134) implies the independence between (Q, T) and W; completing the proof of Lemma 9. ∎

Lemma 10: Let Q, T, W be random variables satisfying $(T, Q) \perp\!\!\!\perp W$ and $Q \perp\!\!\!\perp T + W$. Then, we have $Q \perp\!\!\!\perp T$.

Proof: Similar to the proof of Lemma 9, here also we use the fact that a set of random variables is independent iff their joint characteristic function is the product of their individual characteristic functions. To this end, since $(T, Q) \perp\!\!\!\perp W$, we have

$$E\left[e^{s_1 W + s_2 T + s_3 Q} \right] = E\left[e^{s_1 W} \right] E\left[e^{s_2 T + s_3 Q} \right] \forall (s_1, s_2, s_3). \tag{135}$$

If we set $s_1 = s_2$ in (135), we obtain

$$E\left[e^{s_2 W + s_2 T + s_3 Q} \right] = E\left[e^{s_2 W} \right] E\left[e^{s_2 T + s_3 Q} \right] \quad \forall (s_2, s_3). \tag{136}$$

On the other hand, since $Q \perp\!\!\!\perp T + W$, we have

$$E\left[e^{s_2 W + s_2 T + s_3 Q} \right] = E\left[e^{s_2(W + T)} \right] E\left[e^{s_3 Q} \right] \tag{137}$$
$$= E\left[e^{s_2 W} \right] E\left[e^{s_2 T} \right] E\left[e^{s_3 Q} \right] \tag{138}$$

where (138) comes from the fact that $T \perp\!\!\!\perp W$. In view of (136) and (138), we have

$$E\left[e^{s_2 T + s_3 Q} \right] = E\left[e^{s_2 T} \right] E\left[e^{s_3 Q} \right] \tag{139}$$

which implies that $T \perp\!\!\!\perp Q$; completing the proof of Lemma 10. ∎

We now prove Lemma 1. We note that we have $I(V; Y|Z) = 0$ iff the Markov chain $V \to Z \to Y$ holds. We prove by contradiction that when $D < \sigma_{x|y}^2$, the Markov chain $V \to Z \to Y$ is not possible. To this end, we note that the side information at the eavesdropper can be written as

$$Z = X + N_y + \tilde{N}_z \tag{140}$$

or in other words, we have $N_z = N_y + \tilde{N}_z$ where $\tilde{N}_z$ is a Gaussian random variable independent of (X, N_y) with variance $\sigma_z^2 - \sigma_y^2 > 0$. Next, we note that the Markov chain $V \to X \to Y \to Z$ implies $(V, X) \perp\!\!\!\perp (N_y, \tilde{N}_z)$ in view of Lemma 9. Since Y, Z are jointly Gaussian, Y can be written as

$$Y = \alpha Z + (Y - \alpha Z) \tag{141}$$

where $\alpha = E[YZ]/E[Z^2]$, and as a consequence of this α choice, we have $Z \perp\!\!\!\perp Y - \alpha Z$. Hence, if we have the Markov chain

$$V \to Z \to Y = \alpha Z + (Y - \alpha Z) \tag{142}$$

then, Lemma 9 implies that $V \perp\!\!\!\perp Y - \alpha Z$, where $Y - \alpha Z$ is

$$Y - \alpha Z = (1 - \alpha)X + (1 - \alpha)N_y - \tilde{N}_z. \tag{143}$$

Since $(V, X) \perp\!\!\!\perp (N_y, \tilde{N}_z)$, we have $(V, X) \perp\!\!\!\perp (1-\alpha)N_y - \tilde{N}_z$, and also $V \perp\!\!\!\perp (1-\alpha)X + (1-\alpha)N_y - \tilde{N}_z$ due to the assumption that the Markov chain $V \to Z \to Y$ holds. Hence, in view of Lemma 10, we have $V \perp\!\!\!\perp X$. Moreover, since we have the Markov chain $V \to X \to Y$, $V \perp\!\!\!\perp X$ implies that $V \perp\!\!\!\perp (X, Y)$. Hence, if $V \perp\!\!\!\perp (X, Y)$, we have $\sigma_{x|vy}^2 = \sigma_{x|y}^2$. However, if $D < \sigma_{x|y}^2$, $V \perp\!\!\!\perp X$ is not feasible, and this implies that the Markov chain $V \to Z \to Y$ is not possible; completing the proof of Lemma 1.

APPENDIX C
PROOF OF (52)

Here, we provide the proof of (52). To this end, we consider a slightly more general case where the joint distribution of the source and side information is given by

$$p(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \prod_{i=1}^{L} p(x_i, y_i, z_i) \tag{144}$$

and the distortion constraint is imposed with a diagonal matrix $\mathbf{D}$ whose diagonal entries are denoted by $D_1, \ldots, D_L$. From Theorem 3, the minimum information leakage is given by

$$I_e^{\min} = \min_{\substack{U \to V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z} \\ \sigma_{X_i|VY^L}^2 \le D_i, i=1,\ldots,L}} I(V; \mathbf{X}) - I(V; \mathbf{Y}|U) + I(\mathbf{X}; \mathbf{Z}|U). \tag{145}$$

We first introduce the following auxiliary random variables:

$$U_i = UY^{i-1}Z_{i+1}^L, \qquad i = 1, \ldots, L \tag{146}$$
$$V_i = VY^{i-1}X_{i+1}^L, \qquad i = 1, \ldots, L \tag{147}$$

which satisfy the Markov chain

$$U_i \to V_i \to X_i \to Y_i, Z_i \tag{148}$$

which follows from (144) and the Markov chain $U \to V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z}$.

Next, we introduce the following two lemmas.

Lemma 11([2, Lemma 7]): Let S^n, T^n be length-n random vectors, and W be an arbitrary random variable. We have

$$\sum_{i=1}^{n} I(T_{i+1}^n; S_i|WS^{i-1}) = \sum_{i=1}^{n} I(S^{i-1}; T_i|WT_{i+1}^n). \tag{149}$$

Using Lemma 11, the following lemma can be proved.
Lemma 12:

$$I(W; S^n) - I(W; T^n) = \sum_{i=1}^{n} I(W; S_i|S^{i-1}T_{i+1}^n) - I(W; T_i|S^{i-1}T_{i+1}^n). \tag{150}$$

Now, we proceed with (145) as follows:

$$I_e^{\min}$$

$$= \min_{\substack{U \to V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z} \\ \sigma_{X_i|VY^L}^2 \le D_i, i=1,\ldots,L}} I(V; \mathbf{X}) - I(V; \mathbf{Y}|U) + I(\mathbf{X}; \mathbf{Z}|U) \tag{151}$$

$$= \min_{\substack{U \to V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z} \\ \sigma_{X_i|VY^L}^2 \le D_i, i=1,\ldots,L}} I(V; \mathbf{X}) - I(V; \mathbf{Y}) + I(U; \mathbf{Y}) - I(U; \mathbf{Z}) + I(\mathbf{X}; \mathbf{Z}) \tag{152}$$

$$= \min_{\substack{U \to V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z} \\ \sigma_{X_i|VY^L}^2 \le D_i, i=1,\ldots,L}} \sum_{i=1}^{L} I(V; X_i|Y^{i-1}, X_{i+1}^L) - I(V; Y_i|Y^{i-1}, X_{i+1}^L) + I(U; Y_i|Y^{i-1}, Z_{i+1}^L) - I(U; Z_i|Y^{i-1}, Z_{i+1}^L) + I(\mathbf{X}; \mathbf{Z}) \tag{153}$$

$$= \min_{\substack{U \to V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z} \\ \sigma_{X_i|VY^L}^2 \le D_i, i=1,\ldots,L}} \sum_{i=1}^{L} I(V; X_i|Y^{i-1}, X_{i+1}^L) - I(V; Y_i|Y^{i-1}, X_{i+1}^L) + I(U; Y_i|Y^{i-1}, Z_{i+1}^L) - I(U; Z_i|Y^{i-1}, Z_{i+1}^L) + I(X_i; Z_i) \tag{154}$$

$$= \min_{\substack{U \to V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z} \\ \sigma_{X_i|VY^L}^2 \le D_i, i=1,\ldots,L}} \sum_{i=1}^{L} I(Y^{i-1}, X_{i+1}^L, V; X_i) - I(Y^{i-1}, X_{i+1}^L, V; Y_i) + I(Y^{i-1}, Z_{i+1}^L, U; Y_i) - I(Y^{i-1}, Z_{i+1}^L, U; Z_i) + I(X_i; Z_i) \tag{155}$$

$$= \min_{\substack{U \to V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z} \\ \sigma_{X_i|VY^L}^2 \le D_i, i=1,\ldots,L}} \sum_{i=1}^{L} I(V_i; X_i) - I(V_i; Y_i) + I(U_i; Y_i) - I(U_i; Z_i) + I(X_i; Z_i) \tag{156}$$

$$= \min_{\substack{U \to V \to \mathbf{X} \to \mathbf{Y}, \mathbf{Z} \\ \sigma_{X_i|VY^L}^2 \le D_i, i=1,\ldots,L}} \sum_{i=1}^{L} I(V_i; X_i) - I(V_i; Y_i|U_i) + I(X_i; Z_i|U_i) \tag{157}$$

$$\ge \min_{\substack{U_i \to V_i \to X_i \to Y_i, Z_i \\ \sigma_{X_i|V_iY_i}^2 \le D_i, i=1,\ldots,L}} \sum_{i=1}^{L} I(V_i; X_i) - I(V_i; Y_i|U_i) + I(X_i; Z_i|U_i) \tag{158}$$

where (152) comes from the Markov chain $U \rightarrow V \rightarrow \mathbf{X} \rightarrow \mathbf{Y}, \mathbf{Z}$, (153) follows from Lemma 12, (154) and (155) are due to (144), (156) follows from the definitions of U_i, V_i in (146) and (147), respectively, (157) comes from (148), and (158) follows from

$$\sigma^2_{X_i|VY^L} \geq \sigma^2_{X_i|VY^LX^L_{i+1}} \qquad (159)$$

$$= \sigma^2_{X_i|VY^iX^L_{i+1}} \qquad (160)$$

$$= \sigma^2_{X_i|V_iY_i} \qquad (161)$$

where (159) follows from the fact that conditioning reduces MMSE (see Appendix G for a proof), (160) comes from the following Markov chain:

$$X_i, V, Y^i \rightarrow X^L_{i+1} \rightarrow Y^L_{i+1} \qquad (162)$$

which is a consequence of (144) and the Markov chain $U \rightarrow V \rightarrow \mathbf{X} \rightarrow \mathbf{Y}, \mathbf{Z}$, and (161) is due to the definition of V_i given in (147). Hence, (158) implies that when the joint distribution of the source and side information can be factorized as in (144), the minimum information leakage is given by

$$I^{\min}_e = \min_{\substack{U_i \rightarrow V_i \rightarrow X_i \rightarrow Y_i, Z_i \\ \sigma^2_{X_i|V_iY_i} \leq D_i, \, i=1,\ldots,L}} \sum^L_{i=1} I(V_i; X_i) - I(V_i; Y_i|U_i)$$
$$+ I(X_i; Z_i|U_i). \qquad (163)$$

We now specialize (163) for the case given in Example 2, where $L = 2$ and we have the following Markov chains:

$$X_1 \rightarrow Y_1 \rightarrow Z_1 \qquad (164)$$

$$X_2 \rightarrow Z_2 \rightarrow Y_2. \qquad (165)$$

Under these conditions, $I^{\min}_e$ is given by

$$I^{\min}_e = I^{\min}_{e1} + I^{\min}_{e2} \qquad (166)$$

where $I^{\min}_{e\ell}, \ell = 1, 2$ is given by

$$I^{\min}_{e\ell} = \min_{(U_\ell, V_\ell) \in \mathcal{G}_\ell} I(V_\ell; X_\ell) - I(V_\ell; Y_\ell|U_\ell) + I(X_\ell; Z_\ell|U_\ell) \qquad (167)$$

where $\mathcal{G}_\ell = \{(U_\ell, V_\ell) : U_\ell \rightarrow V_\ell \rightarrow X_\ell \rightarrow Y_\ell \rightarrow Z_\ell, \sigma^2_{X_\ell|V_\ell Y_\ell} \leq D_\ell\}$. Using the Markov chains

$$U_1 \rightarrow V_1 \rightarrow X_1 \rightarrow Y_1 \rightarrow Z_1 \qquad (168)$$

$$U_2 \rightarrow V_2 \rightarrow X_2 \rightarrow Z_2 \rightarrow Y_2 \qquad (169)$$

in $I^{\min}_{e,1}$ and $I^{\min}_{e,2}$, respectively, we obtain

$$I^{\min}_{e1} = \min_{\substack{V_1 \rightarrow X_1 \rightarrow Y_1 \rightarrow Z_1 \\ \sigma^2_{X_1|V_1Y_1} \leq D_1}} I(V_1; X_1) - I(V_1; Y_1) + I(X_1; Z_1) \qquad (170)$$

$$I^{\min}_{e.2} = \min_{\substack{V_2 \rightarrow X_2 \rightarrow Z_2 \rightarrow Y_2 \\ \sigma^2_{X_2|V_2Y_2} \leq D_2}} I(V_2; X_2) + I(X_2; Z_2|V_2). \qquad (171)$$

Plugging (170) and (171) into (166), we obtain the desired result in (52); completing the proof.

APPENDIX D
PROOFS OF (53) AND (54)

We first prove (53). To this end, we note that when the joint distribution of the source and side information is given by

$$p(\mathbf{x}, \mathbf{y}, \mathbf{z}) = \prod^L_{i=1} p(x_i, y_i, z_i) \qquad (172)$$

and the distortion constraint is imposed by a diagonal matrix $\mathbf{D}$ with diagonal entries $D_1, \ldots, D_L$, the minimum information leakage is given by

$$I^{\min}_e = \min_{\substack{U_i \rightarrow V_i \rightarrow X_i \rightarrow Y_i, Z_i \\ \sigma^2_{X_i|V_iY_i} \leq D_i, \, i=1,\ldots,L}} \sum^L_{i=1} I(V_i; X_i) - I(V_i; Y_i|U_i)$$
$$+ I(X_i; Z_i|U_i) \qquad (173)$$

as shown in Appendix C (in particular, see (163)). When we set $U = \phi$, in other words, when we set $U_1 = \phi, \ldots, U_L = \phi$, (173) reduces to

$$I^{\min - \phi}_e = \min_{\substack{V_i \rightarrow X_i \rightarrow Y_i, Z_i \\ \sigma^2_{X_i|V_iY_i} \leq D_i, \, i=1,\ldots,L}} \sum^L_{i=1} I(V_i; X_i) - I(V_i; Y_i)$$
$$+ I(X_i; Z_i) \qquad (174)$$

which is the desired result in (53).

