Secure Source Coding Resilient Against Compromised Users via an Access Structure

Hassan ZivariFard and Rémi A. Chou

***Abstract*—Consider a source and multiple users who observe the independent and identically distributed (i.i.d.) copies of correlated Gaussian random variables. The source wishes to compress its observations and store the result in a public database such that (i) authorized sets of users are able to reconstruct the source with a certain distortion level, and (ii) information leakage to non-authorized sets of colluding users is minimized. In other words, the recovery of the source is restricted to a predefined access structure. The main result of this paper is a closed-form characterization of the fundamental trade-off between the source coding rate and the information leakage rate. As an example, threshold access structures are studied, i.e., the case where any set of at least *t* users is able to reconstruct the source with some predefined distortion level and the information leakage at any set of users with a size smaller than *t* is minimized.**

***Index Terms*—Distributed source coding, secure source coding, secure data storage, equivocation-rate, capacity, side information, rate-distortion region, access structure, compromised users.**

I. Introduction

A SOLUTION to the storage of private data that is resilient to compromised users is secure distributed storage via traditional cryptographic solutions such as secret sharing [2], [3]. Specifically, a solution based on secret sharing consists in encoding the private data and distributing parts of the encoded data among multiple users, via individual secure channels, such that any t users that pool their information together can reconstruct the private data, while any $z(< t)$ colluding users cannot learn any information about the private data. The set of all sets of users capable of reconstructing the private data is referred to as the access structure. For instance, the users could represent servers.

A. Problem Overview

In this paper, we aim to propose a secure distributed data storage strategy that solely relies on a public database and accounts for side information at the users by considering three main modifications of the secret sharing solution described above. First, we do not assume that secure channels are available to transmit the encoded private data to the users, as secure channels come with a cost in practice, instead, we solely rely on the availability of a public database. Second, we consider that the users have side information about the private data. While this consideration is not relevant in the original secret sharing problem where the secret is an arbitrary sequence of symbols and does not represent information, it becomes relevant in a data storage context. Not accounting for the fact that the users can have side information raises the following two challenges that cannot be addressed with results for traditional secret sharing: (i) it leads to overestimating the security guarantees of the protocol, and (ii) it leads to inefficiency in terms of data storage size. Third, in our proposed setting, we relax the lossless reconstruction constraint of traditional secret sharing to a lossy reconstruction constraint [4].

Two distinct bodies of work on secure data storage are related to our model. The first one is secret sharing, which specifically addresses the presence of access structures – we refer to [5] for a comprehensive literature review. The second one is secure source coding [6], [7], [8], [9], [10], [11], [12], [13], which mainly addresses the presence of side information at the users, but in the absence of access structures. By contrast, in this paper, we propose to simultaneously address the presence of an access structure *and* side information at the users within a single framework. Specifically, we consider a source and multiple users who observe the i.i.d. copies of correlated Gaussian random variables. The source wants to compress its observations and store the result in a public database such that (i) only pre-defined sets of authorized users can reconstruct, up to a prescribed distortion level, the source by pooling all their available information, and (ii) information leakage about the source to any other sets of colluding users is minimized. The main result of this paper is a closed-form characterization of the fundamental trade-off between source coding rate and information leakage rate. Our result indicates that if the source is more correlated, in a sense that we make precise in the sequel, with the side information of the authorized sets of users than with the side information of any unauthorized set of users, then the optimal information leakage rate grows linearly with the optimal source coding rate. On the other hand, if this is not the case, the optimal information leakage rate grows non-linearly with the optimal source coding rate. Additionally, for threshold access structures, i.e., when a

Manuscript received 15 December 2023; revised 8 March 2024; accepted 30 May 2024. Date of publication 10 June 2024; date of current version 23 July 2024. This work was supported in part by NSF under Grant CCF-2425371. Part of this work is presented at the 2022 IEEE Information Theory Workshop [DOI: 10.1109/ITW54588.2022.9965904]. *(Corresponding author: Hassan ZivariFard.)*

Hassan ZivariFard is with the Department of Electrical Engineering, Columbia University, New York, NY 10027 USA (e-mail: hz2863@columbia.edu).

Rémi A. Chou is with the Department of Computer Science and Engineering, The University of Texas at Arlington, Arlington, TX 76019 USA (e-mail: remi.chou@uta.edu).

This article has supplementary downloadable material available at https://doi.org/10.1109/JSAIT.2024.3410235, provided by the authors.

Digital Object Identifier 10.1109/JSAIT.2024.3410235

fixed number of users, denoted by t, are needed to reconstruct the source (independently of the specific identities of those users), we show that the capacity region is, in general, not a monotonic function of the threshold t.

B. Novelties and Main Challenges

Next, we discuss the novelties and main challenges of the main result of this paper, which is a characterization of the optimal rate-leakage region for the problem introduced in the previous section. We first describe the main challenges of our converse proof.

- The side information of each authorized or unauthorized set of users is a vector Gaussian random variable, and each component of this vector accounts for the side information of one user of this set. In our study, we use sufficient statistics [14, Sec. 2.9] to convert this vector Gaussian side information to a scalar random variable and facilitate the analysis of our setting. For the converse proof, this conversion allows us to reduce the problem to two cases. A first case (respectively second case), in which the source is more (respectively less) correlated, in a sense that we make precise in the sequel, with the side information of any set of authorized users than with the side information of any unauthorized set of users.
- Another key step in the proof of our converse is the proof of the sufficiency of a single auxiliary random variable in the outer region that we derive, to achieve minimum information leakage at the unauthorized users for each of the two cases discussed above.
- A particularly challenging aspect of our setting is the compound structure of the problem, which arises as a consequence of having multiple authorized and multiple unauthorized sets of users. Specifically, in our achievability region, it leads to, first, an optimization over the distribution of the involved auxiliary random variables and, then, to an optimization over the sets of authorized users and unauthorized users, whereas the order of these two optimizations are reversed in our outer region. In general, such a mismatch between the inner and outer regions leads to a gap between the achievability and the converse, e.g., as in [15] for compound wiretap channels. In our setting, we obtain a capacity result by proving the existence of a saddle point, which proves that the order of the optimizations is irrelevant.

We now discuss the main challenges of our achievability proof.

- The achievability is first proved for discrete random variables and then extended to continuous random variables through quantization. Note that one cannot consider a specific quantization strategy at the unauthorized users to ensure the leakage requirement in an information-theoretic manner; therefore, a key step in this extension is to prove that the leakage constraint holds for continuous random variables.
- For the achievability proof, the use of sufficient statistics also facilitates the evaluation of the achievable rate region, in particular, the computation of the conditional covariance of vector Gaussian sources.

C. Related Works

Of particular relevance to this paper, [6] have established the first characterization of the rate at which an encoder may compress a source such that an authorized user can recover the source in a lossless manner while guaranteeing a minimum information leakage at an unauthorized user who observes the encoded source. Other variations of this problem are studied in [7], [8], [9], [10], [11], [12]. This problem is generalized to a scenario, in which the authorized user may recover the compressed source with some predefined distortion in [9]. Specifically, [9] characterized the optimal tradeoff between the rate, the desired distortion, and the information leakage when both the authorized and unauthorized users observe different i.i.d, side information sequences that are correlated with the compressed source. The secure lossy compression of a vector Gaussian source when both the authorized user and the unauthorized user have vector Gaussian side information have been studied in [13], which derives inner and outer regions on the optimal trade-off between the rate, the desired distortion, and the information leakage. References [16], [17] study this problem in the case where the fidelity of the communication to the authorized user is measured by a distortion metric and the secrecy performance of the system is also evaluated under a distortion metric, a line of study that was first initiated in [18], [19]. Secure source coding when there is a shared secret key between the legitimate terminals has also been studied in [20], [21], [22], [23], [24]. Note that all these previous works do not consider access structures and deal with a source coding problem. The problem studied in this paper subsumes the secure lossy compression of a scalar Gaussian source when both the authorized user and the unauthorized user have scalar Gaussian side information as well as the secure lossy compression of a scalar Gaussian source when both the authorized user and the unauthorized user have vector Gaussian side information.

In [9, Sec. V.A] and [13, Example 1], the authors study a single-user and single-eavesdropper Gaussian secure source coding problem, which is a special case of the problem studied in our paper. Indeed, the problem studied in this paper involves multiple sets of authorized users and multiple sets of unauthorized users (eavesdroppers). Specifically, in our setting, we upper-bound the information leakage over all possible sets of unauthorized users, and for the reconstruction of the source we require that any set of authorized users can recover the source with some fixed distortion level. As discussed above, this creates additional challenges compared to a single authorized and single unauthorized user. Note also that the single-user single-eavesdropper case had not been fully solved, as [13, Example 1] establishes the capacity region when the compression rate is infinity, and [9, Sec. V.A] establishes the capacity when the side information at the eavesdropper is a degraded version of the legitimate receiver's side information. We note that the authors in [9, Remark 8] conjecture that their achievability is optimal in the non-degraded case, however they do not provide a converse proof.

In the context of secret sharing, another related work is [25], where a function of a Gaussian source must be reconstructed in a lossless manner by authorized sets of users and must

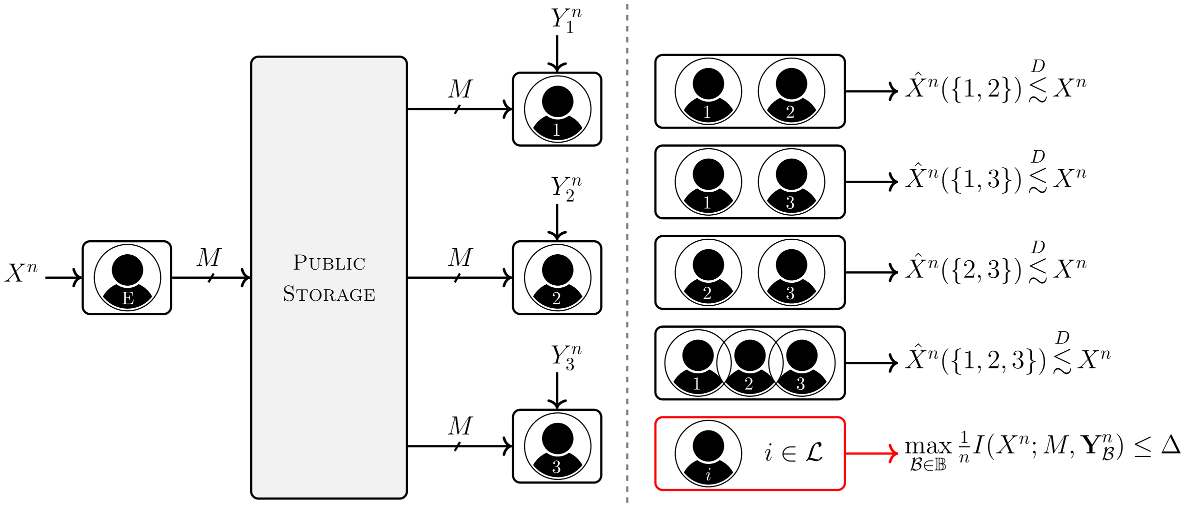
X^n
E
M
Public Storage
M
M
M
Y_1^n
1
Y_2^n
2
Y_3^n
3
$\hat{X}^n(\{1,2\}) \overset{D}{\lesssim} X^n$
$\hat{X}^n(\{1,3\}) \overset{D}{\lesssim} X^n$
$\hat{X}^n(\{2,3\}) \overset{D}{\lesssim} X^n$
$\hat{X}^n(\{1,2,3\}) \overset{D}{\lesssim} X^n$
i
$i \in \mathcal{L}$
$\max_{\mathcal{B}\in\mathbb{B}} \frac{1}{n} I(X^n; M, \mathbf{Y}^n_{\mathcal{B}}) \leq \Delta$

Fig. 1. Secure source coding with three users, i.e., $\mathcal{L} = \{1, 2, 3\}$, when any single user must not learn more than $n\Delta$ bits of information about the source X^n, i.e., we set $\mathbb{A} = \{\{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$, and $\mathbb{B} = \{\{1\}, \{2\}, \{3\}\}$. $\hat{X}^n(\{i, j\}) \overset{D}{\lesssim} X^n$, for $i, j \in \{1, 2, 3\}$ and $i \neq j$, means that the distortion between the reconstructed source by the users i and j together and the source sequence X^n must be less than D.

be kept secret from unauthorized sets of users, who all own side information about the source. Finally, note that, in our results, the length of the compressed data stored in the public database and the source observation at the users scale linearly with the number of source observations n and does not depend on the number of participants but only on the access structure. Specifically, the compressed data stored in the public database must allow the reconstruction of the source for the group of authorized participants that has the least amount of information about the source in their side information. This contrasts with traditional problems that involve access structures, e.g., secret-sharing model [3], for which the best known coding schemes require the share size to scale exponentially with the number of participants for some access structures [5].

D. Paper Organization

The remainder of the paper is organized as follows. We define the notation in Section II and formally define the problem in Section III. We present our main results in Section IV and provide the proofs in Section V. We provide concluding remarks in Section VI.

II. Notation

Let $\mathbb{N}^+$ be the set of positive natural numbers, $\mathbb{R}$ be the set of real numbers, and define $\mathbb{R}_+ \triangleq \{x \in \mathbb{R} | x \geq 0\}$ and $\mathbb{R}_{++} \triangleq \mathbb{R}_+ \backslash \{0\}$. For any $a, b \in \mathbb{R}$, define $\int [\![a : b]\!] \triangleq [\lfloor a \rfloor, \lceil b \rceil] \cap \mathbb{N}^+$ and $[a]^+ \triangleq \max\{0, a\}$. Random variables are denoted by capital letters and their realizations by lower case letters. Vectors are denoted by boldface letters, e.g., $\mathbf{X}$ denotes a random vector and $\mathbf{x}$ denotes a realization of $\mathbf{X}$. $\mathbb{E}_X(\cdot)$ is the expectation with respect to the random variable X, for brevity, we sometimes omit the subscripts in the expectation if it is clear from the context. The set of $\epsilon-$strongly jointly typical sequences of length n, according to P_{XY}, is denoted by $\mathcal{T}_\epsilon^{(n)}(P_{XY})$ [26]. Superscripts denote the dimension of a vector, e.g., X^n. X_i^j denotes $(X_i, X_{i+1}, \ldots, X_j)$, and $X^n_{\sim i}$ denotes the vector X^n except X_i. The cardinality of a set is denoted by $|\cdot|$. The entropy of the discrete random variable X is denoted by $H(X)$, the differential entropy of the random variable X is denoted by $\mathbb{h}(X)$, and the mutual information between the random variables X and Y is denoted by $I(X; Y)$. The support of a probability distribution P is denoted by $\text{supp}(P)$. The n-fold product distribution constructed from the same distribution P is denoted by $P^{\otimes n}$. Throughout the paper, log denotes the base 2 logarithm.

III. Problem Statement

Consider a memoryless source $(\mathcal{X} \times \boldsymbol{\mathcal{Y}}_{\mathcal{L}}, P_{X\mathbf{Y}_{\mathcal{L}}})$, where $\mathcal{L} \triangleq [\![1 : L]\!]$ and $\mathbf{Y}_{\mathcal{L}} \triangleq (Y_\ell)_{\ell\in\mathcal{L}}$, that consists of $L + 1$ alphabets $\mathcal{X} \times \boldsymbol{\mathcal{Y}}_{\mathcal{L}}$ and a joint distribution $P_{X\mathbf{Y}_{\mathcal{L}}}$ over $\mathcal{X} \times \boldsymbol{\mathcal{Y}}_{\mathcal{L}}$. Let $\mathbb{A}$ be a set of subsets of $\mathcal{L}$ such that for any $\mathcal{S} \subseteq \mathcal{L}$, if $\mathcal{S}$ has a subset that belongs to $\mathbb{A}$, then $\mathcal{S} \in \mathbb{A}$, i.e., $\mathbb{A}$ has a monotone access structure [27]. Then, define $\mathbb{B} \triangleq 2^{\mathcal{L}} \backslash \mathbb{A}$ to be the set of all colluding subsets of users for which the information leakage about the source X^n must be minimized (see Fig. 1). Henceforth, for any $\mathcal{A} \in \mathbb{A}$ and for any $\mathcal{B} \in \mathbb{B}$, $\mathbf{Y}_{\mathcal{A}}$ and $\mathbf{Y}_{\mathcal{B}}$ denote $(Y_\ell)_{\ell\in\mathcal{A}}$ and $(Y_\ell)_{\ell\in\mathcal{B}}$, respectively. Let $d : \mathcal{X} \times \boldsymbol{\mathcal{Y}}_{\mathcal{A}} \to [\![0 : d_{\max}]\!]$ be a distortion measure such that $0 \leq d_{\max} < \infty$.

Definition 1: A $(2^{nR}, n)$ source code for the memoryless source $(\mathcal{X} \times \boldsymbol{\mathcal{Y}}_{\mathcal{L}}, p_{X\mathbf{Y}_{\mathcal{L}}})$ consists of

- an encoding function $f : x^n \mapsto m$, which assigns an index $m \in [\![1 : 2^{nR}]\!]$ to each $x^n \in \mathcal{X}^n$. As depicted in Fig. 1, M is stored in a public database;
- decoding functions $\hat{x}_{\mathcal{A}} : m \times \mathbf{y}^n_{\mathcal{A}} \mapsto \hat{x}^n(\mathcal{A}) \cup \{\mathfrak{e}\}$, where $\mathcal{A} \in \mathbb{A}$, which assigns an estimate $\hat{x}^n(\mathcal{A}) \in \mathcal{X}^n$ or an error $\mathfrak{e}$ to each $m \in [\![1 : 2^{nR}]\!]$ and $\mathbf{y}^n_{\mathcal{A}} \in \boldsymbol{\mathcal{Y}}^n_{\mathcal{A}}$.

Definition 2: Let $D > 0$. A pair $(R, \Delta) \in \mathbb{R}^2_+$ is achievable if there exists a sequence of $(2^{nR}, n)$ source codes, such that,

$$\max_{\mathcal{A}\in\mathbb{A}} \limsup_{n\to\infty} \mathbb{E}\left[d\left(X^n, \hat{X}^n(\mathcal{A})\right)\right] \leq D, \tag{1a}$$

$$\max_{\mathcal{B}\in\mathbb{B}} \lim_{n\to\infty} \frac{1}{n} I\left(X^n; M, \mathbf{Y}^n_{\mathcal{B}}\right) \leq \Delta, \tag{1b}$$

where the distortion between the sequences x^n and $\hat{x}^n(\mathcal{A})$ is defined by

$$d\big(x^n, \hat{x}^n(\mathcal{A})\big) \triangleq \frac{1}{n}\sum_{i=1}^{n} d\big(x_i, \hat{x}_i(\mathcal{A})\big). \tag{1c}$$

The set of all achievable pairs is referred to as the rate-leakage region and denoted by $\mathcal{R}(D, \mathbb{A})$.

Equation (1a) means that any set of authorized users $\mathcal{A} \in \mathbb{A}$ can reconstruct the source X^n within the distortion D from the observation $\mathbf{Y}^n_{\mathcal{A}}$ and the public data M, and (1b) means that any colluding set of unauthorized users $\mathcal{B} \in \mathbb{B}$ cannot learn more than $n\Delta$ bits about the source X^n from the observation $\mathbf{Y}^n_{\mathcal{B}}$ and M. In this paper, we consider $P_{X\mathbf{Y}_{\mathcal{L}}}$ the joint distribution of zero-mean jointly Gaussian random variables with a non-singular covariance matrix. We denote the variance of X by σ_X^2. Without loss of generality, for every $\mathcal{A} \in \mathbb{A}$ and $\mathcal{B} \in \mathbb{B}$, by [28, Th. 3.5.2], one can write

$$\mathbf{Y}_{\mathcal{A}} = \mathbf{h}_{\mathcal{A}}X + \mathbf{N}_{\mathcal{A}}, \tag{2a}$$

$$\mathbf{Y}_{\mathcal{B}} = \mathbf{h}_{\mathcal{B}}X + \mathbf{N}_{\mathcal{B}}, \tag{2b}$$

where $\mathbf{h}_{\mathcal{A}} \in \mathbb{R}^{|\mathcal{A}|}_{++}$ and $\mathbf{h}_{\mathcal{B}} \in \mathbb{R}^{|\mathcal{B}|}_{++}$ and $\mathbf{N}_{\mathcal{A}}$ and $\mathbf{N}_{\mathcal{B}}$ are zero-mean Gaussian random vectors with identity covariance matrix and independent of X. Equation (2) is proved in Appendix A. Then, still without loss of generality, by normalizing (2), one can consider the following source model

$$\mathbf{Y}_{\mathcal{A}} = \mathbf{1}_{\mathcal{A}}X + \mathbf{N}_{\mathcal{A}}, \quad \forall \mathcal{A} \in \mathbb{A} \tag{3a}$$

$$\mathbf{Y}_{\mathcal{B}} = \mathbf{1}_{\mathcal{B}}X + \mathbf{N}_{\mathcal{B}}, \quad \forall \mathcal{B} \in \mathbb{B} \tag{3b}$$

where $\mathbf{N}_{\mathcal{A}}$ and $\mathbf{N}_{\mathcal{B}}$ are zero-mean Gaussian random vectors with covariance matrices $\mathbf{\Sigma}_{\mathcal{A}} \succ 0$ and $\mathbf{\Sigma}_{\mathcal{B}} \succ 0$, respectively, that are independent of X and $\mathbf{1}_{\mathcal{A}}$ is the all-ones vector with size $|\mathcal{A}|$. Without loss of generality, we can also consider $\mathbf{N}_{\mathcal{A}}$ and $\mathbf{N}_{\mathcal{B}}$ independent, for $\mathcal{A} \in \mathbb{A}$ and $\mathcal{B} \in \mathbb{B}$, since (1) only depends on the marginal distributions $(P_{X\mathbf{Y}_{\mathcal{A}}})_{\mathcal{A}\in\mathbb{A}}$ and $(P_{X\mathbf{Y}_{\mathcal{B}}})_{\mathcal{B}\in\mathbb{B}}$. In this paper, the distortion of the reconstructed sequence $(\hat{X}_i(\mathcal{A}))_{i=1}^n$ in Definition 2 is measured by the mean square error as,

$$\frac{1}{n}\mathbb{E}\left[\left(X_i - \hat{X}_i(\mathcal{A})\right)^2\right] \leq D. \tag{4}$$

Since the minimizer of the mean square error is the Minimum Mean-Square Error (MMSE) estimator, which is given by the conditional mean, we assume that the authorized users choose this optimal estimator, i.e., the authorized users in $\mathcal{A} \in \mathbb{A}$ form $(\hat{X}_i(\mathcal{A}))_{i=1}^n$ as $\hat{X}_i(\mathcal{A}) \triangleq \mathbb{E}[X_i|\mathbf{Y}^n_{\mathcal{A}}, f(X^n)]$.