Next, we prove (54) by using (173). When we set $U = V$, in other words, when we set $U_1 = V_1, \ldots, U_L = V_L$ in (173), we obtain

$$I^{\min}_e = \min_{\substack{U_i \rightarrow V_i \rightarrow X_i \rightarrow Y_i, Z_i \\ \sigma^2_{X_i|V_iY_i} \leq D_i, \, i=1,\ldots,L}} \sum^L_{i=1} I(V_i; X_i) + I(X_i; Z_i|V_i)$$
$$\qquad (175)$$

which is the desired result in (54).

APPENDIX E
PROOF OF LEMMA 2

We note that since $\mathbf{X}, \mathbf{Y}$ are jointly Gaussian, we have [20, p. 155]

$$\mathbf{K}_{X|Y} = \mathbf{K}_X - \mathbf{K}_{XY}\mathbf{K}^{-1}_Y\mathbf{K}_{YX} \qquad (176)$$

$$= \mathbf{K}_X - \mathbf{K}_X(\mathbf{K}_X + \mathbf{\Sigma}_Y)^{-1}\mathbf{K}_X \qquad (177)$$

$$= \mathbf{K}_X(\mathbf{K}_X + \mathbf{\Sigma}_Y)^{-1}\mathbf{\Sigma}_Y \qquad (178)$$

where (177) comes from the fact that $\mathbf{Y} = \mathbf{X} + \mathbf{N}_Y$. Next, we have the following chain of equalities:

$$\frac{|\mathbf{K}_X(\mathbf{K}_X + \mathbf{\Sigma}_Y)^{-1}|}{|\mathbf{F}(\mathbf{D})(\mathbf{F}(\mathbf{D}) + \mathbf{\Sigma}_Y)^{-1}|}$$

$$= \frac{|\mathbf{K}_X(\mathbf{K}_X + \mathbf{\Sigma}_Y)^{-1}\mathbf{\Sigma}_Y|}{|\mathbf{F}(\mathbf{D})(\mathbf{F}(\mathbf{D}) + \mathbf{\Sigma}_Y)^{-1}\mathbf{\Sigma}_Y|} \qquad (179)$$

$$= \frac{|\mathbf{K}_{X|Y}|}{|(\mathbf{\Sigma}_Y(\mathbf{\Sigma}_Y - \mathbf{D})^{-1}\mathbf{\Sigma}_Y - \mathbf{\Sigma}_Y)\mathbf{\Sigma}^{-1}_Y(\mathbf{\Sigma}_Y - \mathbf{D})|} \qquad (180)$$

$$= \frac{|\mathbf{K}_{X|Y}|}{|\mathbf{D}|} \qquad (181)$$

where (180) follows from the definition of $\mathbf{F}(\mathbf{D})$, i.e., $\mathbf{F}(\mathbf{D}) = \mathbf{\Sigma}_Y(\mathbf{\Sigma}_Y - \mathbf{D})^{-1}\mathbf{\Sigma}_Y - \mathbf{\Sigma}_Y$. Equation (181) implies (72); completing the proof of Lemma 2.

APPENDIX F
PROOF OF LEMMA 3

We first prove the first statement of the lemma. To this end, using (178), we have

$$\mathbf{K}_{X|Y} = \mathbf{K}_X(\mathbf{K}_X + \boldsymbol{\Sigma}_Y)^{-1}\boldsymbol{\Sigma}_Y \qquad (184)$$
$$= \boldsymbol{\Sigma}_Y - \boldsymbol{\Sigma}_Y(\mathbf{K}_X + \boldsymbol{\Sigma}_Y)^{-1}\boldsymbol{\Sigma}_Y. \qquad (185)$$

Hence, using (185), the constraint $\mathbf{D} \preceq \mathbf{K}_{X|Y}$ can be expressed as

$$\mathbf{D} \preceq \boldsymbol{\Sigma}_Y - \boldsymbol{\Sigma}_Y(\mathbf{K}_X + \boldsymbol{\Sigma}_Y)^{-1}\boldsymbol{\Sigma}_Y \qquad (186)$$

which is

$$\boldsymbol{\Sigma}_Y(\mathbf{K}_X + \boldsymbol{\Sigma}_Y)^{-1}\boldsymbol{\Sigma}_Y \preceq \boldsymbol{\Sigma}_Y - \mathbf{D} \qquad (187)$$

where $\boldsymbol{\Sigma}_Y(\mathbf{K}_X + \boldsymbol{\Sigma}_Y)^{-1}\boldsymbol{\Sigma}_Y \succ \mathbf{0}$ implying $\boldsymbol{\Sigma}_Y - \mathbf{D} \succ \mathbf{0}$. Hence, $\boldsymbol{\Sigma}_Y - \mathbf{D}$ is nonsingular, and $(\boldsymbol{\Sigma}_Y - \mathbf{D})^{-1}$ exists.

Next, we prove the second statement of the lemma. To this end, we note that since $(V, \mathbf{X}, \mathbf{Y})$ are jointly Gaussian, $\mathbf{Y} = \mathbf{X} + \mathbf{N}_Y$, and V is independent of $\mathbf{N}_Y$, $\mathbf{K}_{X|VY}$ is given by [20, p. 155]

$$\mathbf{K}_{X|VY} = \mathbf{K}_X - [\mathbf{K}_{XV}\,\mathbf{K}_X]\,\mathbf{M}^{-1}\,[\,\mathbf{K}_{XV}\,\,\mathbf{K}_X\,]^\top \qquad (188)$$

where $\mathbf{M}$ is given by
$$\mathbf{M} = \begin{bmatrix} \mathbf{K}_V & \mathbf{K}_{VX} \\ \mathbf{K}_{XV} & \mathbf{K}_Y \end{bmatrix}. \qquad (189)$$

Using block matrix inversion lemma [21, p. 45], $\mathbf{M}^{-1}$ can be obtained as

$$\mathbf{M}^{-1}$$
$$= \begin{bmatrix} \mathbf{K}_V^{-1} + \mathbf{K}_V^{-1}\mathbf{K}_{VX}\boldsymbol{\Delta}_M^{-1}\mathbf{K}_{XV}\mathbf{K}_V^{-1} & -\mathbf{K}_V^{-1}\mathbf{K}_{VX}\boldsymbol{\Delta}_M^{-1} \\ -\boldsymbol{\Delta}_M^{-1}\mathbf{K}_{XV}\mathbf{K}_V^{-1} & \boldsymbol{\Delta}_M^{-1} \end{bmatrix}$$
$$(190)$$

where $\boldsymbol{\Delta}_M$ is given by

$$\boldsymbol{\Delta}_M = \mathbf{K}_Y - \mathbf{K}_{XV}\mathbf{K}_V^{-1}\mathbf{K}_{VX} \qquad (191)$$
$$= \mathbf{K}_X - \mathbf{K}_{XV}\mathbf{K}_V^{-1}\mathbf{K}_{VX} + \boldsymbol{\Sigma}_Y \qquad (192)$$
$$= \mathbf{K}_{X|V} + \boldsymbol{\Sigma}_Y \qquad (193)$$

where the last equality follows from the fact that $\mathbf{K}_{X|V} = \mathbf{K}_X - \mathbf{K}_{XV}\mathbf{K}_V^{-1}\mathbf{K}_{VX}$. Using (190) and (193), we obtain

$$[\mathbf{K}_{XV}\,\mathbf{K}_X]\,\mathbf{M}^{-1} = [\boldsymbol{\Sigma}_Y\boldsymbol{\Delta}_M^{-1}\mathbf{K}_{XV}\mathbf{K}_V^{-1}\,\,\mathbf{I} - \boldsymbol{\Sigma}_Y\boldsymbol{\Delta}_M^{-1}] \quad (194)$$

using this in conjunction with (193), we obtain

$$[\mathbf{K}_{XV}\,\mathbf{K}_X]\mathbf{M}^{-1}[\mathbf{K}_{XV}\,\mathbf{K}_X]^\top$$
$$= \mathbf{K}_X - \boldsymbol{\Sigma}_Y + \boldsymbol{\Sigma}_Y\boldsymbol{\Delta}_M^{-1}\boldsymbol{\Sigma}_Y. \quad (195)$$

Using (195) in (188), we have

$$\mathbf{K}_{X|VY} = \boldsymbol{\Sigma}_Y - \boldsymbol{\Sigma}_Y\boldsymbol{\Delta}_M^{-1}\boldsymbol{\Sigma}_Y \qquad (196)$$
$$= \boldsymbol{\Sigma}_Y - \boldsymbol{\Sigma}_Y(\mathbf{K}_{X|V} + \boldsymbol{\Sigma}_Y)^{-1}\boldsymbol{\Sigma}_Y \qquad (197)$$

where (197) follows from (193). Thus, using (197), the constraint $\mathbf{K}_{X|VY} \preceq \mathbf{D}$ can be expressed as follows:

$$\boldsymbol{\Sigma}_Y - \boldsymbol{\Sigma}_Y(\mathbf{K}_{X|V} + \boldsymbol{\Sigma}_Y)^{-1}\boldsymbol{\Sigma}_Y \preceq \mathbf{D} \qquad (198)$$

from which, since $\boldsymbol{\Sigma}_Y - \mathbf{D} \succ \mathbf{0}$, the following order can be obtained:

$$\mathbf{K}_{X|V} \preceq \boldsymbol{\Sigma}_Y(\boldsymbol{\Sigma}_Y - \mathbf{D})^{-1}\boldsymbol{\Sigma}_Y - \boldsymbol{\Sigma}_Y = \mathbf{F}(\mathbf{D}) \qquad (199)$$

which completes the proof of Lemma 3.

APPENDIX G
CONDITIONING REDUCES MMSE

Here, we prove that conditioning reduces MMSE. To this end, we introduce the following lemma.

Lemma 13: Let $\mathbf{U}$ and $\mathbf{V}$ be any two n-dimensional random vectors and $g : \mathbb{R}^n \to \mathbb{R}^n$. Then,

$$E\left[g(\mathbf{V})g^\top(\mathbf{V})|\mathbf{U} = \mathbf{u}\right]$$
$$\succeq E\left[g(\mathbf{V})|\mathbf{U} = \mathbf{u}\right]E\left[g^\top(\mathbf{V})|\mathbf{U} = \mathbf{u}\right]. (200)$$

Proof: The proof of this lemma comes from the fact given in (182)–(183), at the bottom of this page. ∎
We now prove the fact that conditioning reduces MMSE.
Lemma 14: If $U \to V \to \mathbf{X}$, then $\mathbf{K}_{X|V} \preceq \mathbf{K}_{X|U}$.
Proof: We have

$$\mathbf{K}_{X|V} = E\left[\mathbf{X}\mathbf{X}^\top\right] - E\left[E\left[\mathbf{X}|\mathbf{V}\right]E\left[\mathbf{X}^\top|\mathbf{V}\right]\right] \qquad (201)$$
$$= E\left[\mathbf{X}\mathbf{X}^\top\right] - E\left[E\left[E\left[\mathbf{X}|\mathbf{V}\right]E\left[\mathbf{X}^\top|\mathbf{V}\right]|\mathbf{U}\right]\right] \qquad (202)$$
$$\preceq E\left[\mathbf{X}\mathbf{X}^\top\right] - E\left[E\left[E\left[\mathbf{X}|\mathbf{V}\right]|\mathbf{U}\right]E\left[E\left[\mathbf{X}^\top|\mathbf{V}\right]|\mathbf{U}\right]\right]$$
$$(203)$$
$$= E\left[\mathbf{X}\mathbf{X}^\top\right] - E\left[E\left[\mathbf{X}|\mathbf{U}\right]E\left[\mathbf{X}^\top|\mathbf{U}\right]\right] \qquad (204)$$

where (203) comes from Lemma 13 and (204) comes from the following fact:

$$E\left[E\left[\mathbf{X}|\mathbf{V}\right]|\mathbf{U}\right] = E\left[\mathbf{X}|\mathbf{U}\right] \qquad (205)$$

which is a consequence of the Markov chain $U \to V \to \mathbf{X}$. ∎

$$\mathbf{0} \preceq E\left[\left(g(\mathbf{V}) - E\left[g(\mathbf{V})|\mathbf{U} = \mathbf{u}\right]\right)\left(g(\mathbf{V}) - E\left[g(\mathbf{V})|\mathbf{U} = \mathbf{u}\right]\right)^\top|\mathbf{U} = \mathbf{u}\right] \qquad (182)$$
$$= E\left[g(\mathbf{V})g^\top(\mathbf{V})|\mathbf{U} = \mathbf{u}\right] - E\left[g(\mathbf{V})|\mathbf{U} = \mathbf{u}\right]E\left[g^\top(\mathbf{V})|\mathbf{U} = \mathbf{u}\right] \qquad (183)$$

We now prove Lemma 4. Since any jointly Gaussian $(U, V, \mathbf{X})$ triple satisfying the Markov chain $U \rightarrow V \rightarrow \mathbf{X}$ also satisfies $\mathbf{K}_{X|V} \preceq \mathbf{K}_{X|U}$ due to Lemma 14, the feasible set of $\bar{L}^G$ already contains all jointly Gaussian (U, V) pairs satisfying the Markov chain $U \rightarrow V \rightarrow \mathbf{X}$. Hence, we have $L^G \geq \bar{L}^G$. Next, we show that $\bar{L}^G \geq L^G$ to complete the proof of Lemma 4. To do so, we need to show that for any jointly Gaussian $(U, V, \mathbf{X})$ with conditional covariance matrices $\mathbf{K}_{X|U}$ and $\mathbf{K}_{X|V}$ satisfying $\mathbf{0} \preceq \mathbf{K}_{X|V} \preceq \mathbf{K}_{X|U} \preceq \mathbf{K}_X$ and $\mathbf{K}_{X|V} \preceq \mathbf{F}(\mathbf{D})$, there exists another jointly Gaussian (U^G, V^G) pair such that this pair has the following properties:

1) $\mathbf{K}_{X|V^G} = \mathbf{K}_{X|V}$.
2) $\mathbf{K}_{X|U^G} = \mathbf{K}_{X|U}$.
3) $U^G \rightarrow V^G \rightarrow \mathbf{X}$.

To this end, we note that (U^G, V^G) can be represented as

$$V^G = \mathbf{A}_V \mathbf{X} + \mathbf{N}_V \tag{206}$$
$$U^G = \mathbf{A}_U \mathbf{X} + \mathbf{N}_U \tag{207}$$

where $(\mathbf{N}_U, \mathbf{N}_V)$ and $\mathbf{X}$ are independent, $\mathbf{N}_U, \mathbf{N}_V$ are zero-mean Gaussian random vectors with identity covariance matrices. The cross covariance of $\mathbf{N}_U$ and $\mathbf{N}_V$ is given by $\mathbf{\Sigma}_{UV} = E\left[\mathbf{N}_U \mathbf{N}_V^\top\right]$, which needs to be selected accordingly to ensure that we have the following Markov chain:

$$U^G \rightarrow V^G \rightarrow \mathbf{X}. \tag{208}$$

The conditional covariance $\mathbf{K}_{X|V^G}$ is given by [20, p. 155]

$$\mathbf{K}_{X|V^G} = \mathbf{K}_X - \mathbf{K}_{XV^G} \mathbf{K}_{V^G}^{-1} \mathbf{K}_{V^G X}. \tag{209}$$

Since we are seeking a V^G such that $\mathbf{K}_{X|V^G} = \mathbf{K}_{X|V}$, we set $\mathbf{K}_{X|V^G} = \mathbf{K}_{X|V}$ in (209) yielding

$$\mathbf{K}_{X|V} = \mathbf{K}_X - \mathbf{K}_{XV^G} \mathbf{K}_{V^G}^{-1} \mathbf{K}_{V^G X} \tag{210}$$
$$= \mathbf{K}_X - \mathbf{K}_X \mathbf{A}_V^\top (\mathbf{A}_V \mathbf{K}_X \mathbf{A}_V^\top + \mathbf{I})^{-1} \mathbf{A}_V \mathbf{K}_X \tag{211}$$

which is equivalent to

$$\mathbf{K}_X^{-1}(\mathbf{K}_X - \mathbf{K}_{X|V})\mathbf{K}_X^{-1} = \mathbf{A}_V^\top (\mathbf{A}_V \mathbf{K}_X \mathbf{A}_V^\top + \mathbf{I})^{-1} \mathbf{A}_V. \tag{212}$$

Next, we note the Woodbury matrix identity [22].

Lemma 15 ([22, p. 17]):

$$\left(\mathbf{A} + \mathbf{C}\mathbf{B}\mathbf{C}^\top\right)^{-1}$$
$$= \mathbf{A}^{-1} - \mathbf{A}^{-1}\mathbf{C}\left(\mathbf{B}^{-1} + \mathbf{C}^\top \mathbf{A}^{-1} \mathbf{C}\right)^{-1} \mathbf{C}^\top \mathbf{A}^{-1}. \tag{213}$$

Using Woodbury matrix identity, we obtain

$$\left(\mathbf{A}_V \mathbf{K}_X \mathbf{A}_V^\top + \mathbf{I}\right)^{-1} = \mathbf{I} - \mathbf{A}_V (\mathbf{K}_X^{-1} + \mathbf{A}_V^\top \mathbf{A}_V)^{-1} \mathbf{A}_V^\top \tag{214}$$

using which in (212), we obtain

$$\mathbf{K}_X^{-1}(\mathbf{K}_X - \mathbf{K}_{X|V})\mathbf{K}_X^{-1}$$
$$= \mathbf{A}_V^\top \left[\mathbf{I} - \mathbf{A}_V (\mathbf{K}_X^{-1} + \mathbf{A}_V^\top \mathbf{A}_V)^{-1} \mathbf{A}_V^\top\right] \mathbf{A}_V \tag{215}$$
$$= \mathbf{A}_V^\top \mathbf{A}_V - \mathbf{A}_V^\top \mathbf{A}_V (\mathbf{K}_X^{-1} + \mathbf{A}_V^\top \mathbf{A}_V)^{-1} \mathbf{A}_V^\top \mathbf{A}_V \tag{216}$$
$$= \mathbf{A}_V^\top \mathbf{A}_V$$
$$\quad - \mathbf{A}_V^\top \mathbf{A}_V (\mathbf{K}_X^{-1} + \mathbf{A}_V^\top \mathbf{A}_V)^{-1} \left(\mathbf{K}_X^{-1} + \mathbf{A}_V^\top \mathbf{A}_V - \mathbf{K}_X^{-1}\right) \tag{217}$$
$$= \mathbf{A}_V^\top \mathbf{A}_V (\mathbf{K}_X^{-1} + \mathbf{A}_V^\top \mathbf{A}_V)^{-1} \mathbf{K}_X^{-1} \tag{218}$$
$$= \left(\mathbf{K}_X^{-1} + \mathbf{A}_V^\top \mathbf{A}_V - \mathbf{K}_X^{-1}\right) \left(\mathbf{K}_X^{-1} + \mathbf{A}_V^\top \mathbf{A}_V\right)^{-1} \mathbf{K}_X^{-1} \tag{219}$$
$$= \mathbf{K}_X^{-1} - \mathbf{K}_X^{-1}(\mathbf{K}_X^{-1} + \mathbf{A}_V^\top \mathbf{A}_V)^{-1} \mathbf{K}_X^{-1} \tag{220}$$

which implies

$$\mathbf{K}_{X|V} = \left(\mathbf{K}_X^{-1} + \mathbf{A}_V^\top \mathbf{A}_V\right)^{-1} \tag{221}$$

which, in turn, implies

$$\mathbf{A}_V^\top \mathbf{A}_V = \mathbf{K}_{X|V}^{-1} - \mathbf{K}_X^{-1}. \tag{222}$$

Hence, if we select $\mathbf{A}_V$ as satisfying (222), we obtain $\mathbf{K}_{X|V^G} = \mathbf{K}_{X|V}$. Similarly, if we select $\mathbf{A}_U$ to satisfy

$$\mathbf{A}_U^\top \mathbf{A}_U = \mathbf{K}_{X|U}^{-1} - \mathbf{K}_X^{-1} \tag{223}$$

then, we also have $\mathbf{K}_{X|U^G} = \mathbf{K}_{X|U}$.

Next, we will explicitly construct $\mathbf{A}_V$ and $\mathbf{A}_U$ matrices to satisfy (222) and (223), respectively. To this end, we introduce the following lemma, which will be used subsequently.

Lemma 16 ([23]): Let $\mathbf{A}, \mathbf{B}$ be two real symmetric positive semidefinite matrices. Then, there exists a nonsingular matrix $\mathbf{W}$ such that

$$\mathbf{A} = \mathbf{W}^\top \mathbf{\Lambda}_A \mathbf{W} \tag{224}$$
$$\mathbf{B} = \mathbf{W}^\top \mathbf{\Lambda}_B \mathbf{W} \tag{225}$$

where $\mathbf{\Lambda}_A$ and $\mathbf{\Lambda}_B$ are diagonal matrices.

Lemma 16 states that two real symmetric positive semi-definite matrices can be diagonalized simultaneously. Using this fact in (222)–(223), we obtain

$$\mathbf{K}_{X|V}^{-1} - \mathbf{K}_X^{-1} = \mathbf{W}^\top \mathbf{\Lambda}_V^2 \mathbf{W} \tag{226}$$
$$\mathbf{K}_{X|U}^{-1} - \mathbf{K}_X^{-1} = \mathbf{W}^\top \mathbf{\Lambda}_U^2 \mathbf{W} \tag{227}$$

for some nonsingular matrix $\mathbf{W}$, and diagonal matrices $\mathbf{\Lambda}_U, \mathbf{\Lambda}_V$. Since $\mathbf{K}_{X|V} \preceq \mathbf{K}_{X|U}$, we have $\mathbf{K}_{X|V}^{-1} \succeq \mathbf{K}_{X|U}^{-1}$, which, in view of (226)–(227) imply

$$\mathbf{W}^\top \left(\mathbf{\Lambda}_V^2 - \mathbf{\Lambda}_U^2\right) \mathbf{W} \succeq \mathbf{0}. \tag{228}$$

Since $\mathbf{W}$ is nonsingular, (228) implies that

$$\mathbf{\Lambda}_V \succeq \mathbf{\Lambda}_U. \tag{229}$$

Finally, we choose

$$\mathbf{A}_V = \mathbf{\Lambda}_V \mathbf{W} \tag{230}$$
$$\mathbf{A}_U = \mathbf{\Lambda}_U \mathbf{W} \tag{231}$$

which, in view of (222)–(223) and (226)–(227), imply $\mathbf{K}_{X|V^G} = \mathbf{K}_{X|V}$ and $\mathbf{K}_{X|U^G} = \mathbf{K}_{X|U}$.

Next, we show that a proper selection of the cross-covariance matrix $\mathbf{\Sigma}_{UV}$ would yield the desired Markov chain

$$U^G \to V^G \to \mathbf{X}. \tag{232}$$

To this end, we introduce the following matrix:

$$\mathbf{A}_{UV} = \mathbf{\Lambda}_U \mathbf{\Lambda}_V^\dagger \tag{233}$$

where the diagonal matrix $\mathbf{\Lambda}_V^\dagger$ is defined as follows:

$$\Lambda_{V,ii}^\dagger = \begin{cases} \frac{1}{\Lambda_{V,ii}}, & if\ \Lambda_{V,ii} \neq 0 \\ 0, & \text{otherwise.} \end{cases} \tag{234}$$

Since $\mathbf{\Lambda}_U \preceq \mathbf{\Lambda}_V$, we have $\mathbf{\Lambda}_U \mathbf{\Lambda}_V^\dagger \mathbf{\Lambda}_V = \mathbf{\Lambda}_U$. Hence, we have

$$\mathbf{A}_{UV} \mathbf{A}_V = \mathbf{A}_U. \tag{235}$$

We also note the following:

$$\mathbf{A}_{UV} \mathbf{A}_{UV}^\top = \mathbf{\Lambda}_U \left(\mathbf{\Lambda}_V^\dagger\right)^2 \mathbf{\Lambda}_U \preceq \mathbf{I} \tag{236}$$

since $\mathbf{\Lambda}_U \preceq \mathbf{\Lambda}_V$.

Now, we are ready to show that U^G and V^G satisfy the Markov chain $U^G \to V^G \to \mathbf{X}$ by specifying $\mathbf{\Sigma}_{UV}$. We set $\mathbf{N}_U$ as follows:

$$\mathbf{N}_U = \mathbf{A}_{UV} \mathbf{N}_V + \tilde{\mathbf{N}} \tag{237}$$

where $\tilde{\mathbf{N}}$ is a zero-mean Gaussian random vector with covariance matrix $\mathbf{I} - \mathbf{A}_{UV} \mathbf{A}_{UV}^\top$, and is independent of $\mathbf{N}_V$. In view of (237), we have

$$U^G = \mathbf{A}_U \mathbf{X} + \mathbf{N}_U \tag{238}$$
$$= \mathbf{A}_{UV} \mathbf{A}_V \mathbf{X} + \mathbf{A}_{UV} \mathbf{N}_V + \tilde{\mathbf{N}} \tag{239}$$
$$= \mathbf{A}_{UV} V^G + \tilde{\mathbf{N}} \tag{240}$$

which implies that (U^G, V^G) satisfy the Markov chain $U^G \to V^G \to \mathbf{X}$; completing the proof.

APPENDIX I
PROOF OF LEMMA 5

The Lagrangian for the optimization problem $\bar{L}^G$ is given as follows:

$$\begin{aligned} \mathcal{L}\left(\bar{L}^G\right) = &\frac{1}{2} \log \frac{|\mathbf{K}_X|}{|\mathbf{K}_{X|V}|} - \frac{1}{2} \log \frac{|\mathbf{K}_{X|U} + \mathbf{\Sigma}_Y|}{|\mathbf{K}_{X|V} + \mathbf{\Sigma}_Y|} \\ &+ \frac{1}{2} \log \frac{|\mathbf{K}_{X|U} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} - \text{tr}(\mathbf{M}_0 \mathbf{K}_{X|V}) \\ &- \text{tr}(\mathbf{M}_U(\mathbf{K}_{X|U} - \mathbf{K}_{X|V})) \\ &- \text{tr}(\mathbf{M}_X(\mathbf{K}_X - \mathbf{K}_{X|U})) - \text{tr}(\mathbf{M}_D(\mathbf{F}(\mathbf{D}) - \mathbf{K}_{X|V})) \end{aligned} \tag{241}$$

where the positive semidefinite matrices $\mathbf{M}_0, \mathbf{M}_U, \mathbf{M}_D, \mathbf{M}_X$ are the Lagrange multipliers for the following constraints:

$$\mathbf{K}_{X|V} \succeq \mathbf{0} \tag{242}$$
$$\mathbf{K}_{X|U} - \mathbf{K}_{X|V} \succeq \mathbf{0} \tag{243}$$
$$\mathbf{F}(\mathbf{D}) - \mathbf{K}_{X|V} \succeq \mathbf{0} \tag{244}$$
$$\mathbf{K}_X - \mathbf{K}_{X|U} \succeq \mathbf{0} \tag{245}$$

respectively. Let $\mathbf{K}_{X|V}^*$ and $\mathbf{K}_{X|U}^*$ be the minimizers of the optimization problem $\bar{L}^G$. Using (241), the KKT conditions can be found as follows:

$$\nabla_{\mathbf{K}_{X|V}} \mathcal{L}(\bar{L}^G)\,|_{\mathbf{K}_{X|V}=\mathbf{K}_{X|V}^*} = \mathbf{0} \tag{246}$$
$$\nabla_{\mathbf{K}_{X|U}} \mathcal{L}(\bar{L}^G)\,|_{\mathbf{K}_{X|U}=\mathbf{K}_{X|U}^*} = \mathbf{0} \tag{247}$$
$$\text{tr}(\mathbf{M}_0 \mathbf{K}_{X|V}^*) = 0 \tag{248}$$
$$\text{tr}(\mathbf{M}_U(\mathbf{K}_{X|U}^* - \mathbf{K}_{X|V}^*)) = 0 \tag{249}$$
$$\text{tr}(\mathbf{M}_D(\mathbf{F}(\mathbf{D}) - \mathbf{K}_{X|V}^*)) = 0 \tag{250}$$
$$\text{tr}(\mathbf{M}_X(\mathbf{K}_X - \mathbf{K}_{X|U}^*)) = 0. \tag{251}$$

We first note that we have $\mathbf{K}_{X|V}^* \succ \mathbf{0}$, otherwise $\bar{L}^G \to \infty$. Hence, using the fact that if $\mathbf{A} \succeq \mathbf{0}, \mathbf{B} \succeq \mathbf{0}, \text{tr}(\mathbf{AB}) \geq 0$, and (248), we obtain $\mathbf{M}_0 = \mathbf{0}$. Next, using the fact that $\mathbf{M}_0 = \mathbf{0}$ in (246), we obtain the KKT condition given in (84). Equation (247) implies (85). Finally, using the fact that $\mathbf{A} \succeq \mathbf{0}, \mathbf{B} \succeq \mathbf{0}$, $\text{tr}(\mathbf{AB}) = \text{tr}(\mathbf{BA}) \geq 0$ in (249)–(251), we can obtain the KKT conditions given in (86)–(88), respectively.