IV. Main Results

Henceforth, for some $\mathcal{A} \in \mathbb{A}$, we assume $0 \leq D \leq \sigma^2_{X|\mathbf{Y}_{\mathcal{A}}}$, where $\sigma^2_{X|\mathbf{Y}_{\mathcal{A}}}$ is the conditional variance of X given $\mathbf{Y}_{\mathcal{A}}$, $\sigma^2_{X|\mathbf{Y}_{\mathcal{A}}} = \mathbb{E}[(X - \mathbb{E}[X|\mathbf{Y}_{\mathcal{A}}])^2|\mathbf{Y}_{\mathcal{A}}]$. If $D \geq \sigma^2_{X|\mathcal{Y}_{\mathcal{A}}}$ for all $\mathcal{A}$ in $\mathbb{A}$, then $\mathcal{R}(D, \mathbb{A}) = \{(R, \Delta) : R \geq 0, \Delta \geq \max_{\mathcal{B}\in\mathbb{B}}\{I(X; Y_{\mathcal{B}})\}\}$, because the achievability scheme that consists in setting $M \triangleq \emptyset$ implies

$$\frac{1}{n}\mathbb{E}\left[\left(X_i - \hat{X}_i(\mathcal{A})\right)^2\right] = \sigma^2_{X|\mathbf{Y}_{\mathcal{A}}}.$$

A. Results for General Access Structures

The main result of this paper is a closed-form expression for the optimal trade-off between the compression rate and the leakage rate of the source, which is provided in the following theorem.

Theorem 1: Let $D > 0$. For any access structure $\mathbb{A}$,

$$\mathcal{R}(D, \mathbb{A}) = \left\{\begin{array}{l} (R, \Delta) : \\ R \geq \left[\frac{1}{2}\log\frac{\sigma_X^2}{D} - \frac{1}{2}\log\left(1 + \frac{\sigma_X^2}{\operatorname{tr}\left(\mathbf{\Sigma}^{-1}_{\mathcal{A}^\star}\right)^{-1}}\right)\right]^+ \\ \Delta \geq \begin{cases} g_1(\mathcal{A}^\star, \mathcal{B}^\star) & \textit{when } \operatorname{tr}\left(\mathbf{\Sigma}^{-1}_{\mathcal{A}^\star}\right) \geq \operatorname{tr}\left(\mathbf{\Sigma}^{-1}_{\mathcal{B}^\star}\right) \\ g_2(\mathcal{A}^\star, \mathcal{B}^\star) & \textit{when } \operatorname{tr}\left(\mathbf{\Sigma}^{-1}_{\mathcal{A}^\star}\right) \leq \operatorname{tr}\left(\mathbf{\Sigma}^{-1}_{\mathcal{B}^\star}\right) \end{cases} \end{array}\right\}, \tag{5}$$

where

$$g_1(\mathcal{A}^\star, \mathcal{B}^\star) \triangleq \left[\frac{1}{2}\log\frac{\sigma_X^2}{D} - \frac{1}{2}\log\left(1 + \frac{\sigma_X^2}{\operatorname{tr}\left(\mathbf{\Sigma}^{-1}_{\mathcal{A}^\star}\right)^{-1}}\right)\right]^+ + \frac{1}{2}\log\left(1 + \frac{\sigma_X^2}{\operatorname{tr}\left(\mathbf{\Sigma}^{-1}_{\mathcal{B}^\star}\right)^{-1}}\right),$$

$$g_2(\mathcal{A}^\star, \mathcal{B}^\star) \triangleq \frac{1}{2}\log\left(\left[\frac{\sigma_X^2}{D} - \left(1 + \frac{\sigma_X^2}{\operatorname{tr}\left(\mathbf{\Sigma}^{-1}_{\mathcal{A}^\star}\right)^{-1}}\right)\right]^+ + 1 + \frac{\sigma_X^2}{\operatorname{tr}\left(\mathbf{\Sigma}^{-1}_{\mathcal{B}^\star}\right)^{-1}}\right),$$

$\mathcal{A}^\star \in \operatorname{argmin}_{\mathcal{A}\in\mathbb{A}}\{\operatorname{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{A}})\}$, and $\mathcal{B}^\star \in \operatorname{argmax}_{\mathcal{B}\in\mathbb{B}}\{\operatorname{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{B}})\}$.

The converse of Theorem 1 is provided in Section V. The achievability proof of Theorem 1 is similar to that of [9, Th. 3] and is omitted for brevity but is made available as a supplementary file.

Remark 1 (Comparison With [13, Example 1] and [9, Sec. V.A]): When there is only one authorized and one unauthorized user, the problem setup in (1) with $\mathbb{A} \triangleq \{1\}$ and $\mathbb{B} \triangleq \{2\}$ reduces to the problem setup in [13, Example 1] and [9, Sec. V.A] and Theorem 1 yields the capacity region

$$\mathcal{R}(D, \mathbb{A}) = \left\{\begin{array}{l} (R, \Delta) : \\ R \geq \left[\frac{1}{2}\log\frac{\sigma_X^2}{D} - \frac{1}{2}\log\left(1 + \frac{\sigma_X^2}{\sigma_1^2}\right)\right]^+ \\ \Delta \geq \begin{cases} g_1 & \text{when } \sigma_1^2 \leq \sigma_2^2 \\ g_2 & \text{when } \sigma_1^2 \geq \sigma_2^2 \end{cases} \end{array}\right\},$$

where

$$g_1 \triangleq \left[\frac{1}{2}\log\frac{\sigma_X^2}{D} - \frac{1}{2}\log\left(1 + \frac{\sigma_X^2}{\sigma_1^2}\right)\right]^+ + \frac{1}{2}\log\left(1 + \frac{\sigma_X^2}{\sigma_2^2}\right),$$

$$g_2 \triangleq \frac{1}{2}\log\left(\left[\frac{\sigma_X^2}{D} - \left(1 + \frac{\sigma_X^2}{\sigma_1^2}\right)\right]^+ + 1 + \frac{\sigma_X^2}{\sigma_2^2}\right).$$

In the lower bound of the compression rate R in Theorem 1, the term $\frac{1}{2}\log\frac{\sigma_X^2}{D}$ is the source coding capacity in the absence of side information [26, Th. 3.6], and the term $\frac{1}{2}\log(1 + \frac{\sigma_X^2}{\operatorname{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{A}^\star})^{-1}})$ is the gain provided by the side information at the authorized users. In the lower bound on the information

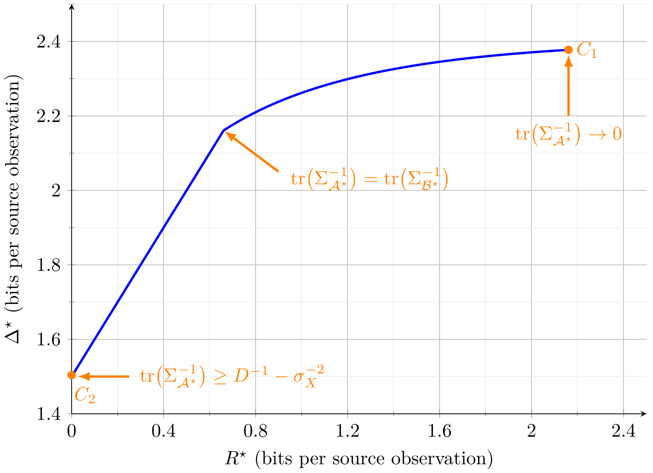

Fig. 2. $(R^\star, \Delta^\star)$ represents the corner points of the rate-leakage region $\mathcal{R}(D, \mathbb{A})$ characterized in Theorem 1, for fixed noise variances, when $\sigma_X^2 = 2$, $D = 0.1$, and $\mathrm{tr}(\mathbf{\Sigma}_{\mathcal{B}^\star}^{-1}) = 3.5$.

leakage Δ in Theorem 1, the term $(1 + \frac{\sigma_X^2}{\mathrm{tr}(\mathbf{\Sigma}_{\mathcal{B}^\star}^{-1})^{-1}})$ represents a penalty coming from the side information at the unauthorized users. When $\sigma_X^2 = 2$, $D = 0.1$, and $\mathrm{tr}(\mathbf{\Sigma}_{\mathcal{B}^\star}^{-1}) = 3.5$, the leakage rate $\Delta^\star$ is depicted in Fig. 2 with respect to the storage rate $R^\star$, where $(R^\star, \Delta^\star)$ represents the corner points of the region $\mathcal{R}(D, \mathbb{A})$ characterized in Theorem 1. As seen in Fig. 2, the leakage does not grow linearly with the storage rate $R^\star$, when $\mathrm{tr}(\mathbf{\Sigma}_{\mathcal{A}^\star}^{-1}) \leq \mathrm{tr}(\mathbf{\Sigma}_{\mathcal{B}^\star}^{-1})$. Intuitively, in this regime, the storage rate R^* decreases as $\mathrm{tr}(\mathbf{\Sigma}_{\mathcal{A}^\star}^{-1})$ grows but, since the unauthorized users in $\mathcal{B}^\star$ have a "less noisy" side information about the source than the authorized users in $\mathcal{A}^\star$ have, the information leakage Δ^* does not increase with the storage rate $R^\star$ as fast as it does when the authorized sets of users $\mathcal{A}^\star$ have a "less noisy" side information about the source than the authorized set of users $\mathcal{B}^\star$. In Fig. 2, the corner point $C_1 = (\frac{1}{2}\log\frac{\sigma_X^2}{D}, \frac{1}{2}\log\frac{\sigma_X^2}{D} + \frac{1}{2}\log(1 + \frac{\sigma_X^2}{\mathrm{tr}(\mathbf{\Sigma}_{\mathcal{B}^\star}^{-1})^{-1}}))$ corresponds to the case in which the side information at the authorized set of users is not correlated with the source, i.e., $\mathrm{tr}(\mathbf{\Sigma}_{\mathcal{A}^\star}^{-1}) \to 0$, and therefore the communication rate is maximal. On the other hand, the corner point $C_2 = (0, \frac{1}{2}\log(1 + \frac{\sigma_X^2}{\mathrm{tr}(\mathbf{\Sigma}_{\mathcal{B}^\star}^{-1})^{-1}}))$ corresponds to the case in which the distortion between the side information at the authorized sets of users and the source is less than D, meaning that the encoder does not need to generate M. Note that, in this case, from (14a), $D \geq \sigma_{X|\mathbf{Y}_{\mathcal{A}^\star}}^2$ translates to, $\mathrm{tr}(\mathbf{\Sigma}_{\mathcal{A}^\star}^{-1}) \geq D^{-1} - \sigma_X^{-2}$.

B. Results for Threshold Access Structures

In this section, we consider a special type of access structure, which is known as the threshold access structure [3] and defined, for a threshold $t \in [\![1 : L]\!]$, as

$$\mathbb{A}_t \triangleq \{\mathcal{A} \subseteq \mathcal{L} : |\mathcal{A}| \geq t\}. \tag{6}$$

In other words, the threshold access structure is such that any set of t users is able to reconstruct the compressed source with some predefined distortion. Similar to the general case, the complement of the set $\mathbb{A}_t$ is defined as $\mathbb{B}_t \triangleq 2^{\mathcal{L}} \backslash \mathbb{A}_t = \{\mathcal{B} \subseteq \mathcal{L} : |\mathcal{B}| < t\}$, and we consider $\mathcal{A}_t^\star \in \mathrm{argmin}_{\mathcal{A} \in \mathbb{A}_t} \mathrm{tr}(\mathbf{\Sigma}_{\mathcal{A}}^{-1})$ and $\mathcal{B}_t^\star \in \mathrm{argmax}_{\mathcal{B} \in \mathbb{B}_t}\{\mathrm{tr}(\mathbf{\Sigma}_{\mathcal{B}}^{-1})\}$. The following result presents necessary and sufficient conditions to determine whether the optimal trade-off between the compression rate and the leakage rate is decreasing or increasing with the threshold t.

Theorem 2: Let $t \in [\![1 : L]\!]$, suppose that $\mathrm{tr}(\mathbf{\Sigma}_{\mathcal{A}_t^\star}^{-1}) < D^{-1} - \sigma_X^{-2}$, which means that the source X^n needs to be encoded to satisfy (4) as discussed after Remark 1, and define $R(D, \mathbb{A}_t) \triangleq \min\{R : (R, \Delta) \in \mathcal{R}(D, \mathbb{A}_t)\}$. Then, we have,

- $\mathcal{R}(D, \mathbb{A}_L) \supseteq \mathcal{R}(D, \mathbb{A}_t) \Leftrightarrow \frac{\sigma_X^{-2} + \mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{A}_t^\star}^{-1}\right)}{\sigma_X^{-2} + \mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{B}_t^\star}^{-1}\right)} \leq \frac{\sigma_X^{-2} + \mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{A}_L^\star}^{-1}\right)}{\sigma_X^{-2} + \mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{B}_L^\star}^{-1}\right)}$;
- $R(D, \mathbb{A}_t) \geq R(D, \mathbb{A}_{t+i})$, for $i \in [\![1 : L - t]\!]$.

Theorem 3: For any $t \in [\![1 : L]\!]$, let $\Delta(D, \mathbb{A}_t) \triangleq \min\left\{\Delta : (R, \Delta) \in \mathcal{R}(D, \mathbb{A}_t)\right\}$, and suppose that $\mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{A}_t^\star}^{-1}\right) < D^{-1} - \sigma_X^{-2}$, which means that the source X^n needs to be encoded to satisfy (4) as discussed after Remark 1. Then, for any $t \in [\![1 : L]\!]$, and $i \in [\![1 : L - t]\!]$,

- when $\mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{A}_t^\star}^{-1}\right) \leq \mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{B}_t^\star}^{-1}\right)$ and $\mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{A}_{t+i}^\star}^{-1}\right) \leq \mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{B}_{t+i}^\star}^{-1}\right)$,
$$\Delta(D, \mathbb{A}_t) \geq \Delta(D, \mathbb{A}_{t+i}) \Leftrightarrow \mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{A}_{t+i}^\star}^{-1}\right) - \mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{A}_t^\star}^{-1}\right) \geq \mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{B}_{t+i}^\star}^{-1}\right) - \mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{B}_t^\star}^{-1}\right);$$
- when $\mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{A}_t^\star}^{-1}\right) \geq \mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{B}_t^\star}^{-1}\right)$ and $\mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{A}_{t+i}^\star}^{-1}\right) \geq \mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{B}_{t+i}^\star}^{-1}\right)$,
$$\Delta(D, \mathbb{A}_t) \geq \Delta(D, \mathbb{A}_{t+i}) \Leftrightarrow \frac{\sigma_X^{-2} + \mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{B}_t^\star}^{-1}\right)}{\sigma_X^{-2} + \mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{A}_t^\star}^{-1}\right)} \geq \frac{\sigma_X^{-2} + \mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{B}_{t+i}^\star}^{-1}\right)}{\sigma_X^{-2} + \mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{A}_{t+i}^\star}^{-1}\right)};$$
- when $\mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{A}_t^\star}^{-1}\right) \geq \mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{B}_t^\star}^{-1}\right)$ and $\mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{A}_{t+i}^\star}^{-1}\right) \leq \mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{B}_{t+i}^\star}^{-1}\right)$,
$$\Delta(D, \mathbb{A}_t) \leq \Delta(D, \mathbb{A}_{t+i});$$
- when $\mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{A}_t^\star}^{-1}\right) \leq \mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{B}_t^\star}^{-1}\right)$ and $\mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{A}_{t+i}^\star}^{-1}\right) \geq \mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{B}_{t+i}^\star}^{-1}\right)$,
$$\Delta(D, \mathbb{A}_t) \geq \Delta(D, \mathbb{A}_{t+i}).$$

The proofs of Theorem 2 and Theorem 3 are available in Appendix B.

Example 1: Consider an encoder and five users. Let $D = 0.1$, $\sigma_X^2 = 2$, and $\mathbf{\Sigma}_{\mathcal{L}} = \begin{bmatrix} 1 & 0.8 & 0.9 & 0.7 & 0.6 \end{bmatrix}^\intercal$.

From the definitions of $\mathbf{\Sigma}_{\mathcal{A}_t^\star}$ and $\mathbf{\Sigma}_{\mathcal{B}_t^\star}$, we have $\mathbf{\Sigma}_{\mathcal{A}_5^\star} = \mathrm{diag}(1, 0.8, 0.9, 0.7, 0.6)$ and $\mathbf{\Sigma}_{\mathcal{B}_5^\star} = \mathrm{diag}(0.8, 0.9, 0.7, 0.6)$. Hence, $\mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{A}_5^\star}^{-1}\right) = 6.4563$ and $\mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{B}_5^\star}^{-1}\right) = 5.4563$. Plugging these in Theorem 1 results to $R \geq 0.2618$ and $\Delta \geq 2.085$.

When $t = 4$, $\mathbf{\Sigma}_{\mathcal{A}_4^\star} = \mathrm{diag}(1, 0.8, 0.9, 0.7)$ and $\mathbf{\Sigma}_{\mathcal{B}_4^\star} = \mathrm{diag}(0.8, 0.7, 0.6)$. Hence, $\mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{A}_4^\star}^{-1}\right) = 4.7897$ and $\mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{B}_4^\star}^{-1}\right) = 4.3452$, and by Theorem 1, $R \geq 0.4594$ and $\Delta \geq 2.1282$.

When $t = 3$, $\mathbf{\Sigma}_{\mathcal{A}_3^\star} = \mathrm{diag}(1, 0.9, 0.8)$ and $\mathbf{\Sigma}_{\mathcal{B}_3^\star} = \mathrm{diag}(0.7, 0.6)$. Hence, $\mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{A}_3^\star}^{-1}\right) = 3.3611$ and $\mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{B}_3^\star}^{-1}\right) = 3.0952$, and by Theorem 1, $R \geq 0.6865$ and $\Delta \geq 2.1415$.

Finally, when $t = 2$, $\mathbf{\Sigma}_{\mathcal{A}_2^\star} = \mathrm{diag}(1, 0.9)$ and $\mathbf{\Sigma}_{\mathcal{B}_2^\star} = 0.6$. Therefore, $\mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{A}_2^\star}^{-1}\right) = 2.1111$ and $\mathrm{tr}\left(\mathbf{\Sigma}_{\mathcal{B}_2^\star}^{-1}\right) = 0.6$, and by Theorem 1, $R \geq 0.9686$ and $\Delta \geq 2.1282$.

This example verifies the relationships between the compression rate and the leakage rate for different thresholds

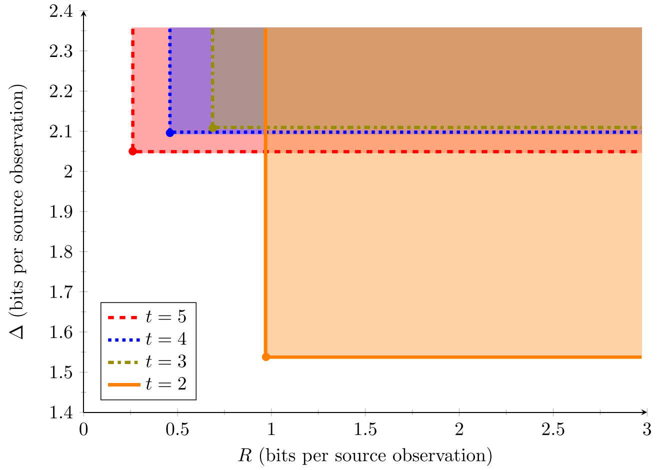

Fig. 3. The rate-leakage region for threshold access structures when $D = 0.1$, $\sigma_X^2 = 2$, and $\mathbf{\Sigma}_{\mathcal{L}} = \begin{bmatrix}1 & 0.8 & 0.9 & 0.7 & 0.6\end{bmatrix}^\intercal$.

provided in Theorem 2 and Theorem 3. For instance, in Theorem 3 for $t = 3$ and $i = 1$, we operate in the second case and the condition $\frac{\sigma_X^{-2}+\mathrm{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{B}^\star_t})}{\sigma_X^{-2}+\mathrm{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{A}^\star_t})} \geq \frac{\sigma_X^{-2}+\mathrm{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{B}^\star_{t+i}})}{\sigma_X^{-2}+\mathrm{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{A}^\star_{t+i}})}$ is satisfied so that $\Delta(D, \mathbb{A}_t) \geq \Delta(D, \mathbb{A}_{t+i})$, which is consistent with Fig. 3.

V. Converse Proof of Theorem 1

In Section V-A, we provide a general outer region on the rate-leakage region $\mathcal{R}(D, \mathbb{A})$. In Sections V-B, V-C, and V-D, we show that this outer region reduces to the region in Theorem 1. Specifically, we convert the problem to a scalar problem by using sufficient statistics in Section V-B. Then, in Section V-C, we study the case when the side information of any set of authorized users is more correlated, in a sense that we make precise in the sequel, with the source than the side information of any unauthorized set of users. Finally, in Section V-D, we study the case when the side information of the unauthorized sets of users is more correlated with the source than with the side information of the authorized sets of users.