APPENDIX J
PROOF OF LEMMA 6

We start with the second statement of the lemma. To this end, we note that (85) and (89) imply the following:

$$(\mathbf{K}_{X|U}^* + \tilde{\mathbf{\Sigma}}_Y)^{-1} = (\mathbf{K}_{X|U}^* + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M}_U \tag{252}$$
$$= (\mathbf{K}_{X|U}^* + \mathbf{\Sigma}_Z)^{-1} + \mathbf{M}_X. \tag{253}$$

Next, using the fact that if $\mathbf{A} \succ \mathbf{0}, \mathbf{B} \succ \mathbf{0}$, and $\mathbf{A} \succeq \mathbf{B}$, we have $\mathbf{A}^{-1} \preceq \mathbf{B}^{-1}$ in conjunction with the fact that $\mathbf{M}_U \succeq \mathbf{0}, \mathbf{M}_X \succeq \mathbf{0}$, we can obtain the second statement of the lemma from (252)–(253).

Next, we consider the third statement of the lemma as follows:

$$\mathbf{K}_{X|V}^* + \tilde{\mathbf{\Sigma}}_Y$$
$$= \mathbf{K}_{X|V}^* + \left[(\mathbf{K}_{X|U}^* + \mathbf{\Sigma}_Y)^{-1} + \mathbf{M}_U\right]^{-1} - \mathbf{K}_{X|U}^* \tag{254}$$
$$= \mathbf{K}_{X|V}^* + \left[\mathbf{I} + (\mathbf{K}_{X|U}^* + \mathbf{\Sigma}_Y)\mathbf{M}_U\right]^{-1}(\mathbf{K}_{X|U}^* + \mathbf{\Sigma}_Y)$$
$$\quad - \mathbf{K}_{X|U}^* \tag{255}$$
$$= \mathbf{K}_{X|V}^* + \left[\mathbf{I} + (\mathbf{K}_{X|U}^* - \mathbf{K}_{X|V}^* + \mathbf{K}_{X|V}^* + \mathbf{\Sigma}_Y)\mathbf{M}_U\right]^{-1}$$
$$\quad \times (\mathbf{K}_{X|U}^* + \mathbf{\Sigma}_Y) - \mathbf{K}_{X|U}^* \tag{256}$$
$$= \mathbf{K}_{X|V}^* + \left[\mathbf{I} + (\mathbf{K}_{X|V}^* + \mathbf{\Sigma}_Y)\mathbf{M}_U\right]^{-1}(\mathbf{K}_{X|U}^* + \mathbf{\Sigma}_Y)$$
$$\quad - \mathbf{K}_{X|U}^* \tag{257}$$

$$= \mathbf{K}_{X|V}^* + \left[(\mathbf{K}_{X|V}^* + \boldsymbol{\Sigma}_Y)^{-1} + \mathbf{M}_U \right]^{-1} (\mathbf{K}_{X|V}^* + \boldsymbol{\Sigma}_Y)^{-1}$$
$$\times (\mathbf{K}_{X|U}^* + \boldsymbol{\Sigma}_Y) - \mathbf{K}_{X|U}^* \qquad (258)$$

$$= \mathbf{K}_{X|V}^* + \left[(\mathbf{K}_{X|V}^* + \boldsymbol{\Sigma}_Y)^{-1} + \mathbf{M}_U \right]^{-1} (\mathbf{K}_{X|V}^* + \boldsymbol{\Sigma}_Y)^{-1}$$
$$\times (\mathbf{K}_{X|U}^* - \mathbf{K}_{X|V}^* + \mathbf{K}_{X|V}^* + \boldsymbol{\Sigma}_Y) - \mathbf{K}_{X|U}^* \qquad (259)$$

$$= \mathbf{K}_{X|V}^* + \left[(\mathbf{K}_{X|V}^* + \boldsymbol{\Sigma}_Y)^{-1} + \mathbf{M}_U \right]^{-1} (\mathbf{K}_{X|V}^* + \boldsymbol{\Sigma}_Y)^{-1}$$
$$\times (\mathbf{K}_{X|U}^* - \mathbf{K}_{X|V}^*) + \left[(\mathbf{K}_{X|V}^* + \boldsymbol{\Sigma}_Y)^{-1} + \mathbf{M}_U \right]^{-1}$$
$$- \mathbf{K}_{X|U}^* \qquad (260)$$

$$= \mathbf{K}_{X|V}^* + \left[(\mathbf{K}_{X|V}^* + \boldsymbol{\Sigma}_Y)^{-1} + \mathbf{M}_U \right]^{-1}$$
$$\times \left[(\mathbf{K}_{X|V}^* + \boldsymbol{\Sigma}_Y)^{-1} + \mathbf{M}_U \right] (\mathbf{K}_{X|U}^* - \mathbf{K}_{X|V}^*)$$
$$+ \left[(\mathbf{K}_{X|V}^* + \boldsymbol{\Sigma}_Y)^{-1} + \mathbf{M}_U \right]^{-1} - \mathbf{K}_{X|U}^* \qquad (261)$$

$$= \mathbf{K}_{X|V}^* + (\mathbf{K}_{X|U}^* - \mathbf{K}_{X|V}^*) + \left[(\mathbf{K}_{X|V}^* + \boldsymbol{\Sigma}_Y)^{-1} + \mathbf{M}_U \right]^{-1}$$
$$- \mathbf{K}_{X|U}^* \qquad (262)$$

$$= \left[(\mathbf{K}_{X|V}^* + \boldsymbol{\Sigma}_Y)^{-1} + \mathbf{M}_U \right]^{-1} \qquad (263)$$

where (254) comes from (252), (257) and (261) follow from (86).

Now, we consider the fourth statement of the lemma as follows:

$$(\mathbf{K}_{X|U}^* + \tilde{\boldsymbol{\Sigma}}_Y)^{-1} (\mathbf{K}_{X|V}^* + \tilde{\boldsymbol{\Sigma}}_Y)$$
$$= \mathbf{I} + (\mathbf{K}_{X|U}^* + \tilde{\boldsymbol{\Sigma}}_Y)^{-1} (\mathbf{K}_{X|V}^* - \mathbf{K}_{X|U}^*) \qquad (264)$$
$$= \mathbf{I} + \left[(\mathbf{K}_{X|U}^* + \boldsymbol{\Sigma}_Y)^{-1} + \mathbf{M}_U \right] (\mathbf{K}_{X|V}^* - \mathbf{K}_{X|U}^*)$$
$$\qquad (265)$$
$$= \mathbf{I} + (\mathbf{K}_{X|U}^* + \boldsymbol{\Sigma}_Y)^{-1} (\mathbf{K}_{X|V}^* - \mathbf{K}_{X|U}^*) \qquad (266)$$
$$= (\mathbf{K}_{X|U}^* + \boldsymbol{\Sigma}_Y)^{-1} (\mathbf{K}_{X|V}^* + \boldsymbol{\Sigma}_Y) \qquad (267)$$

where (265) follows from (252), and (266) comes from (86).

Next, we consider the fifth statement of the lemma as follows:

$$(\mathbf{K}_{X|U}^* + \tilde{\boldsymbol{\Sigma}}_Y)^{-1} (\mathbf{K}_X + \tilde{\boldsymbol{\Sigma}}_Y)$$
$$= \mathbf{I} + (\mathbf{K}_{X|U}^* + \tilde{\boldsymbol{\Sigma}}_Y)^{-1} (\mathbf{K}_X - \mathbf{K}_{X|U}^*) \qquad (268)$$
$$= \mathbf{I} + \left[(\mathbf{K}_{X|U}^* + \boldsymbol{\Sigma}_Z)^{-1} + \mathbf{M}_X \right] (\mathbf{K}_X - \mathbf{K}_{X|U}^*) \qquad (269)$$
$$= \mathbf{I} + (\mathbf{K}_{X|U}^* + \boldsymbol{\Sigma}_Z)^{-1} (\mathbf{K}_X - \mathbf{K}_{X|U}^*) \qquad (270)$$
$$= (\mathbf{K}_{X|U}^* + \boldsymbol{\Sigma}_Z)^{-1} (\mathbf{K}_X + \boldsymbol{\Sigma}_Z) \qquad (271)$$

where (269) comes from (253) and (270) is due to (88).

Now, we prove the last statement of the lemma. To this end, we note that the third statement of this lemma and (84) imply the following:

$$(\mathbf{K}_{X|V}^* + \tilde{\boldsymbol{\Sigma}}_Y)^{-1} + \mathbf{M}_D = (\mathbf{K}_{X|V}^*)^{-1} \qquad (272)$$

which will be used in the sequel. Now, the last statement of this lemma follows from

$$(\mathbf{K}_{X|V}^* + \tilde{\boldsymbol{\Sigma}}_Y)^{-1} (\mathbf{F}(\mathbf{D}) + \tilde{\boldsymbol{\Sigma}}_Y)$$
$$= \mathbf{I} + (\mathbf{K}_{X|V}^* + \tilde{\boldsymbol{\Sigma}}_Y)^{-1} (\mathbf{F}(\mathbf{D}) - \mathbf{K}_{X|V}^*) \qquad (273)$$
$$= \mathbf{I} + \left[(\mathbf{K}_{X|V}^*)^{-1} - \mathbf{M}_D \right] (\mathbf{F}(\mathbf{D}) - \mathbf{K}_{X|V}^*) \qquad (274)$$
$$= \mathbf{I} + (\mathbf{K}_{X|V}^*)^{-1} (\mathbf{F}(\mathbf{D}) - \mathbf{K}_{X|V}^*) \qquad (275)$$
$$= (\mathbf{K}_{X|V}^*)^{-1} \mathbf{F}(\mathbf{D}) \qquad (276)$$

where (274) comes from (272) and (275) is due to (87).

Finally, we note that (272) also implies the first statement of the lemma; completing the proof.

APPENDIX K
PROOF OF LEMMA 7

A) Background: We need some properties of the Fisher information and the differential entropy, which are provided next.

Definition 1 ([24, Definition 3]): Let $(\mathbf{U}, \mathbf{X})$ be an arbitrarily correlated length-n random vector pair with well-defined densities. The conditional Fisher information matrix of $\mathbf{X}$ given $\mathbf{U}$ is defined as

$$\mathbf{J}(\mathbf{X}|\mathbf{U}) = E \left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U}) \boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^\top \right] \qquad (277)$$

where the expectation is over the joint density $f(\mathbf{u}, \mathbf{x})$, and the conditional score function $\boldsymbol{\rho}(\mathbf{x}|\mathbf{u})$ is

$$\boldsymbol{\rho}(\mathbf{x}|\mathbf{u}) = \nabla \log f(\mathbf{x}|\mathbf{u}) = \left[\frac{\partial \log f(\mathbf{x}|\mathbf{u})}{\partial x_1} \cdots \frac{\partial \log f(\mathbf{x}|\mathbf{u})}{\partial x_n} \right]^\top. \qquad (278)$$

We first present the conditional form of the Cramer–Rao inequality, which is proved in [24].

Lemma 17 ([24, Lemma 13]): Let $\mathbf{U}, \mathbf{X}$ be arbitrarily correlated random vectors with well-defined densities. Let the conditional covariance matrix of $\mathbf{X}$ be $\text{Cov}(\mathbf{X}|\mathbf{U}) \succ \mathbf{0}$, then we have

$$\mathbf{J}(\mathbf{X}|\mathbf{U}) \succeq \text{Cov}(\mathbf{X}|\mathbf{U})^{-1} \qquad (279)$$

which is satisfied with equality if $(\mathbf{U}, \mathbf{X})$ is jointly Gaussian with conditional covariance matrix $\text{Cov}(\mathbf{X}|\mathbf{U})$.

The following lemma will be used in the upcoming proof. The unconditional version of this lemma, i.e., the case $\mathbf{T} = \phi$, is proved in [24, Lemma 6].