A. A General Outer Region

We first provide a general outer region on the secure rate-distortion region of the problem defined in Section III, which is based on [9, Sec. III-B].

Theorem 4: For every $(\mathbb{A}, \mathbb{B})$, the region $\mathcal{R}(D, \mathbb{A})$ is included in $\bigcap_{(\mathcal{A},\mathcal{B})\in(\mathbb{A},\mathbb{B})} \mathcal{R}_G(\mathbf{Y}_{\mathcal{A}}, \mathbf{Y}_{\mathcal{B}})$, where

$$\mathcal{R}_G(\mathbf{Y}_{\mathcal{A}}, \mathbf{Y}_{\mathcal{B}}) \triangleq \bigcup_{\substack{U-V-X-(\mathbf{Y}_{\mathcal{A}},\mathbf{Y}_{\mathcal{B}})\\ \mathbb{E}\left[\sigma^2_{X|\mathbf{Y}_{\mathcal{A}},V}\right]\leq D}} \left\{\begin{array}{l}(R, \Delta) :\\ R > I(V; X|\mathbf{Y}_{\mathcal{A}})\\ \Delta > I(V; X) - I(V; \mathbf{Y}_{\mathcal{A}}|U) + I(X; \mathbf{Y}_{\mathcal{B}}|U)\end{array}\right\}.$$

Proof: Consider the secure source coding problem in [9, Sec. III-B], which consists of a memoryless source $\left((\mathcal{X}, \mathcal{Y}_1, \mathcal{Y}_2), P_{XY_1Y_2}\right)$ with three outputs X^n, at the encoder, Y_1^n, at the legitimate terminal, and Y_2^n, at the eavesdropper. In this setting, the encoder wishes to encode its observed sequence in such a way that the legitimate receiver can reconstruct the source sequence X^n with distortion D, and the information leakage about X^n at the eavesdropper is minimized. An (n, R)-code for source coding is defined by an encoding function $f : \mathcal{X}^n \to [\![1 : 2^{nR}]\!]$ and a decoding function $g : [\![1 : 2^{nR}]\!] \times \mathcal{Y}_1^n \to \mathcal{X}^n$. In this problem, a pair $(R, \Delta) \in \mathbb{R}^2_+$ is achievable if there exists a sequence of (n, R)-codes such that,

$$\limsup_{n\to\infty} \mathbb{E}\left[d\left(x^n, \hat{X}(f(X^n), Y_1^n)\right)\right] \leq D, \tag{7a}$$

$$\lim_{n\to\infty} \frac{1}{n} I\left(X^n; V^n, Y_2^n\right) \leq \Delta, \tag{7b}$$

where $V^n \triangleq f(X^n)$. The outer region derived for this problem in [9, Sec. III-B] is $\mathcal{R}_G(Y_1, Y_2)$. Now, consider the secure source coding problem defined in Section III and the rate pair $(R, \Delta) \in \mathcal{R}(D, \mathbb{A})$ such that (1a) and (1b) are satisfied. In particular, (7) is satisfied for any $\mathcal{A} \in \mathbb{A}$ and $\mathcal{B} \in \mathbb{B}$ when Y_1^n is replaced by $\mathbf{Y}^n_{\mathcal{A}}$ and Y_2^n is replaced by $\mathbf{Y}^n_{\mathcal{B}}$. It means that for any $\mathcal{A} \in \mathbb{A}$ and $\mathcal{B} \in \mathbb{B}$, $(R, \Delta) \in \mathcal{R}_G(\mathbf{Y}_{\mathcal{A}}, \mathbf{Y}_{\mathcal{B}})$ and Theorem 4 holds.

The proof that the distortion constraint in $\mathcal{R}_G(\mathbf{Y}_{\mathcal{A}}, \mathbf{Y}_{\mathcal{B}})$ reduces to $\mathbb{E}\left[\sigma^2_{X|\mathbf{Y}_{\mathcal{A}},V}\right] \leq D$ for Gaussian sources can be found in Appendix C. ■

Remark 2 (Leakage Measure): In [9, Th. 3], the equivocation is used as a measure of leakage but, since we consider continuous sources in our setting, to avoid a negative equivocation, we replace the equivocation with mutual information leakage (see Definition 2).

B. Conversion to a Scalar Problem

To prove the converse part of Theorem 1, we use the notion of sufficient statistics [14, Sec. 2.9] and the following lemma from [29] to convert the problem in (3) to a problem in which the encoder, the authorized users, and the unauthorized users observe a scalar Gaussian source.

Lemma 1 [29, Lemma 3.1]: Consider the channel with input X and output $\mathbf{Y}$ given by

$$\mathbf{Y} = \mathbf{h}X + \mathbf{N},$$

where $\mathbf{N}$ is a zero-mean Gaussian vector with covariance matrix $\mathbf{\Sigma}$ and $\mathbf{h} \in \mathbb{R}^n$. A sufficient statistic to correctly determine X from $\mathbf{Y}$ is the following scalar

$$\tilde{Y} \triangleq \mathbf{h}^\intercal \mathbf{\Sigma}^{-1} \mathbf{Y}.$$

Fix $\mathcal{A} \in \mathbb{A}$ and $\mathcal{B} \in \mathbb{B}$. By Lemma 1, sufficient statistics to correctly determine X from $\mathbf{Y}_{\mathcal{A}}$ and $\mathbf{Y}_{\mathcal{B}}$ in (3) are the following scalars,

$$\tilde{Y}_{\mathcal{A}} = \mathbf{1}^\intercal_{\mathcal{A}} \mathbf{\Sigma}^{-1}_{\mathcal{A}} \mathbf{Y}_{\mathcal{A}}, \quad \tilde{Y}_{\mathcal{B}} = \mathbf{1}^\intercal_{\mathcal{B}} \mathbf{\Sigma}^{-1}_{\mathcal{B}} \mathbf{Y}_{\mathcal{B}}. \tag{8}$$

Hence, we have

$$V^n - X^n - \mathbf{Y}^n_{\mathcal{A}} - \tilde{Y}^n_{\mathcal{A}}, \tag{9a}$$

$$V^n - X^n - \tilde{Y}^n_{\mathcal{A}} - \mathbf{Y}^n_{\mathcal{A}}, \tag{9b}$$

$$V^n - X^n - \mathbf{Y}^n_{\mathcal{B}} - \tilde{Y}^n_{\mathcal{B}}, \tag{9c}$$
$$V^n - X^n - \tilde{Y}^n_{\mathcal{B}} - \mathbf{Y}^n_{\mathcal{B}}, \tag{9d}$$

where

- the Markov chain in (9a) follows since V^n is a function of X^n and $\tilde{Y}^n_{\mathcal{A}}$ is a function of $\mathbf{Y}^n_{\mathcal{A}}$;
- the Markov chain in (9b) follows since V^n is a function of X^n and from [14, Sec. 2.9] $X^n - \tilde{Y}^n_{\mathcal{A}} - \mathbf{Y}^n_{\mathcal{A}}$;
- the Markov chains in (9c) and (9d) are obtained similarly.

Next we rewrite (3) as

$$\tilde{Y}_{\mathcal{A}} = h_{\mathcal{A}} X + \tilde{N}_{\mathcal{A}}, \quad \tilde{Y}_{\mathcal{B}} = h_{\mathcal{B}} X + \tilde{N}_{\mathcal{B}}, \tag{9e}$$

where

$$h_{\mathcal{A}} \triangleq \mathbf{1}^{\mathsf{T}}_{\mathcal{A}} \mathbf{\Sigma}^{-1}_{\mathcal{A}} \mathbf{1}_{\mathcal{A}} = \mathrm{tr}\Big(\mathbf{\Sigma}^{-1}_{\mathcal{A}}\Big), \tag{9f}$$
$$h_{\mathcal{B}} \triangleq \mathbf{1}^{\mathsf{T}}_{\mathcal{B}} \mathbf{\Sigma}^{-1}_{\mathcal{B}} \mathbf{1}_{\mathcal{B}} = \mathrm{tr}\Big(\mathbf{\Sigma}^{-1}_{\mathcal{B}}\Big), \tag{9g}$$
$$\tilde{N}_{\mathcal{A}} = \mathbf{1}^{\mathsf{T}}_{\mathcal{A}} \mathbf{\Sigma}^{-1}_{\mathcal{A}} \mathbf{N}_{\mathcal{A}}, \quad \tilde{N}_{\mathcal{B}} = \mathbf{1}^{\mathsf{T}}_{\mathcal{B}} \mathbf{\Sigma}^{-1}_{\mathcal{B}} \mathbf{N}_{\mathcal{B}}, \tag{9h}$$

where (9g) follows since $\mathbf{\Sigma}_{\mathcal{A}}$ and $\mathbf{\Sigma}_{\mathcal{B}}$ are diagonal matrices.

We now show that the sufficient statistics in (8) preserves the distortion constraint and the leakage constraint in Definition 2. By the distortion constraint in Theorem 4, we have

$$D \geq \frac{1}{n} \sum_{i=1}^{n} \mathbb{E}\Big[\big(X_i - \mathbb{E}[X_i | V^n, \mathbf{Y}^n_{\mathcal{A}}]\big)^2\Big]. \tag{10}$$

Expanding the Right Hand Side (RHS) of (10) results to,

$$\begin{aligned}
&\mathbb{E}\Big[\big(X_i - \mathbb{E}[X_i|V^n, \mathbf{Y}^n_{\mathcal{A}}]\big)^2\Big] \\
&= \int_{x_i}\int_{v^n}\int_{\mathbf{y}^n_{\mathcal{A}}} \big(x_i - \mathbb{E}\big[X_i|v^n, \mathbf{y}^n_{\mathcal{A}}\big]\big)^2 P\big(x_i, v^n, \mathbf{y}^n_{\mathcal{A}}\big) dx_i dv^n d\mathbf{y}^n_{\mathcal{A}} \\
&= \int_{x_i}\int_{v^n}\int_{\mathbf{y}^n_{\mathcal{A}}}\int_{\tilde{y}^n_{\mathcal{A}}} \big(x_i - \mathbb{E}\big[X_i|v^n, \mathbf{y}^n_{\mathcal{A}}\big]\big)^2 \\
&\quad \times P\big(x_i, v^n, \mathbf{y}^n_{\mathcal{A}}, \tilde{y}^n_{\mathcal{A}}\big) dx_i dv^n d\mathbf{y}^n_{\mathcal{A}} d\tilde{y}^n_{\mathcal{A}} \\
&\overset{(a)}{=} \int_{x_i}\int_{v^n}\int_{\mathbf{y}^n_{\mathcal{A}}}\int_{\tilde{y}^n_{\mathcal{A}}} \left(x_i - \int_{\tilde{x}_i} \tilde{x}_i P(\tilde{x}_i|v^n, \mathbf{y}^n_{\mathcal{A}}) d\tilde{x}_i\right)^2 \\
&\quad \times P\big(x_i, v^n, \mathbf{y}^n_{\mathcal{A}}, \tilde{y}^n_{\mathcal{A}}\big) dx_i dv^n d\mathbf{y}^n_{\mathcal{A}} d\tilde{y}^n_{\mathcal{A}} \\
&\overset{(b)}{=} \int_{x_i}\int_{v^n}\int_{\mathbf{y}^n_{\mathcal{A}}}\int_{\tilde{y}^n_{\mathcal{A}}} \left(x_i - \int_{\tilde{x}_i} \tilde{x}_i P(\tilde{x}_i|v^n, \tilde{y}^n_{\mathcal{A}}) d\tilde{x}_i\right)^2 \\
&\quad \times P\big(x_i, v^n, \mathbf{y}^n_{\mathcal{A}}, \tilde{y}^n_{\mathcal{A}}\big) dx_i dv^n d\mathbf{y}^n_{\mathcal{A}} d\tilde{y}^n_{\mathcal{A}} \\
&= \int_{x_i}\int_{v^n}\int_{\tilde{y}^n_{\mathcal{A}}} \left(x_i - \int_{\tilde{x}_i} \tilde{x}_i P(\tilde{x}_i|v^n, \tilde{y}^n_{\mathcal{A}}) d\tilde{x}_i\right)^2 \\
&\quad \times P\big(x_i, v^n, \tilde{y}^n_{\mathcal{A}}\big) dx_i dv^n d\tilde{y}^n_{\mathcal{A}} \\
&= \mathbb{E}\Big[\big(X_i - E[X_i|V^n, \tilde{Y}^n_{\mathcal{A}}]\big)^2\Big],
\end{aligned}$$

where

(*a*) follows since $\mathbb{E}[X_i|v^n, \mathbf{y}^n_{\mathcal{A}}] = \int_{\tilde{x}_i} \tilde{x}_i P(\tilde{x}_i|v^n, \mathbf{y}^n_{\mathcal{A}}) d\tilde{x}_i$;

(*b*) follows from $P(\tilde{x}_i|v^n, \mathbf{y}^n_{\mathcal{A}}) = P(\tilde{x}_i|v^n, \mathbf{y}^n_{\mathcal{A}}, \tilde{y}^n_{\mathcal{A}}) = P(\tilde{x}_i|v^n, \tilde{y}^n_{\mathcal{A}})$ by the Markov chains in (9a) and (9b).

Therefore, rewriting (3) as (8) preserves the distortion constraint. We now show that it also preserves the information leakage,

$$\begin{aligned}
I\big(X^n; M, \mathbf{Y}^n_{\mathcal{B}}\big) &= I\big(X^n; V^n, \mathbf{Y}^n_{\mathcal{B}}\big) \\
&= I\big(X^n; V^n\big) + I\big(X^n; \mathbf{Y}^n_{\mathcal{B}}|V^n\big) \\
&\overset{(a)}{=} I\big(X^n; V^n\big) + I\big(X^n; \mathbf{Y}^n_{\mathcal{B}}, \tilde{Y}^n_{\mathcal{B}}|V^n\big) \\
&\overset{(b)}{=} I\big(X^n; V^n\big) + I\big(X^n; \tilde{Y}^n_{\mathcal{B}}|V^n\big) \\
&= I\big(X^n; V^n, \tilde{Y}^n_{\mathcal{B}}\big),
\end{aligned}$$

where (*a*) and (*b*) follow from (9c) and (9d), respectively. Next, when $\mathrm{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{B}}) \leq \mathrm{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{A}})$, we redefine $\tilde{Y}_{\mathcal{B}}$ as,

$$\tilde{Y}_{\mathcal{B}} = \frac{h_{\mathcal{B}}}{h_{\mathcal{A}}} \tilde{Y}_{\mathcal{A}} + N',$$

where $N' \sim \mathcal{N}(0, \mathrm{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{B}})(1 - \frac{\mathrm{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{B}})}{\mathrm{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{A}})}))$. Note that after redefining $\tilde{Y}_{\mathcal{B}}$, the joint distribution between X and $\tilde{Y}_{\mathcal{A}}$ and the joint distribution between X and $\tilde{Y}_{\mathcal{B}}$ are preserved, therefore the constraints in Definition 2 are preserved. As a result, we have the Markov chain $X - \tilde{Y}_{\mathcal{A}} - \tilde{Y}_{\mathcal{B}}$. Hence, when $\mathrm{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{B}}) \leq \mathrm{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{A}})$, without loss of generality, we can suppose that $X - \tilde{Y}_{\mathcal{A}} - \tilde{Y}_{\mathcal{B}}$. In this first case, we informally say that the authorized set of users have better side information. Similarly, when $\mathrm{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{A}}) < \mathrm{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{B}})$, we can suppose that $X - \tilde{Y}_{\mathcal{B}} - \tilde{Y}_{\mathcal{A}}$. In this second case, we informally say that the unauthorized set of users have a better side information.

We now study each of these two cases separately in Sections V-C and V-D.

C. When Authorized Users Have Better Side Information

Fix $\mathcal{A} \in \mathbb{A}$, and $\mathcal{B} \in \mathbb{B}$. Suppose $\mathrm{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{B}}) \leq \mathrm{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{A}})$. In this case, as discussed in Section V-B, the union in Theorem 4 can be taken over $(U, V, X, \tilde{Y}_{\mathcal{A}}, \tilde{Y}_{\mathcal{B}})$ such that $U - V - X - \tilde{Y}_{\mathcal{A}} - \tilde{Y}_{\mathcal{B}}$. Then,

$$\begin{aligned}
\Delta &\geq I(V; X) - I\big(V; \tilde{Y}_{\mathcal{A}}|U\big) + I\big(X; \tilde{Y}_{\mathcal{B}}|U\big) \\
&\overset{(a)}{=} I(V; X) - I\big(V; \tilde{Y}_{\mathcal{A}}\big) + I\big(U; \tilde{Y}_{\mathcal{A}}\big) + I\big(X; \tilde{Y}_{\mathcal{B}}\big) - I\big(U; \tilde{Y}_{\mathcal{B}}\big) \\
&\overset{(b)}{\geq} I(V; X) - I\big(V; \tilde{Y}_{\mathcal{A}}\big) + I\big(X; \tilde{Y}_{\mathcal{B}}\big) \\
&\overset{(c)}{=} I\big(V; X|\tilde{Y}_{\mathcal{A}}\big) + I\big(X; \tilde{Y}_{\mathcal{B}}\big),
\end{aligned}$$

where (*a*), (*b*), and (*c*) follow since $U - V - X - \tilde{Y}_{\mathcal{A}} - \tilde{Y}_{\mathcal{B}}$. This implies that the region in Theorem 4 is included in the following region

$$\bigcap_{(\mathcal{A},\mathcal{B})\in(\mathbb{A},\mathbb{B})} \bigcup_{\substack{V - X - \tilde{Y}_{\mathcal{A}} - \tilde{Y}_{\mathcal{B}} \\ \mathbb{E}\left[\sigma^2_{X|\tilde{Y}_{\mathcal{A}},V}\right] \leq D}} \left\{\begin{array}{l} (R, \Delta) : \\ R > I\big(V; X|\tilde{Y}_{\mathcal{A}}\big) \\ \Delta > I\big(V; X|\tilde{Y}_{\mathcal{A}}\big) + I\big(X; \tilde{Y}_{\mathcal{B}}\big) \end{array}\right\}. \tag{11}$$

Optimizing the rate and the leakage constraints in (11) separately results in a larger region, i.e., an outer region. As a result, the region in (11) is included in the following region,

$$\bigcap_{(\mathcal{A},\mathcal{B})\in(\mathbb{A},\mathbb{B})}\left\{\begin{array}{l}(R,\Delta):\\ R>\displaystyle\min_{\substack{V-X-\tilde{Y}_{\mathcal{A}}-\tilde{Y}_{\mathcal{B}}\\ \mathbb{E}\left[\sigma^2_{X|\tilde{Y}_{\mathcal{A}},V}\right]\leq D}} I\big(V;X|\tilde{Y}_{\mathcal{A}}\big)\\ \Delta>\displaystyle\min_{\substack{V-X-\tilde{Y}_{\mathcal{A}}-\tilde{Y}_{\mathcal{B}}\\ \mathbb{E}\left[\sigma^2_{X|\tilde{Y}_{\mathcal{A}},V}\right]\leq D}}\big[I\big(V;X|\tilde{Y}_{\mathcal{A}}\big)+I\big(X;\tilde{Y}_{\mathcal{B}}\big)\big]\end{array}\right\}. \tag{12}$$

Since the source is Gaussian the term $I(X;\tilde{Y}_{\mathcal{B}})$ is fixed, and we know that the term $I(V;X|\tilde{Y}_{\mathcal{A}})=\mathbb{h}(X|\tilde{Y}_{\mathcal{A}})-\mathbb{h}(X|\tilde{Y}_{\mathcal{A}},V)$ is minimized by joint Gaussian $(V,X,\tilde{Y}_{\mathcal{A}})$ [30, Lemma 1]. Hence, the region in (12) is again included in the intersection of all $(\mathcal{A},\mathcal{B})\in(\mathbb{A},\mathbb{B})$, i.e., $\bigcap_{(\mathcal{A},\mathcal{B})\in(\mathbb{A},\mathbb{B})}$ of the following region,

$$\left\{\begin{array}{l}(R,\Delta):\\ R>\displaystyle\min_{\sigma^2_{X|\tilde{Y}_{\mathcal{A}},V}\leq D}\tfrac{1}{2}\log\frac{\sigma^2_{X|\tilde{Y}_{\mathcal{A}}}}{\sigma^2_{X|\tilde{Y}_{\mathcal{A}},V}}\\ \Delta>\displaystyle\min_{\sigma^2_{X|\tilde{Y}_{\mathcal{A}},V}\leq D}\left[\tfrac{1}{2}\log\frac{\sigma^2_{X|\tilde{Y}_{\mathcal{A}}}}{\sigma^2_{X|\tilde{Y}_{\mathcal{A}},V}}+\tfrac{1}{2}\log\frac{\sigma^2_X}{\sigma^2_{X|\tilde{Y}_{\mathcal{B}}}}\right]\end{array}\right\}.$$

From the monotonicity of the log function, the region above is included,

$$\bigcap_{(\mathcal{A},\mathcal{B})\in(\mathbb{A},\mathbb{B})}\left\{\begin{array}{l}(R,\Delta):\\ R>\tfrac{1}{2}\log\frac{\sigma^2_{X|\tilde{Y}_{\mathcal{A}}}}{D}\\ \Delta>\tfrac{1}{2}\log\frac{\sigma^2_{X|\tilde{Y}_{\mathcal{A}}}}{D}+\tfrac{1}{2}\log\frac{\sigma^2_X}{\sigma^2_{X|\tilde{Y}_{\mathcal{B}}}}\end{array}\right\}. \tag{13}$$