Lemma 18 ([24, Lemma 6]): Let $\mathbf{T}, \mathbf{U}, \mathbf{V}_1, \mathbf{V}_2$ be random vectors such that $(\mathbf{T}, \mathbf{U})$ and $(\mathbf{V}_1, \mathbf{V}_2)$ are independent. Moreover, let $\mathbf{V}_1, \mathbf{V}_2$ be Gaussian random vectors with covariance matrices $\boldsymbol{\Sigma}_1, \boldsymbol{\Sigma}_2$ such that $\mathbf{0} \prec \boldsymbol{\Sigma}_1 \preceq \boldsymbol{\Sigma}_2$. Then, we have

$$\mathbf{J}^{-1}(\mathbf{U} + \mathbf{V}_2|\mathbf{T}) - \boldsymbol{\Sigma}_2 \succeq \mathbf{J}^{-1}(\mathbf{U} + \mathbf{V}_1|\mathbf{T}) - \boldsymbol{\Sigma}_1. \qquad (280)$$

The following lemma will also be used in the upcoming proof.

Lemma 19 ([24, Lemma 8]): Let $\mathbf{K}_1, \mathbf{K}_2$ be positive semidefinite matrices satisfying $\mathbf{0} \preceq \mathbf{K}_1 \preceq \mathbf{K}_2$, and $\mathbf{f}(\mathbf{K})$ be a matrix-valued function such that $\mathbf{f}(\mathbf{K}) \succeq \mathbf{0}$ for $\mathbf{K}_1 \preceq \mathbf{K} \preceq \mathbf{K}_2$. Moreover, $\mathbf{f}(\mathbf{K})$ is assumed to be gradient of a scalar field. Then, we have

$$\int_{\mathbf{K}_1}^{\mathbf{K}_2} \mathbf{f}(\mathbf{K}) d\mathbf{K} \geq 0. \qquad (281)$$

The following generalization of the de Bruijn identity [25], [26] is due to [27], where the unconditional form of this identity, i.e., $\mathbf{U} = \phi$, is proved. Its generalization to this conditional form for an arbitrary $\mathbf{U}$ is rather straightforward, and is given in [24, Lemma 16].

Lemma 20 ([24, Lemma 16]): Let $(\mathbf{U}, \mathbf{X})$ be an arbitrarily correlated random vector pair with finite second order moments, and also be independent of the random vector $\mathbf{N}$ which is zero-mean Gaussian with covariance matrix $\boldsymbol{\Sigma}_N \succ \mathbf{0}$. Then, we have

$$\nabla_{\boldsymbol{\Sigma}_N} h(\mathbf{X} + \mathbf{N} | \mathbf{U}) = \frac{1}{2} \mathbf{J}(\mathbf{X} + \mathbf{N} | \mathbf{U}). \qquad (282)$$

The following lemma provides a connection between the conditional covariance matrix and the Fisher information matrices of a random vector.

Lemma 21: Let $(V, \mathbf{X})$ be two arbitrary random vectors with finite second moments, and $\mathbf{N}$ be a zero-mean Gaussian random vector with covariance matrix $\boldsymbol{\Sigma}_N$. Let $\mathbf{Y} = \mathbf{X} + \mathbf{N}$. Assume $(V, \mathbf{X})$ and $\mathbf{N}$ are independent. We have

$$\mathbf{K}_{X|VY} = \boldsymbol{\Sigma}_N - \boldsymbol{\Sigma}_N \mathbf{J}(\mathbf{X} + \mathbf{N}|V) \boldsymbol{\Sigma}_N. \qquad (283)$$

Lemma 21 is proved in [27] for $V = \phi$. Its generalization to the current conditional form can be obtained by using the conditional Fisher information and Lemma 20.

B) Proof: We first consider the cost function of the optimization problem $\bar{L}$

$$C(\bar{L}) = I(V; \mathbf{X}) - I(V; \tilde{\mathbf{Y}} | U) + I(\mathbf{X}; \mathbf{Z} | U) \qquad (284)$$

$$= I(V; \mathbf{X}) - I(V; \tilde{\mathbf{Y}}) + I(U; \tilde{\mathbf{Y}}) + I(\mathbf{X}; \mathbf{Z}) - I(U; \mathbf{Z}) \qquad (285)$$

$$= I(V; \mathbf{X}) - I(V; \tilde{\mathbf{Y}}) + I(U; \tilde{\mathbf{Y}}, \mathbf{Z}) + I(\mathbf{X}; \mathbf{Z}) - I(U; \mathbf{Z}) \qquad (286)$$

$$= I(V; \mathbf{X}) - I(V; \tilde{\mathbf{Y}}) + I(U; \tilde{\mathbf{Y}} | \mathbf{Z}) + I(\mathbf{X}; \mathbf{Z}) \qquad (287)$$

$$\geq I(V; \mathbf{X}) - I(V; \tilde{\mathbf{Y}}) + I(\mathbf{X}; \mathbf{Z}) \qquad (288)$$

where (285)–(286) come from the following Markov chain:

$$U \to V \to \mathbf{X} \to \tilde{\mathbf{Y}} \to \mathbf{Y}, \mathbf{Z} \qquad (289)$$

and (288) comes from the nonnegativity of the mutual information. On the other hand, (288) can be obtained from (92) by choosing $U = \phi$, i.e., we have

$$\bar{L} \leq \min_{\substack{V \to \mathbf{X} \to \tilde{\mathbf{Y}} \to \mathbf{Y}, \mathbf{Z} \\ \mathbf{K}_{X|VY} \preceq \mathbf{D}}} I(V; \mathbf{X}) - I(V; \tilde{\mathbf{Y}}) + I(\mathbf{X}; \mathbf{Z}). \qquad (290)$$

Hence, (288) and (290) imply the following:

$$\bar{L} = \min_{\substack{V \to \mathbf{X} \to \tilde{\mathbf{Y}} \to \mathbf{Y}, \mathbf{Z} \\ \mathbf{K}_{X|VY} \preceq \mathbf{D}}} I(V; \mathbf{X}) - I(V; \tilde{\mathbf{Y}}) + I(\mathbf{X}; \mathbf{Z}) \qquad (291)$$

$$= \min_{\substack{V \to \mathbf{X} \to \tilde{\mathbf{Y}} \to \mathbf{Y}, \mathbf{Z} \\ \mathbf{K}_{X|VY} \preceq \mathbf{D}}} I(V; \mathbf{X} | \tilde{\mathbf{Y}}) + I(\mathbf{X}; \mathbf{Z}) \qquad (292)$$

where (292) comes from the Markov chain $V \to \mathbf{X} \to \tilde{\mathbf{Y}}$. We note that the optimization problem in (292) is similar to the one we already studied in (67)–(71). Indeed, if the constraint $\mathbf{K}_{X|VY} \preceq \mathbf{D}$ in (292) was $\mathbf{K}_{X|V\tilde{Y}} \preceq \mathbf{D}$, both optimization problems would be identical, and using the analysis in (67)–(71), we could conclude that (292) is minimized by a Gaussian V satisfying $\mathbf{K}_{X|V\tilde{Y}} \preceq \mathbf{D}$. However, the difference between these two constraints necessitates a new proof, and indeed, showing the optimality of Gaussian V for the optimization problem in (292) is not as straightforward as showing the optimality of Gaussian V for the optimization problem in (67).

We find the minimizer for the optimization problem $\bar{L}$ in two steps. In the first step, for a given feasible V, we explicitly construct a feasible Gaussian $\bar{V}$ which provides the same value for the cost function of $\bar{L}$ as the original V does. Thus, this first step implies that restricting V to be Gaussian does not change the optimum value of the optimization problem $\bar{L}$. Consequently, in the second step of the proof, we minimize $\bar{L}$ over all feasible Gaussian V. To this end, we note that the cost function of the optimization problem $\bar{L}$ can be written as

$$C(\bar{L}) = h(\tilde{\mathbf{Y}} | V) - h(\mathbf{X} | V) + c \qquad (293)$$

for some constant c, which is independent of V. From now on, we focus on the difference of the two differential entropy terms in (293). Next, we note that using Lemma 20, we have

$$h(\tilde{\mathbf{Y}} | V) - h(\mathbf{X} | V) = \frac{1}{2} \int_0^{\tilde{\boldsymbol{\Sigma}}_Y} \mathbf{J}(\mathbf{X} + \mathbf{N} | V) d\boldsymbol{\Sigma}_N \qquad (294)$$

where $\mathbf{N}$ is zero-mean Gaussian random vector with covariance matrix $\boldsymbol{\Sigma}_N$ satisfying $\mathbf{0} \preceq \boldsymbol{\Sigma}_N$. Next, we find upper and lower bounds for (294). We note that Lemma 18 implies the following upper bound for $\mathbf{J}(\mathbf{X} + \mathbf{N} | V)$:

$$\mathbf{J}(\mathbf{X} + \mathbf{N} | V) \preceq \left[\mathbf{J}^{-1}(\mathbf{X} | V) + \boldsymbol{\Sigma}_N \right]^{-1}. \qquad (295)$$

Using (295) in (294) in conjunction with Lemma 19, we obtain

$$h(\tilde{\mathbf{Y}} | V) - h(\mathbf{X} | V) \leq \frac{1}{2} \log \frac{|\mathbf{J}^{-1}(\mathbf{X} | V) + \tilde{\boldsymbol{\Sigma}}_Y|}{|\mathbf{J}^{-1}(\mathbf{X} | V)|}. \qquad (296)$$

We note that due to Lemma 17, we have $\mathbf{J}(\mathbf{X} | V) \succeq \mathbf{K}_{X|V}^{-1} \succ \mathbf{0}$, i.e., (296) is well defined. Similarly, using Lemma 18, we have

$$\mathbf{J}^{-1}(\mathbf{X} + \tilde{\mathbf{N}}_Y | V) - \tilde{\boldsymbol{\Sigma}}_Y \succeq \mathbf{J}^{-1}(\mathbf{X} + \mathbf{N} | V) - \boldsymbol{\Sigma}_N \qquad (297)$$

for all $\boldsymbol{\Sigma}_N \preceq \tilde{\boldsymbol{\Sigma}}_Y$, which implies

$$\mathbf{J}(\mathbf{X} + \mathbf{N} | V) \succeq \left[\mathbf{J}^{-1}(\mathbf{X} + \tilde{\mathbf{N}}_Y | V) - \tilde{\boldsymbol{\Sigma}}_Y + \boldsymbol{\Sigma}_N \right]^{-1}. \qquad (298)$$

Using (298) in (294) in conjunction with Lemma 19, we obtain

$$h(\tilde{\mathbf{Y}} | V) - h(\mathbf{X} | V) \geq \frac{1}{2} \log \frac{|\mathbf{J}^{-1}(\mathbf{X} + \tilde{\mathbf{N}}_Y | V)|}{|\mathbf{J}^{-1}(\mathbf{X} + \tilde{\mathbf{N}}_Y | V) - \tilde{\boldsymbol{\Sigma}}_Y|}. \qquad (299)$$

Now, we rewrite the bounds in (296) and (299). To this end, we define the following function:

$$f(t) = \frac{1}{2} \log \frac{|\mathbf{K}(t) + \tilde{\mathbf{\Sigma}}_Y|}{|\mathbf{K}(t)|}, \quad 0 \le t \le 1 \quad (300)$$

where the matrix $\mathbf{K}(t)$ is given as follows:

$$\mathbf{K}(t) = t\mathbf{J}^{-1}(\mathbf{X}|V) + (1-t)\left[\mathbf{J}^{-1}(\mathbf{X} + \tilde{\mathbf{N}}_Y|V) - \tilde{\mathbf{\Sigma}}_Y\right]. \quad (301)$$

Hence, using $f(t)$ in (300), the bounds in (296) and (299) can be rewritten as follows:

$$f(0) \le h(\tilde{\mathbf{Y}}|V) - h(\mathbf{X}|V) \le f(1). \quad (302)$$

Since $f(t)$ is continuous in t, there exists t^* such that

$$f(t^*) = h(\tilde{\mathbf{Y}}|V) - h(\mathbf{X}|V) \quad (303)$$

$$= \frac{1}{2} \log \frac{|\mathbf{K}(t^*) + \tilde{\mathbf{\Sigma}}_Y|}{|\mathbf{K}(t^*)|} \quad (304)$$

where $\mathbf{K}(t^*)$ is bounded as follows:

$$\mathbf{J}^{-1}(\mathbf{X}|V) \preceq \mathbf{K}(t^*) \preceq \mathbf{J}^{-1}(\mathbf{X} + \tilde{\mathbf{N}}_Y|V) - \tilde{\mathbf{\Sigma}}_Y \quad (305)$$

$$\preceq \mathbf{J}^{-1}(\mathbf{X} + \mathbf{N}_Y|V) - \mathbf{\Sigma}_Y \quad (306)$$

where we used the fact that $0 \le t^* \le 1$ and Lemma 18. Thus, (304) implies that if we pick a Gaussian $\bar{V}$ satisfying $\mathbf{K}_{X|\bar{V}} = \mathbf{K}(t^*)$, it provides the same value for the cost function of $\bar{L}$ as the original V does.

Next, we check whether this Gaussian $\bar{V}$ is feasible, i.e., whether it satisfies $\mathbf{K}_{X|\bar{V}Y} \preceq \mathbf{D}$. To this end, using Lemma 21, we obtain

$$\mathbf{K}_{X|\bar{V}Y} = \mathbf{\Sigma}_Y - \mathbf{\Sigma}_Y \mathbf{J}(\mathbf{Y}|\bar{V})\mathbf{\Sigma}_Y. \quad (307)$$

Since $\bar{V}$ is Gaussian, Lemma 17 implies that

$$\mathbf{J}(\mathbf{Y}|\bar{V}) = \mathbf{K}_{Y|\bar{V}}^{-1} \quad (308)$$

$$= (\mathbf{K}_{X|\bar{V}} + \mathbf{\Sigma}_Y)^{-1} \quad (309)$$

where (309) follows from the fact that $(\bar{V}, \mathbf{X})$ and $\mathbf{N}_Y$ are independent. Moreover, due to (306), we have $\mathbf{K}_{X|\bar{V}} \preceq \mathbf{J}^{-1}(\mathbf{Y}|V) - \mathbf{\Sigma}_Y$, which together with (309) imply the following:

$$\mathbf{J}(\mathbf{Y}|\bar{V}) \succeq \mathbf{J}(\mathbf{Y}|V). \quad (310)$$

Using (310) in (307), we obtain

$$\mathbf{K}_{X|\bar{V}Y} \preceq \mathbf{\Sigma}_Y - \mathbf{\Sigma}_Y \mathbf{J}(\mathbf{Y}|V)\mathbf{\Sigma}_Y \quad (311)$$

$$= \mathbf{K}_{X|VY} \quad (312)$$

$$\preceq \mathbf{D} \quad (313)$$

where (312) follows from Lemma 21 and (313) is due to the assumption that V is feasible, i.e., $\mathbf{K}_{X|VY} \preceq \mathbf{D}$. Equation (313) implies that the constructed Gaussian random vector $\bar{V}$ is feasible, i.e., for each feasible V, there exists a feasible Gaussian $\bar{V}$ which provides the same value for the cost function of $\bar{L}$; completing the first step of the proof.