Now we have,

$$\begin{aligned}\sigma^2_{X|\tilde{Y}_{\mathcal{A}}}&=\sigma^2_X-\frac{\sigma^2_{X,\tilde{Y}_{\mathcal{A}}}}{\sigma^2_{\tilde{Y}_{\mathcal{A}}}}\\ &\overset{(a)}{=}\sigma^2_X-\frac{h^2_{\mathcal{A}}\sigma^4_X}{h^2_{\mathcal{A}}\sigma^2_X+\operatorname{tr}\left(\mathbf{\Sigma}^{-1}_{\mathcal{A}}\right)}\\ &\overset{(b)}{=}\sigma^2_X-\frac{\operatorname{tr}\left(\mathbf{\Sigma}^{-1}_{\mathcal{A}}\right)\sigma^4_X}{\operatorname{tr}\left(\mathbf{\Sigma}^{-1}_{\mathcal{A}}\right)\sigma^2_X+1}\\ &=\frac{\sigma^2_X}{\operatorname{tr}\left(\mathbf{\Sigma}^{-1}_{\mathcal{A}}\right)\sigma^2_X+1},\end{aligned}\tag{14a}$$

where
(a) follows by calculating $\sigma^2_{X,\tilde{Y}_{\mathcal{A}}}$ and $\sigma^2_{\tilde{Y}_{\mathcal{A}}}$ from (8);
(b) follows since from (8) we have $h_{\mathcal{A}}=\operatorname{tr}\left(\mathbf{\Sigma}^{-1}_{\mathcal{A}}\right)$.
Similarly, we have

$$\sigma^2_{X|\tilde{Y}_{\mathcal{B}}}=\frac{\sigma^2_X}{\operatorname{tr}\left(\mathbf{\Sigma}^{-1}_{\mathcal{B}}\right)\sigma^2_X+1}. \tag{14b}$$

Hence, the region in (13) can be written as the intersection of all $(\mathcal{A},\mathcal{B})\in(\mathbb{A},\mathbb{B})$, i.e., $\bigcap_{(\mathcal{A},\mathcal{B})\in(\mathbb{A},\mathbb{B})}$ of the following region,

$$\left\{\begin{array}{l}(R,\Delta):\\ R>\tfrac{1}{2}\log\frac{\sigma^2_X}{D\left(\operatorname{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{A}})\sigma^2_X+1\right)}\\ \Delta>\tfrac{1}{2}\log\frac{\sigma^2_X}{D\left(\operatorname{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{A}})\sigma^2_X+1\right)}+\tfrac{1}{2}\log\left(\operatorname{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{B}})\sigma^2_X+1\right)\end{array}\right\}. \tag{15}$$

Since the arguments of the log functions are decreasing in $\operatorname{tr}\left(\mathbf{\Sigma}^{-1}_{\mathcal{A}}\right)$ and increasing in $\operatorname{tr}\left(\mathbf{\Sigma}^{-1}_{\mathcal{B}}\right)$ we can compute the intersection in (15) and rewrite the region in (15) as follows,

$$.\left\{\begin{array}{l}(R,\Delta):\\ R>\tfrac{1}{2}\log\frac{\sigma^2_X}{D\left(\operatorname{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{A}^\star})\sigma^2_X+1\right)}\\ \Delta>\tfrac{1}{2}\log\frac{\sigma^2_X}{D\left(\operatorname{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{A}^\star})\sigma^2_X+1\right)}+\tfrac{1}{2}\log\left(\operatorname{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{B}^\star})\sigma^2_X+1\right)\end{array}\right\},$$

where $\mathcal{A}^\star\in\operatorname{argmin}_{\mathcal{A}\in\mathbb{A}}\{\operatorname{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{A}})\}$ and $\mathcal{B}^\star\in\operatorname{argmax}_{\mathcal{B}\in\mathbb{B}}\{\operatorname{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{B}})\}$. Note that we also have $\Delta\geq I(X;\mathbf{Y}_{\mathcal{B}^\star})=\frac{1}{2}\log(1+\sigma^2_X\operatorname{tr}\left(\mathbf{\Sigma}^{-1}_{\mathcal{B}^\star}\right))$, whence the definition of g_1, in Theorem 1.

D. When Unauthorized Users Have Better Side Information

Fix $\mathcal{A}\in\mathbb{A}$, $\mathcal{B}\in\mathbb{B}$, and suppose that $\operatorname{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{A}})<\operatorname{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{B}})$. We will need the following lemma.

Lemma 2: Consider $Y=hX+N$, where h is a constant, and X and N are independent, zero-mean Gaussian random variables with variance σ^2_X and σ^2_N, respectively. When $D\leq\sigma^2_{X|Y}$ and V is Gaussian, we have

- $\frac{\sigma^2_N}{h^2}-D>0$;
- $\sigma^2_{X|V,Y}\leq D\Leftrightarrow\sigma^2_{X|V}\leq(D^{-1}-h^2\sigma_N^{-2})^{-1}$;
- $\sigma^2_{X|V,Y}=D\Leftrightarrow\sigma^2_{X|V}=(D^{-1}-h^2\sigma_N^{-2})^{-1}$.

The proof of Lemma 2 is provided in Appendix D.

As discussed in Section V-B, the union in Theorem 4 can be taken over $(U,V,X,\tilde{Y}_{\mathcal{A}},\tilde{Y}_{\mathcal{B}})$ such that $U-V-X-\tilde{Y}_{\mathcal{B}}-\tilde{Y}_{\mathcal{A}}$. Similar to Section V-C, optimizing the rate and equivocation constraints in Theorem 4 separately results in a larger region, i.e., an outer region. Optimizing the rate in Theorem 4 yields,

$$\begin{aligned}R&\geq\min_{\substack{V-X-\tilde{Y}_{\mathcal{A}}\\ \mathbb{E}\left[\sigma^2_{X|\tilde{Y}_{\mathcal{A}},V}\right]\leq D}} I\big(V;X|\tilde{Y}_{\mathcal{A}}\big)\\ &\geq\frac{1}{2}\log\frac{\sigma^2_X}{D\left(\operatorname{tr}(\mathbf{\Sigma}^{-1}_{\mathcal{A}})\sigma^2_X+1\right)},\end{aligned}\tag{16}$$

where the last inequality holds as in the derivation of (15).

Now optimizing the information leakage constraint in Theorem 4 yields,

$$\begin{aligned}\Delta>&\min_{\substack{U-V-X-\tilde{Y}_{\mathcal{B}}-\tilde{Y}_{\mathcal{A}}\\ \mathbb{E}\left[\sigma^2_{X|\tilde{Y}_{\mathcal{A}},V}\right]\leq D}}\big[I(V;X)-I\big(V;\tilde{Y}_{\mathcal{A}}|U\big)+I\big(X;\tilde{Y}_{\mathcal{B}}|U\big)\big]\\ \overset{(a)}{=}&\min_{\substack{U-V-X-\tilde{Y}_{\mathcal{B}}-\tilde{Y}_{\mathcal{A}}\\ \mathbb{E}\left[\sigma^2_{X|\tilde{Y}_{\mathcal{A}},V}\right]\leq D}}\big[I(V;X)-I\big(V;\tilde{Y}_{\mathcal{A}}\big)+I\big(U;\tilde{Y}_{\mathcal{A}}\big)\end{aligned}$$

$$
\begin{aligned}
&\quad + I\big(X;\tilde{Y}_{\mathcal{B}}\big) - I\big(U;\tilde{Y}_{\mathcal{B}}\big)\big] \\
&\overset{(b)}{=} I\big(X;\tilde{Y}_{\mathcal{B}}\big) + \min_{\substack{U-V-X-\tilde{Y}_{\mathcal{B}}-\tilde{Y}_{\mathcal{A}} \\ \mathbb{E}\left[\sigma^2_{X|\tilde{Y}_{\mathcal{A}},V}\right]\le D}} \big[I(V;X) - I\big(V;\tilde{Y}_{\mathcal{A}}\big) \\
&\quad - I\big(U;\tilde{Y}_{\mathcal{B}}|\tilde{Y}_{\mathcal{A}}\big)\big] \\
&\overset{(c)}{\geq} I\big(X;\tilde{Y}_{\mathcal{B}}\big) + \min_{\substack{U-V-X-\tilde{Y}_{\mathcal{B}}-\tilde{Y}_{\mathcal{A}} \\ \mathbb{E}\left[\sigma^2_{X|\tilde{Y}_{\mathcal{A}},V}\right]\le D}} \big[I(V;X) - I\big(V;\tilde{Y}_{\mathcal{A}}\big) \\
&\quad - I\big(V;\tilde{Y}_{\mathcal{B}}|\tilde{Y}_{\mathcal{A}}\big)\big] \\
&= I\big(X;\tilde{Y}_{\mathcal{B}}\big) + \min_{\substack{V-X-\tilde{Y}_{\mathcal{B}}-\tilde{Y}_{\mathcal{A}} \\ \mathbb{E}\left[\sigma^2_{X|\tilde{Y}_{\mathcal{A}},V}\right]\le D}} \big[I(V;X) - I\big(V;\tilde{Y}_{\mathcal{A}},\tilde{Y}_{\mathcal{B}}\big)\big] \\
&\overset{(d)}{=} I\big(X;\tilde{Y}_{\mathcal{B}}\big) + \min_{\substack{V-X-\tilde{Y}_{\mathcal{B}}-\tilde{Y}_{\mathcal{A}} \\ \mathbb{E}\left[\sigma^2_{X|\tilde{Y}_{\mathcal{A}},V}\right]\le D}} \big[I(V;X) - I\big(V;\tilde{Y}_{\mathcal{B}}\big)\big] \\
&\overset{(e)}{=} \min_{\substack{V-X-\tilde{Y}_{\mathcal{B}}-\tilde{Y}_{\mathcal{A}} \\ \mathbb{E}\left[\sigma^2_{X|\tilde{Y}_{\mathcal{A}},V}\right]\le D}} C(V), \qquad (17)
\end{aligned}
$$

where

(a) follows since $U - V - X - \tilde{Y}_{\mathcal{B}} - \tilde{Y}_{\mathcal{A}}$ forms a Markov Chain;

(b) follows since $U - \tilde{Y}_{\mathcal{B}} - \tilde{Y}_{\mathcal{A}}$ forms a Markov Chain;

(c) follows since $U - V - \tilde{Y}_{\mathcal{B}} - \tilde{Y}_{\mathcal{A}}$ forms a Markov Chain;

(d) follows since $V - \tilde{Y}_{\mathcal{B}} - \tilde{Y}_{\mathcal{A}}$ forms a Markov Chain;

(e) follows by defining,

$$
\begin{aligned}
C(V) &\triangleq I\big(X;\tilde{Y}_{\mathcal{B}}\big) + I(V;X) - I\big(V;\tilde{Y}_{\mathcal{B}}\big) \\
&= \mathbb{h}\big(\tilde{Y}_{\mathcal{B}}|V\big) - \mathbb{h}(X|V) + k_1 \\
&= \mathbb{h}\left(\frac{1}{h_{\mathcal{B}}}\tilde{Y}_{\mathcal{B}}|V\right) - \mathbb{h}(X|V) + \log|h_{\mathcal{B}}| + k_1, \\
&= \mathbb{h}\left(\frac{1}{h_{\mathcal{B}}}\tilde{Y}_{\mathcal{B}}|V\right) - \mathbb{h}(X|V) + k_2, \qquad (18)
\end{aligned}
$$

where $k_1 \triangleq I(X;\tilde{Y}_{\mathcal{B}}) + \mathbb{h}(\tilde{Y}_{\mathcal{B}}) - \mathbb{h}(X)$ is a constant which is independent of V and $k_2 \triangleq \log|h_{\mathcal{B}}| + k_1$.