Hence, in view of this first step of the proof, we can restrict V to be Gaussian which leads to the following form for $\bar{L}$:

$$\bar{L} = \min_{\substack{V \to \mathbf{X} \to \tilde{\mathbf{Y}} \to \mathbf{Y}, \mathbf{Z} \\ V \text{ is Gaussian} \\ \mathbf{K}_{X|VY} \preceq \mathbf{D}}} I(V; \mathbf{X}) - I(V; \tilde{\mathbf{Y}}) + I(\mathbf{X}; \mathbf{Z}) \quad (314)$$

$$= \min_{\substack{V \to \mathbf{X} \to \tilde{\mathbf{Y}} \to \mathbf{Y}, \mathbf{Z} \\ V \text{ is Gaussian} \\ \mathbf{K}_{X|V} \preceq \mathbf{F}(\mathbf{D})}} I(V; \mathbf{X}) - I(V; \tilde{\mathbf{Y}}) + I(\mathbf{X}; \mathbf{Z}) \quad (315)$$

$$= \min_{\mathbf{K}_{X|V} \preceq \mathbf{F}(\mathbf{D})} \frac{1}{2} \log \frac{|\mathbf{K}_X|}{|\mathbf{K}_{X|V}|} - \frac{1}{2} \log \frac{|\mathbf{K}_X + \tilde{\mathbf{\Sigma}}_Y|}{|\mathbf{K}_{X|V} + \tilde{\mathbf{\Sigma}}_Y|}$$
$$+ \frac{1}{2} \log \frac{|\mathbf{K}_X + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \quad (316)$$

$$= \frac{1}{2} \log \frac{|\mathbf{K}_X|}{|\mathbf{F}(\mathbf{D})|} - \frac{1}{2} \log \frac{|\mathbf{K}_X + \tilde{\mathbf{\Sigma}}_Y|}{|\mathbf{F}(\mathbf{D}) + \tilde{\mathbf{\Sigma}}_Y|} + \frac{1}{2} \log \frac{|\mathbf{K}_X + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \quad (317)$$

where (315) follows from Lemma 3, and (317) comes from the fact that

$$\frac{|\mathbf{K}_{X|V} + \tilde{\mathbf{\Sigma}}_Y|}{|\mathbf{K}_{X|V}|} \quad (318)$$

is monotonically decreasing in the positive semidefinite matrices $\mathbf{K}_{X|V}$; completing the proof of Lemma 7.

APPENDIX L
PROOF OF LEMMA 8

We note that due to Theorem 3, we already have single-letter descriptions for the regions $\mathcal{R}_o(\mathbf{D})$ and $\mathcal{R}_\alpha(\mathbf{D})$. Thus, to prove Lemma 8, it suffices to show that for any given feasible (U, V), these two regions satisfy the relationship given in Lemma 8. We first note the following Markov chains:

$$U \to V \to \mathbf{X} \to \bar{\bar{\mathbf{Y}}}_\alpha \to \mathbf{Y} \quad (319)$$

$$U \to V \to \mathbf{X} \to \bar{\bar{\mathbf{Z}}}_\alpha \to \mathbf{Z}. \quad (320)$$

Next, we show that any feasible (U, V) for the region $\mathcal{R}_o(\mathbf{D})$ is also feasible for the region $\lim_{\alpha \to 0} \mathcal{R}_\alpha(\mathbf{D})$. To this end, we note that

$$\mathbf{D} \succeq \mathbf{K}_{X|VY} \quad (321)$$

$$\succeq \mathbf{K}_{X|VY\bar{\mathbf{Y}}_\alpha} \quad (322)$$

$$= \mathbf{K}_{X|V\bar{Y}_\alpha} \quad (323)$$

where (322) is due to the fact that conditioning reduces MMSE and (323) follows from the Markov chain in (319). Moreover, it can be shown that $\lim_{\alpha \to 0} \mathbf{K}_{X|V\bar{Y}_\alpha}$ exists and is equal to $\mathbf{K}_{X|VY}$. Hence, this observation and (323) imply that (U, V) is also feasible for the region $\lim_{\alpha \to 0} \mathcal{R}_\alpha(\mathbf{D})$.

Next, we show that for a given (U, V), any rate inside the region $\mathcal{R}_o(\mathbf{D})$ is also inside $\lim_{\alpha \to 0} \mathcal{R}_\alpha(\mathbf{D})$. To this end, for a given (U, V), we denote the minimum achievable rates in $\mathcal{R}_o(\mathbf{D})$ and $\mathcal{R}_\alpha(\mathbf{D})$ by R_o and R_α, respectively. Due to Theorem 3, we have

$$R_o - R_\alpha = [I(V; \mathbf{X}) - I(V; \mathbf{Y})] - [I(V; \mathbf{X}) - I(V; \bar{\bar{\mathbf{Y}}}_\alpha)] \quad (324)$$

$$= I(V; \bar{\bar{\mathbf{Y}}}_\alpha) - I(V; \mathbf{Y}) \quad (325)$$

$$= I(V; \bar{\bar{\mathbf{Y}}}_\alpha | \mathbf{Y}) \quad (326)$$

$$\ge 0 \quad (327)$$

where (326) comes from the Markov chain in (319). Equation (326) implies that any achievable rate within the region $\mathcal{R}_o(\mathbf{D})$ is also included in the region $\lim_{\alpha \to 0} \mathcal{R}_\alpha(\mathbf{D})$.

Finally, we show that for a given (U, V), any achievable information leakage inside the region $\mathcal{R}_o(\mathbf{D})$ is also inside $\lim_{\alpha \to 0} \mathcal{R}_\alpha(\mathbf{D})$. To this end, for a given (U, V), we denote the minimum information leakage in $\mathcal{R}_o(\mathbf{D})$ and $\mathcal{R}_\alpha(\mathbf{D})$ by $I_{e,o}$ and $I_{e,\alpha}$, respectively. Due to Theorem 3, we have

$$
\begin{aligned}
&I_{e,o} - I_{e,\alpha} \\
&= \left[I(V; \mathbf{X}) - I(V; \mathbf{Y}|U) + I(\mathbf{X}; \mathbf{Z}|U) \right] \\
&\quad - \left[I(V; \mathbf{X}) - I(V; \bar{\bar{\mathbf{Y}}}_\alpha|U) + I(\mathbf{X}; \bar{\bar{\mathbf{Z}}}_\alpha|U) \right] \qquad (328) \\
&= \left[I(V; \bar{\bar{\mathbf{Y}}}_\alpha|U) - I(V; \mathbf{Y}|U) \right] + \left[I(\mathbf{X}; \mathbf{Z}|U) - I(\mathbf{X}; \bar{\bar{\mathbf{Z}}}_\alpha|U) \right] \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (329) \\
&= I(V; \bar{\bar{\mathbf{Y}}}_\alpha|U, \mathbf{Y}) + \left[I(\mathbf{X}; \mathbf{Z}|U) - I(\mathbf{X}; \bar{\bar{\mathbf{Z}}}_\alpha|U) \right] \qquad (330) \\
&\geq I(\mathbf{X}; \mathbf{Z}|U) - I(\mathbf{X}; \bar{\bar{\mathbf{Z}}}_\alpha|U) \qquad (331) \\
&\geq I(\mathbf{X}; \mathbf{Z}) - I(\mathbf{X}; \bar{\bar{\mathbf{Z}}}_\alpha) \qquad (332) \\
&= \frac{1}{2} \log |\mathbf{H}_Z \mathbf{K}_X \mathbf{H}_Z^\top + \mathbf{I}| \\
&\quad - \frac{1}{2} \log \frac{|\mathbf{K}_X + \mathbf{R}_Z(\mathbf{\Lambda}_Z + \alpha \mathbf{I})^{-2} \mathbf{R}_Z^\top|}{|\mathbf{R}_Z(\mathbf{\Lambda}_Z + \alpha \mathbf{I})^{-2} \mathbf{R}_Z^\top|} \qquad (333) \\
&= \frac{1}{2} \log |\mathbf{H}_Z \mathbf{K}_X \mathbf{H}_Z^\top + \mathbf{I}| \\
&\quad - \frac{1}{2} \log \frac{|\mathbf{K}_X + \mathbf{R}_Z(\mathbf{\Lambda}_Z + \alpha \mathbf{I})^{-1} \mathbf{Q}_Z^\top \mathbf{Q}_Z (\mathbf{\Lambda}_Z + \alpha \mathbf{I})^{-1} \mathbf{R}_Z^\top|}{|\mathbf{R}_Z(\mathbf{\Lambda}_Z + \alpha \mathbf{I})^{-1} \mathbf{Q}_Z^\top \mathbf{Q}_Z (\mathbf{\Lambda}_Z + \alpha \mathbf{I})^{-1} \mathbf{R}_Z^\top|} \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (334) \\
&= \frac{1}{2} \log |\mathbf{H}_Z \mathbf{K}_X \mathbf{H}_Z^\top + \mathbf{I}| \\
&\quad - \frac{1}{2} \log |\mathbf{Q}_Z(\mathbf{\Lambda}_Z + \alpha \mathbf{I}) \mathbf{R}_Z^\top \mathbf{K}_X \mathbf{R}_Z (\mathbf{\Lambda}_Z + \alpha \mathbf{I}) \mathbf{Q}_Z^\top + \mathbf{I}| \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (335)
\end{aligned}
$$

where (330) comes from the Markov chain in (319) and (332) follows from the Markov chain in (320). Equation (335) implies that

$$
\begin{aligned}
&\lim_{\alpha \to 0} I_{e,o} - I_{e,\alpha} \\
&\geq \frac{1}{2} \log |\mathbf{H}_Z \mathbf{K}_X \mathbf{H}_Z^\top + \mathbf{I}| \\
&\quad - \lim_{\alpha \to 0} \frac{1}{2} \log |\mathbf{Q}_Z(\mathbf{\Lambda}_Z + \alpha \mathbf{I}) \mathbf{R}_Z^\top \mathbf{K}_X \mathbf{R}_Z (\mathbf{\Lambda}_Z + \alpha \mathbf{I}) \mathbf{Q}_Z^\top + \mathbf{I}| \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad (336) \\
&= \frac{1}{2} \log |\mathbf{H}_Z \mathbf{K}_X \mathbf{H}_Z^\top + \mathbf{I}| \\
&\quad - \frac{1}{2} \log |\mathbf{Q}_Z \mathbf{\Lambda}_Z \mathbf{R}_Z^\top \mathbf{K}_X \mathbf{R}_Z \mathbf{\Lambda}_Z \mathbf{Q}_Z^\top + \mathbf{I}| \qquad (337) \\
&= \frac{1}{2} \log |\mathbf{H}_Z \mathbf{K}_X \mathbf{H}_Z^\top + \mathbf{I}| - \frac{1}{2} \log |\mathbf{H}_Z \mathbf{K}_X \mathbf{H}_Z^\top + \mathbf{I}| \qquad (338) \\
&= 0 \qquad (339)
\end{aligned}
$$

where (337) comes from the continuity of the determinant in positive semidefinite matrices. Equation (339) implies that any achievable information leakage in the region $\mathcal{R}_o(\mathbf{D})$ is also

inside the region $\lim_{\alpha \to 0} \mathcal{R}_\alpha(\mathbf{D})$; completing the proof of Lemma 8.

APPENDIX M
PROOF OF THEOREM 6

We start the proof of Theorem 6 by first expressing Theorem 4 for the side information model given by (107)–(108). In other words, we first provide an outer bound for the region $\mathcal{R}_\alpha(\mathbf{D})$ by using Theorem 4. To this end, to be able to use Theorem 4, we need $\mathbf{D} \preceq \mathbf{K}_{X|\bar{Y}_\alpha}$. However, since we originally have $\mathbf{D} \preceq \mathbf{K}_{X|Y}$ and $\mathbf{K}_{X|\bar{Y}_\alpha} \preceq \mathbf{K}_{X|Y}$, where the latter one follows from the Markov chain $\mathbf{X} \to \bar{\mathbf{Y}}_\alpha \to \mathbf{Y}$ and the fact that conditioning reduces MMSE, $\mathbf{K}_{X|\bar{Y}_\alpha} - \mathbf{D}$ might be indefinite. However, the only place we use the condition $\mathbf{D} \preceq \mathbf{K}_{X|Y}$ is to be able to show the equivalence between $\mathbf{K}_{X|VY} \preceq \mathbf{D}$ and $\mathbf{K}_{X|V} \preceq \mathbf{F}(\mathbf{D})$ for Gaussian V in Lemma 3. In particular, we only need the fact that $\mathbf{\Sigma}_Y - \mathbf{D}$ is nonsingular to show this equivalence, and which is implied by $\mathbf{D} \preceq \mathbf{K}_{X|Y}$. However, still there might be distortion matrices $\mathbf{D}$ for which although we have nonsingular $\mathbf{\Sigma}_Y - \mathbf{D}$, the condition $\mathbf{D} \preceq \mathbf{K}_{X|Y}$ is not satisfied. Hence, if we can find an α^* such that

$$
\mathbf{\Sigma}_{Y,\alpha} - \mathbf{D} \succ \mathbf{0}, \quad 0 < \alpha \leq \alpha^* \qquad (340)
$$

we can still use Theorem 4 to obtain an outer bound for the region $\mathcal{R}_\alpha(\mathbf{D})$. Now, we establish the existence of such an α^*. Using the assumption $\mathbf{D} \preceq \mathbf{K}_{X|Y}$, we have

$$
\mathbf{D} \preceq \mathbf{K}_{X|Y} = (\mathbf{K}_X^{-1} + \mathbf{H}_Y^\top \mathbf{H}_Y)^{-1} \qquad (341)
$$

where the equality follows from (221). Equation (341) implies that

$$
\begin{aligned}
\mathbf{0} &\prec \mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y \qquad (342) \\
&= \mathbf{D}^{-1} - \mathbf{R}_Y \mathbf{\Lambda}_Y^2 \mathbf{R}_Y^\top \qquad (343)
\end{aligned}
$$

where we use the singular value decomposition of $\mathbf{H}_Y$. Thus, since $\mathbf{D}^{-1} - \mathbf{R}_Y \mathbf{\Lambda}_Y^2 \mathbf{R}_Y^\top$ is strictly positive definite, there exists $0 < \beta$ such that

$$
\begin{aligned}
\mathbf{D}^{-1} - \mathbf{R}_Y \mathbf{\Lambda}_Y^2 \mathbf{R}_Y^\top &\succ \beta^2 \mathbf{I} \qquad (344) \\
&= \beta^2 \mathbf{R}_Y \mathbf{R}_Y^\top \qquad (345)
\end{aligned}
$$

which implies

$$
\mathbf{D}^{-1} \succ \mathbf{R}_Y (\mathbf{\Lambda}_Y^2 + \beta^2) \mathbf{R}_Y^\top \qquad (346)
$$

which, in turn, implies the existence of an α^* such that

$$
\mathbf{D}^{-1} \succ \mathbf{R}_Y (\mathbf{\Lambda}_Y + \alpha)^2 \mathbf{R}_Y^\top, \quad 0 < \alpha \leq \alpha^*. \qquad (347)
$$

Hence, using the definition of $\mathbf{\Sigma}_{Y,\alpha}$ in (347), we obtain

$$
\mathbf{D}^{-1} \succ \mathbf{\Sigma}_{Y,\alpha}^{-1}, \quad 0 < \alpha \leq \alpha^* \qquad (348)
$$

which is equivalent to the desired condition in (340) which is needed to use Theorem 4 to obtain an outer bound for the region $\mathcal{R}_\alpha(\mathbf{D})$. Hence, assuming that $0 < \alpha \leq \alpha^*$, an outer bound

for the region $\mathcal{R}_\alpha(\mathbf{D})$ can be written as the union of rate and information leakage (R, I_e) pairs satisfying

$$
\begin{aligned}
R &\geq \frac{1}{2}\log\frac{|\mathbf{K}_{X|\bar{Y}_\alpha}|}{|\mathbf{D}|} \\
&= \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{F}_\alpha(\mathbf{D})|} - \frac{1}{2}\log\frac{|\mathbf{K}_X + \boldsymbol{\Sigma}_{Y,\alpha}|}{|\mathbf{F}_\alpha(\mathbf{D}) + \boldsymbol{\Sigma}_{Y,\alpha}|}
\end{aligned} \tag{349}
$$

$$
\begin{aligned}
I_e \geq \min_{\substack{0 \preceq \mathbf{K}_{X|V} \preceq \mathbf{K}_{X|U} \preceq \mathbf{K}_X \\ \mathbf{K}_{X|V} \preceq \mathbf{F}_\alpha(\mathbf{D})}} &\frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{K}_{X|V}|} \\
&- \frac{1}{2}\log\frac{|\mathbf{K}_{X|U} + \boldsymbol{\Sigma}_{Y,\alpha}|}{|\mathbf{K}_{X|V} + \boldsymbol{\Sigma}_{Y,\alpha}|} + \frac{1}{2}\log\frac{|\mathbf{K}_{X|U} + \boldsymbol{\Sigma}_{Z,\alpha}|}{|\boldsymbol{\Sigma}_{Z,\alpha}|}
\end{aligned} \tag{350}
$$

where $\mathbf{F}_\alpha(\mathbf{D}) = \boldsymbol{\Sigma}_{Y,\alpha}(\boldsymbol{\Sigma}_{Y,\alpha} - \mathbf{D})^{-1}\boldsymbol{\Sigma}_{Y,\alpha} - \boldsymbol{\Sigma}_{Y,\alpha}$. We now find the limiting region that comes from the one described by (349)–(350) as $\alpha \to 0$. To this end, we introduce the following lemma that will be used subsequently.

Lemma 22:

$$
\lim_{\alpha \to 0} \mathbf{K}_{X|\bar{Y}_\alpha} = \mathbf{K}_{X|Y} \tag{351}
$$

$$
\lim_{\alpha \to 0} \mathbf{F}_\alpha(\mathbf{D}) = (\mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y)^{-1}. \tag{352}
$$

The proof of Lemma 22 is given in Appendix N.

We first consider the rate bound in (349) as follows:

$$
\lim_{\alpha \to 0} \frac{1}{2}\log\frac{|\mathbf{K}_{X|\bar{Y}_\alpha}|}{|\mathbf{D}|} = \frac{1}{2}\log\frac{|\mathbf{K}_{X|Y}|}{|\mathbf{D}|} \tag{359}
$$

which follows from the continuity of the determinant in positive semidefinite matrices and (351). Similarly, for the second expression in the rate bound in (349), we have

$$
\begin{aligned}
\lim_{\alpha \to 0} &\frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{F}_\alpha(\mathbf{D})|} - \frac{1}{2}\log\frac{|\mathbf{K}_X + \boldsymbol{\Sigma}_{Y,\alpha}|}{|\mathbf{F}_\alpha(\mathbf{D}) + \boldsymbol{\Sigma}_{Y,\alpha}|} \\
&= \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|(\mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y)^{-1}|} \\
&\quad - \frac{1}{2}\log\frac{|\mathbf{H}_Y \mathbf{K}_X \mathbf{H}_Y^\top + \mathbf{I}|}{|\mathbf{H}_Y(\mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y)^{-1}\mathbf{H}_Y^\top + \mathbf{I}|}
\end{aligned} \tag{360}
$$

which follows from the derivation given by (353)–(358), which is at the bottom of the page. In this derivation, (353) is due to the continuity of the determinant in positive semidefinite matrices and (352), (354) comes from the definition of $\boldsymbol{\Sigma}_{Y,\alpha}$, (357) comes from the continuity of the determinant in positive semidefinite matrices and (352), and (358) is obtained by using the singular value decomposition of $\mathbf{H}_Y$. Hence, (359) and (360) imply that any rate R inside the region $\lim_{\alpha \to 0} \mathcal{R}_\alpha(\mathbf{D})$ satisfies

$$
R \geq \frac{1}{2}\log\frac{|\mathbf{K}_{X|Y}|}{|\mathbf{D}|} \tag{361}
$$

$$
\begin{aligned}
&= \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|(\mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y)^{-1}|} \\
&\quad - \frac{1}{2}\log\frac{|\mathbf{H}_Y \mathbf{K}_X \mathbf{H}_Y^\top + \mathbf{I}|}{|\mathbf{H}_Y(\mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y)^{-1}\mathbf{H}_Y^\top + \mathbf{I}|}.
\end{aligned} \tag{362}
$$

Following a similar analysis, the limit of the information leakage in (350) can be found as

$$
\begin{aligned}
\min_{\substack{0 \preceq \mathbf{K}_{X|V} \preceq \mathbf{K}_{X|U} \preceq \mathbf{K}_X \\ \mathbf{K}_{X|V} \preceq (\mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y)^{-1}}} &\frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{K}_{X|V}|} \\
&- \frac{1}{2}\log\frac{|\mathbf{H}_Y \mathbf{K}_{X|U} \mathbf{H}_Y^\top + \mathbf{I}|}{|\mathbf{H}_Y \mathbf{K}_{X|V} \mathbf{H}_Y^\top + \mathbf{I}|} + \frac{1}{2}\log|\mathbf{H}_Y \mathbf{K}_{X|U} \mathbf{H}_Y^\top + \mathbf{I}|
\end{aligned} \tag{363}
$$

which implies that any information leakage I_e inside the region $\lim_{\alpha \to 0} \mathcal{R}_\alpha(\mathbf{D})$ should be larger than (363); completing the proof of Theorem 6.

APPENDIX N
PROOF OF LEMMA 22

We first prove the following lemma which will be used subsequently.

$$
\lim_{\alpha \to 0} \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|\mathbf{F}_\alpha(\mathbf{D})|} - \frac{1}{2}\log\frac{|\mathbf{K}_X + \boldsymbol{\Sigma}_{Y,\alpha}|}{|\mathbf{F}_\alpha(\mathbf{D}) + \boldsymbol{\Sigma}_{Y,\alpha}|}
$$

$$
= \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|(\mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y)^{-1}|} - \lim_{\alpha \to 0}\frac{1}{2}\log\frac{|\mathbf{K}_X + \boldsymbol{\Sigma}_{Y,\alpha}|}{|\mathbf{F}_\alpha(\mathbf{D}) + \boldsymbol{\Sigma}_{Y,\alpha}|} \tag{353}
$$

$$
= \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|(\mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y)^{-1}|} - \lim_{\alpha \to 0}\frac{1}{2}\log\frac{|\mathbf{K}_X + \mathbf{R}_Y(\boldsymbol{\Lambda}_Y + \alpha\mathbf{I})^{-2}\mathbf{R}_Y^\top|}{|\mathbf{F}_\alpha(\mathbf{D}) + \mathbf{R}_Y(\boldsymbol{\Lambda}_Y + \alpha\mathbf{I})^{-2}\mathbf{R}_Y^\top|} \tag{354}
$$

$$
= \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|(\mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y)^{-1}|} - \lim_{\alpha \to 0}\frac{1}{2}\log\frac{|\mathbf{K}_X + \mathbf{R}_Y(\boldsymbol{\Lambda}_Y + \alpha\mathbf{I})^{-1}\mathbf{Q}_Y^\top \mathbf{Q}_Y(\boldsymbol{\Lambda}_Y + \alpha\mathbf{I})^{-1}\mathbf{R}_Y^\top|}{|\mathbf{F}_\alpha(\mathbf{D}) + \mathbf{R}_Y(\boldsymbol{\Lambda}_Y + \alpha\mathbf{I})^{-1}\mathbf{Q}_Y^\top \mathbf{Q}_Y(\boldsymbol{\Lambda}_Y + \alpha\mathbf{I})^{-1}\mathbf{R}_Y^\top|} \tag{355}
$$

$$
= \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|(\mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y)^{-1}|} - \lim_{\alpha \to 0}\frac{1}{2}\log\frac{|\mathbf{Q}_Y(\boldsymbol{\Lambda}_Y + \alpha\mathbf{I})\mathbf{R}_Y^\top \mathbf{K}_X \mathbf{R}_Y(\boldsymbol{\Lambda}_Y + \alpha\mathbf{I})\mathbf{Q}_Y^\top + \mathbf{I}|}{|\mathbf{Q}_Y(\boldsymbol{\Lambda}_Y + \alpha\mathbf{I})\mathbf{R}_Y^\top \mathbf{F}_\alpha(\mathbf{D})\mathbf{R}_Y(\boldsymbol{\Lambda}_Y + \alpha\mathbf{I})\mathbf{Q}_Y^\top + \mathbf{I}|} \tag{356}
$$

$$
= \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|(\mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y)^{-1}|} - \frac{1}{2}\log\frac{|\mathbf{Q}_Y \boldsymbol{\Lambda}_Y \mathbf{R}_Y^\top \mathbf{K}_X \mathbf{R}_Y \boldsymbol{\Lambda}_Y \mathbf{Q}_Y^\top + \mathbf{I}|}{|\mathbf{Q}_Y \boldsymbol{\Lambda}_Y \mathbf{R}_Y^\top (\mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y)^{-1}\mathbf{R}_Y \boldsymbol{\Lambda}_Y \mathbf{Q}_Y^\top + \mathbf{I}|} \tag{357}
$$

$$
= \frac{1}{2}\log\frac{|\mathbf{K}_X|}{|(\mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y)^{-1}|} - \frac{1}{2}\log\frac{|\mathbf{H}_Y \mathbf{K}_X \mathbf{H}_Y^\top + \mathbf{I}|}{|\mathbf{H}_Y(\mathbf{D}^{-1} - \mathbf{H}_Y^\top \mathbf{H}_Y)^{-1}\mathbf{H}_Y^\top + \mathbf{I}|} \tag{358}
$$

Lemma 23: Let $\mathbf{K}(\alpha) = (\mathbf{A} + f(\alpha)\mathbf{B})^{-1}$, $0 < \alpha \le \alpha^*$, where $\mathbf{A} \succ f(\alpha)\mathbf{B} \succeq \mathbf{0}$, $0 \le \alpha \le \alpha^*$ and $f(\alpha)$ is continuous in α. Then, we have

$$\lim_{\alpha \to 0} \mathbf{K}(\alpha) = (\mathbf{A} + f(0)\mathbf{B})^{-1}. \tag{364}$$

Proof: In the proof of this lemma, we use the fact that if $\lim_{n \to \infty} \mathbf{C}^n = \mathbf{0}$, we have

$$(\mathbf{I} + \mathbf{C})^{-1} = \sum_{n=0}^{\infty} (-1)^n \mathbf{C}^n \tag{365}$$

where $\mathbf{C}^0 = \mathbf{I}$ [21, p. 19]. Now, we consider

$$\mathbf{K}(\alpha) = (\mathbf{A} + f(\alpha)\mathbf{B})^{-1} \tag{366}$$
$$= \mathbf{A}^{-1/2}(\mathbf{I} + f(\alpha)\mathbf{A}^{-1/2}\mathbf{B}\mathbf{A}^{-1/2})^{-1}\mathbf{A}^{-1/2} \tag{367}$$

where due to $\mathbf{A} \succ f(\alpha)\mathbf{B} \succeq \mathbf{0}$, we have

$$\mathbf{I} \succ f(\alpha)\mathbf{A}^{-1/2}\mathbf{B}\mathbf{A}^{-1/2} \succeq \mathbf{0} \tag{368}$$

which implies

$$\lim_{n \to \infty} \left(f(\alpha)\mathbf{A}^{-1/2}\mathbf{B}\mathbf{A}^{-1/2} \right)^n = \mathbf{0}. \tag{369}$$

Hence, we can use (365) in (367) to obtain

$$\mathbf{K}(\alpha) = \mathbf{A}^{-1/2} \left[\sum_{n=0}^{\infty} (-1)^n f^n(\alpha)(\mathbf{A}^{-1/2}\mathbf{B}\mathbf{A}^{-1/2})^n \right] \mathbf{A}^{-1/2} \tag{370}$$

which implies

$$\lim_{\alpha \to 0} \mathbf{K}(\alpha)$$
$$= \lim_{\alpha \to 0} \mathbf{A}^{-1/2} \left[\sum_{n=0}^{\infty} (-1)^n f^n(\alpha)(\mathbf{A}^{-1/2}\mathbf{B}\mathbf{A}^{-1/2})^n \right] \mathbf{A}^{-1/2} \tag{371}$$
$$= \mathbf{A}^{-1/2} \left[\sum_{n=0}^{\infty} (-1)^n f^n(0)(\mathbf{A}^{-1/2}\mathbf{B}\mathbf{A}^{-1/2})^n \right] \mathbf{A}^{-1/2} \tag{372}$$
$$= \mathbf{A}^{-1/2} \left[\mathbf{I} + f(0)\mathbf{A}^{-1/2}\mathbf{B}\mathbf{A}^{-1/2} \right]^{-1} \mathbf{A}^{-1/2} \tag{373}$$
$$= (\mathbf{A} + f(0)\mathbf{B})^{-1} \tag{374}$$

where (373) comes from (365); completing the proof of Lemma 23. ∎

We now consider (351) in Lemma 22 as follows:

$$\mathbf{K}_{X|\bar{\mathbf{Y}}_\alpha} = \mathbf{K}_X(\mathbf{K}_X + \mathbf{\Sigma}_{Y,\alpha})^{-1}\mathbf{\Sigma}_{Y,\alpha} \tag{375}$$
$$= (\mathbf{K}_X^{-1} + \mathbf{\Sigma}_{Y,\alpha}^{-1})^{-1} \tag{376}$$
$$= \left[\mathbf{K}_X^{-1} + \mathbf{R}_Y(\mathbf{\Lambda}_Y + \alpha\mathbf{I})^2\mathbf{R}_Y^\top \right]^{-1} \tag{377}$$
$$= \left[\mathbf{K}_X^{-1} + \mathbf{R}_Y\mathbf{\Lambda}_Y^2\mathbf{R}_Y^\top + \mathbf{R}_Y(2\alpha\mathbf{\Lambda}_Y + \alpha^2\mathbf{I})\mathbf{R}_Y^\top \right]^{-1} \tag{378}$$

where $0 < \alpha \le \alpha^*$. Equation (375) comes from (178), (377) is due to the definition of $\mathbf{\Sigma}_{Y,\alpha}$. We note that

$$\mathbf{K}_X^{-1} + \mathbf{R}_Y\mathbf{\Lambda}_Y^2\mathbf{R}_Y^\top \succ \mathbf{0} \tag{379}$$

and thus, α^* can be selected to ensure that

$$\mathbf{K}_X^{-1} + \mathbf{R}_Y\mathbf{\Lambda}_Y^2\mathbf{R}_Y^\top \succ \mathbf{R}_Y(2\alpha\mathbf{\Lambda}_Y + \alpha^2\mathbf{I})\mathbf{R}_Y^\top \tag{380}$$

for all $0 \le \alpha \le \alpha^*$. Hence, we can use Lemma 23 in (378) to obtain

$$\lim_{\alpha \to 0} \mathbf{K}_{X|\bar{\mathbf{Y}}_\alpha} = \left[\mathbf{K}_X^{-1} + \mathbf{R}_Y\mathbf{\Lambda}_Y^2\mathbf{R}_Y^\top \right]^{-1} \tag{381}$$
$$= \left[\mathbf{K}_X^{-1} + \mathbf{R}_Y\mathbf{\Lambda}_Y\mathbf{Q}_Y^\top\mathbf{Q}_Y\mathbf{\Lambda}_Y\mathbf{R}_Y^\top \right]^{-1} \tag{382}$$
$$= (\mathbf{K}_X^{-1} + \mathbf{H}_Y^T\mathbf{H}_Y)^{-1} \tag{383}$$
$$= \mathbf{K}_{X|Y} \tag{384}$$

where (383) comes from the singular value decomposition of $\mathbf{H}_Y$ and (384) is due to (221); completing the proof of (351).

Next, we consider (352) in Lemma 22 as follows:

$$\mathbf{F}_\alpha(\mathbf{D}) = \mathbf{\Sigma}_{Y,\alpha}(\mathbf{\Sigma}_{Y,\alpha} - \mathbf{D})^{-1}\mathbf{\Sigma}_{Y,\alpha} - \mathbf{\Sigma}_{Y,\alpha} \tag{385}$$
$$= \mathbf{\Sigma}_{Y,\alpha}(\mathbf{\Sigma}_{Y,\alpha} - \mathbf{D})^{-1}\mathbf{D} \tag{386}$$
$$= (\mathbf{D}^{-1} - \mathbf{\Sigma}_{Y,\alpha}^{-1})^{-1} \tag{387}$$
$$= (\mathbf{D}^{-1} - \mathbf{R}_Y(\mathbf{\Lambda}_Y + \alpha\mathbf{I})^2\mathbf{R}_Y^\top)^{-1} \tag{388}$$
$$= \left[\mathbf{D}^{-1} - \mathbf{R}_Y\mathbf{\Lambda}_Y^2\mathbf{R}_Y^\top - \mathbf{R}_Y(2\alpha\mathbf{\Lambda}_Y + \alpha^2\mathbf{I})\mathbf{R}_Y^\top \right]^{-1} \tag{389}$$
$$= \left[\mathbf{D}^{-1} - \mathbf{R}_Y\mathbf{\Lambda}_Y\mathbf{Q}_Y^\top\mathbf{Q}_Y\mathbf{\Lambda}_Y\mathbf{R}_Y^\top - \mathbf{R}_Y(2\alpha\mathbf{\Lambda}_Y + \alpha^2\mathbf{I})\mathbf{R}_Y^\top \right]^{-1} \tag{390}$$
$$= \left[\mathbf{D}^{-1} - \mathbf{H}_Y^\top\mathbf{H}_Y - \mathbf{R}_Y(2\alpha\mathbf{\Lambda}_Y + \alpha^2\mathbf{I})\mathbf{R}_Y^\top \right]^{-1} \tag{391}$$

where $0 < \alpha \le \alpha^*$. Equation (388) comes from the definition of $\mathbf{\Sigma}_{Y,\alpha}$ and (391) is obtained by using the singular value decomposition of $\mathbf{H}_Y$. We note that $\mathbf{D}^{-1} - \mathbf{H}_Y^\top\mathbf{H}_Y$ is strictly positive definite as (342) indicates, and hence, there exists an α^* such that

$$\mathbf{D}^{-1} - \mathbf{H}_Y^\top\mathbf{H}_Y \succ \mathbf{R}_Y(2\alpha\mathbf{\Lambda}_Y + \alpha^2\mathbf{I})\mathbf{R}_Y^\top \tag{392}$$

for all $0 \le \alpha \le \alpha^*$. Consequently, we can use Lemma 23 in (391) to obtain

$$\lim_{\alpha \to 0} \mathbf{F}_\alpha(\mathbf{D}) = (\mathbf{D}^{-1} - \mathbf{H}_Y^\top\mathbf{H}_Y)^{-1} \tag{393}$$

which completes the proof of Lemma 22.

REFERENCES

[1] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.

[2] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[3] D. Gunduz, E. Erkip, and H. V. Poor, "Secure lossless compression with side information," in *Proc. IEEE Inf. Theory Workshop*, 2008, pp. 169–173.

[4] D. Gunduz, E. Erkip, and H. V. Poor, "Lossless compression with security constraints," in *Proc. IEEE Int. Symp. Inf. Theory*, 2008, pp. 111–115.

[5] V. Prabhakaran and K. Ramchandran, "On secure distributed source coding," in *Proc. IEEE Inf. Theory Workshop*, 2007, pp. 442–447.

[6] R. Tandon, S. Ulukus, and K. Ramchandran, "Secure source coding with a helper," in *Proc. 47th Annu. Allerton Conf. Commun., Control Comput.*, Oct. 2009, pp. 1061–1068.

[7] R. Tandon, S. UlukusK, and Ramchandran, "Secure source coding with a helper," *IEEE Trans. Inf. Theory*, to be published.

[8] W. Luh and D. Kundur, "Distributed keyless secret sharing over noiseless channels," *Proc. IEEE Global Telecommun. Conf.*, pp. 44–48, 2007.

[9] L. Grokop, A. Sahai, and M. Gastpar, "Discriminatory source coding for a noiseless broadcast channel," in *Proc. Int. Symp. Inf. Theory*, 2005, pp. 77–81.

[10] P. Cuff, "A framework for partial secrecy," in *Proc. IEEE Globecom Telecommun. Conf.*, 2010, pp. 1–5.

[11] H. Yamamoto, "A source coding problem for sources with additional outputs to keep secret from the receiver or wiretappers," *IEEE Trans. Inf. Theory*, vol. 29, no. 6, pp. 918–923, Nov. 1983.

[12] H. Yamamoto, "A rate-distortion problem for a communication system with a secondary decoder to be hindered," *IEEE Trans. Inf. Theory*, vol. 34, no. 4, pp. 835–842, Jul. 1988.

[13] H. Yamamoto, "Rate-distortion theory for the Shannon cipher system," *IEEE Trans. Inf. Theory*, vol. 43, no. 3, pp. 827–835, May 1997.

[14] N. Merhav, "On the Shannon cipher system with a capacity-limited key-distribution channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 1269–1273, Mar. 2006.

[15] N. Merhav, "Shannon's secrecy system with informed receivers and its applications to systematic coding for wiretapped channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2723–2734, Jun. 2008.

[16] J. Villard and P. Piantanida, "Secure lossy source coding with side information at the decoders," presented at the 49th Annu. Allerton Conf. Commun., Control Comput., Sep. 2010, (arXiv: 1009.3891v1).

[17] A. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. 22, no. 1, pp. 1–10, Jan. 1976.

[18] T. Liu and P. Viswanath, "An extremal inequality motivated by multiterminal information theoretic problems," *IEEE Trans. Inf. Theory*, vol. 53, no. 5, pp. 1839–1851, May 2007.

[19] H. Weingarten, Y. Steinberg, and S. S. (Shitz, "The capacity region of the Gaussian multiple-input multiple-output broadcast channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3936–3964, Sep. 2006.

[20] H. V. Poor, *An Introduction to Signal Detection and Estimation*, 2nd ed. New York, NY, USA: Springer-Verlag, 1994.

[21] K. B. Petersen and M. S. Petersen, The Matrix Cookbook 2008 [Online]. Available: http://matrixcookbook.com

[22] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge, MA, USA: Cambridge Univ. Press, 1985.

[23] R. W. Newcomb, "On the simultaneous diagonalization of two semidefinite matrices," *Quart. Appl. Math.*, vol. 19, pp. 144–146, 1961.

[24] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," *IEEE Trans. Inf. Theory*, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.

[25] A. J. Stam, "Some inequalities satisfied by the quantities of information of Fisher and Shannon," *Inf. Control*, vol. 2, pp. 101–112, Jun. 1959.

[26] N. M. Blachman, "The convolution inequality for entropy powers," *IEEE Trans. Inf. Theory*, vol. IT-11, no. 2, pp. 267–271, Apr. 1965.

[27] D. P. Palomar and S. Verdu, "Gradient of mutual information in linear vector Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 52, no. 1, pp. 141–154, Jan. 2006.

Ersen Ekrem (S'08) received his Ph.D. degree from the Department of Electrical and Computer Engineering at the University of Maryland, College Park in August 2012. Prior to that, he received the B.S. and M.S. degrees in electrical and electronics engineering from Bogazici University, Istanbul, Turkey, in 2006 and 2007, respectively. Currently, he is with Qualcomm, Santa Clara, USA.

He received the Distinguished Dissertation Fellowship from the ECE Department at the University of Maryland, College Park, in 2012. His research interests include information theory and wireless communications.

Sennur Ulukus (S'90–M'98) is a Professor of Electrical and Computer Engineering at the University of Maryland at College Park, where she also holds a joint appointment with the Institute for Systems Research (ISR). Prior to joining UMD, she was a Senior Technical Staff Member at AT&T Labs-Research. She received her Ph.D. degree in Electrical and Computer Engineering from Wireless Information Network Laboratory (WINLAB), Rutgers University, and B.S. and M.S. degrees in Electrical and Electronics Engineering from Bilkent University. Her research interests are in wireless communication theory and networking, network information theory for wireless communications, signal processing for wireless communications, information-theoretic physical-layer security, and energy-harvesting communications.

Dr. Ulukus received the 2003 IEEE Marconi Prize Paper Award in Wireless Communications, an 2005 NSF CAREER Award, the 2010–2011 ISR Outstanding Systems Engineering Faculty Award, and the 2012 George Corcoran Education Award. She served as an Associate Editor for the the IEEE TRANSACTIONS ON INFORMATION THEORY (2007–2010) and the IEEE TRANSACTIONS ON COMMUNICATIONS (2003–2007). She served as a Guest Editor for the *Journal of Communications and Networks* for the special issue on energy harvesting in wireless networks (2012), the IEEE TRANSACTIONS ON INFORMATION THEORY for the special issue on interference networks (2011), the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS for the special issue on multiuser detection for advanced communication systems and networks (2008). She served as the TPC co-chair of the Communication Theory Symposium at 2013 IEEE ICC, Physical-Layer Security Workshop at 2011 IEEE Globecom, Physical-Layer Security Workshop at 2011 IEEE ICC, 2011 Communication Theory Workshop (IEEE CTW), Wireless Communications Symposium at 2010 IEEE ICC, Medium Access Control Track at 2008 IEEE WCNC, and Communication Theory Symposium at 2007 IEEE Globecom. She was the Secretary of the IEEE Communication Theory Technical Committee (CTTC) in 2007–2009.