Lemma 3: When X and $\tilde{Y}_{\mathcal{B}}$ are Gaussian random variables, as defined in (9), and $V - X - \tilde{Y}_{\mathcal{B}}$ forms a Markov chain

$$
C(V) \triangleq \mathbb{h}\left(\frac{1}{h_{\mathcal{B}}}\tilde{Y}_{\mathcal{B}}|V\right) - \mathbb{h}(X|V),
$$

is minimized when the auxiliary random variable V is a Gaussian random variable.

Proof: The proof follows from the extremal inequality [31] and [32, Th. 1]. For completeness, we prove Lemma 3 in Appendix E. ■

Hence, we can rewrite the RHS of (17) as follows,

$$
\begin{aligned}
&\min_{\substack{V-X-\tilde{Y}_{\mathcal{B}}-\tilde{Y}_{\mathcal{A}} \\ \mathbb{E}\left[\sigma^2_{X|\tilde{Y}_{\mathcal{A}},V}\right]\le D}} C(V) \\
&\overset{(a)}{=} \min_{\substack{V-X-\tilde{Y}_{\mathcal{B}}-\check{Y}_{\mathcal{A}} \\ V\text{ is Gaussian} \\ \sigma^2_{X|V,\check{Y}_{\mathcal{A}}}\le D}} \big[I\big(X;\tilde{Y}_{\mathcal{B}}\big) + I(V;X) - I\big(V;\tilde{Y}_{\mathcal{B}}\big)\big] \\
&\overset{(b)}{=} \min_{\substack{V-X-\tilde{Y}_{\mathcal{B}}-\check{Y}_{\mathcal{A}} \\ V\text{ is Gaussian} \\ \sigma^2_{X|V}\le F_{\mathcal{A}}(D)}} \big[I\big(X;\tilde{Y}_{\mathcal{B}}\big) + I(V;X) - I\big(V;\tilde{Y}_{\mathcal{B}}\big)\big] \\
&\overset{(c)}{=} \min_{\sigma^2_{X|V}\le F_{\mathcal{A}}(D)} \Bigg[\frac{1}{2}\log\frac{h^2_{\mathcal{B}}\sigma^2_X + \tilde{\sigma}^2_{\mathcal{B}}}{\tilde{\sigma}^2_{\mathcal{B}}} + \frac{1}{2}\log\frac{\sigma^2_X}{\sigma^2_{X|V}} \\
&\qquad - \frac{1}{2}\log\frac{h^2_{\mathcal{B}}\sigma^2_X + \tilde{\sigma}^2_{\mathcal{B}}}{h^2_{\mathcal{B}}\sigma^2_{X|V} + \tilde{\sigma}^2_{\mathcal{B}}}\Bigg] \\
&\overset{(d)}{\geq} \frac{1}{2}\log\frac{h^2_{\mathcal{B}}\sigma^2_X + \tilde{\sigma}^2_{\mathcal{B}}}{\tilde{\sigma}^2_{\mathcal{B}}} + \frac{1}{2}\log\frac{\sigma^2_X}{F_{\mathcal{A}}(D)} \\
&\quad - \frac{1}{2}\log\frac{h^2_{\mathcal{B}}\sigma^2_X + \tilde{\sigma}^2_{\mathcal{B}}}{h^2_{\mathcal{B}}F_{\mathcal{A}}(D) + \tilde{\sigma}^2_{\mathcal{B}}} \\
&\overset{(e)}{=} \frac{1}{2}\log\Big(\mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}})F_{\mathcal{A}}(D) + 1\Big) + \frac{1}{2}\log\frac{\sigma^2_X}{F_{\mathcal{A}}(D)}, \qquad (19)
\end{aligned}
$$

where

(a) follows from Lemma 3;

(b) follows from Lemma 2 with

$$
F_{\mathcal{A}}(D) \triangleq \frac{\tilde{\sigma}^2_{\mathcal{A}}D}{\tilde{\sigma}^2_{\mathcal{A}} - h^2_{\mathcal{A}}D} = \frac{D}{1 - \mathrm{tr}\Big(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}^\star}\Big)D}; \qquad (20)
$$

(c) follows by calculating the mutual information of the random variables defined in (8) using the fact that $\tilde{N}_{\mathcal{B}}$ is independent of (X, V), specifically,

$$
\begin{aligned}
I\big(V;\tilde{Y}_{\mathcal{B}}\big) &= \mathbb{h}\big(\tilde{Y}_{\mathcal{B}}\big) - \mathbb{h}\big(\tilde{Y}_{\mathcal{B}}|V\big) \\
&= \frac{1}{2}\log\Big(2\pi e\big(h^2_{\mathcal{B}}\sigma^2_X + \tilde{\sigma}^2_{\mathcal{B}}\big)\Big) \\
&\quad - \frac{1}{2}\log\Big(2\pi e\big(h^2_{\mathcal{B}}\sigma^2_{X|V} + \tilde{\sigma}^2_{\mathcal{B}}\big)\Big) \\
&= \frac{1}{2}\log\frac{h^2_{\mathcal{B}}\sigma^2_X + \tilde{\sigma}^2_{\mathcal{B}}}{h^2_{\mathcal{B}}\sigma^2_{X|V} + \tilde{\sigma}^2_{\mathcal{B}}};
\end{aligned}
$$

(d) follows since $\frac{h^2_{\mathcal{B}}\sigma^2_{X|V} + \tilde{\sigma}^2_{\mathcal{B}}}{\sigma^2_{X|V}}$ is a monotonically decreasing function in $\sigma^2_{X|V}$;

(e) follows since from (8), $h_{\mathcal{B}} = \tilde{\sigma}^2_{\mathcal{B}} = \mathrm{tr}\Big(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}}\Big)$.

Therefore, by (16), (17), and (19), the region in Theorem 4 is included in the intersection of all $(\mathcal{A},\mathcal{B}) \in (\mathbb{A},\mathbb{B})$, i.e., $\bigcap_{(\mathcal{A},\mathcal{B})\in(\mathbb{A},\mathbb{B})}$ of the following region,

$$
\left\{\begin{array}{l}
(R,\Delta): \\
R > \frac{1}{2}\log\frac{\sigma^2_X}{D\left(\mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}})\sigma^2_X + 1\right)} \\
\Delta > \frac{1}{2}\log\Big(\mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}})F_{\mathcal{A}}(D) + 1\Big) + \frac{1}{2}\log\frac{\sigma^2_X}{F_{\mathcal{A}}(D)}
\end{array}\right\}. \qquad (21)
$$

Then, the region in (21) is included in the following region,

$$
\left\{\begin{array}{l}
(R,\Delta): \\
R > \max\limits_{\mathcal{A}\in\mathbb{A}}\frac{1}{2}\log\frac{\sigma^2_X}{D\left(\mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}})\sigma^2_X + 1\right)} \\
\Delta > \max\limits_{(\mathcal{A},\mathcal{B})\in(\mathbb{A},\mathbb{B})}\frac{1}{2}\log\left(\mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}})\sigma^2_X + \frac{\sigma^2_X}{F_{\mathcal{A}}(D)}\right)
\end{array}\right\}.
$$

Since the arguments of the log function for the bound on R is decreasing in $\mathrm{tr}\Big(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}}\Big)$ and the argument of the log function for the bound on Δ is decreasing in $\mathrm{tr}\left(\boldsymbol{\Sigma}_{\mathcal{A}}^{-1}\right)$ and increasing in $\mathrm{tr}\left(\boldsymbol{\Sigma}_{\mathcal{B}}^{-1}\right)$, we can compute rewrite the region in (21) as follows,

$$\left\{\begin{array}{l}(R, \Delta) : \\ R > \frac{1}{2}\log\frac{\sigma_X^2}{D\left(\mathrm{tr}(\boldsymbol{\Sigma}_{\mathcal{A}^\star}^{-1})\sigma_X^2+1\right)} \\ \Delta > \frac{1}{2}\log\left(\mathrm{tr}(\boldsymbol{\Sigma}_{\mathcal{B}^\star}^{-1})\sigma_X^2 + \frac{\sigma_X^2}{F_{\mathcal{A}^\star}(D)}\right)\end{array}\right\},$$

where $\mathcal{A}^\star \in \mathrm{argmin}_{\mathcal{A}\in\mathbb{A}}\{\mathrm{tr}\left(\boldsymbol{\Sigma}_{\mathcal{A}}^{-1}\right)\}$, $\mathcal{B}^\star \in \mathrm{argmax}_{\mathcal{B}\in\mathbb{B}}\{\mathrm{tr}\left(\boldsymbol{\Sigma}_{\mathcal{B}}^{-1}\right)\}$, and $F_{\mathcal{A}^\star}(D) = \frac{D}{1-\mathrm{tr}\left(\boldsymbol{\Sigma}_{\mathcal{A}^\star}^{-1}\right)D}$.

Note that, from (1b), we have $\Delta \geq I(X;\mathbf{Y}_{\mathcal{B}}) = \frac{1}{2}\log\left(1+\frac{\sigma_X^2}{\mathrm{tr}\left(\boldsymbol{\Sigma}_{\mathcal{B}^\star}^{-1}\right)^{-1}}\right)$. Therefore, we have the following bound on the leakage rate,

$$\Delta \geq \max\left\{\frac{1}{2}\log\left(1+\frac{\sigma_X^2}{\mathrm{tr}(\boldsymbol{\Sigma}_{\mathcal{B}^\star}^{-1})^{-1}}\right),\right.$$
$$\left.\frac{1}{2}\log\left(\frac{\sigma_X^2}{D}+\frac{\sigma_X^2}{\mathrm{tr}(\boldsymbol{\Sigma}_{\mathcal{B}^\star}^{-1})^{-1}}-\frac{\sigma_X^2}{\mathrm{tr}(\boldsymbol{\Sigma}_{\mathcal{A}^\star}^{-1})^{-1}}\right)\right\},$$

which can be written as $g_2(\mathcal{A}^\star, \mathcal{B}^\star)$ defined in Theorem 1.

VI. Conclusion

In this paper, we study a secure source coding problem with multiple users when the encoder and the users observe copies of correlated scalar Gaussian random variables. Specifically, the objective is to guarantee a given distortion level of recovery of the source for some sets of authorized users and simultaneously minimize information leakage about the source for some other sets of users. This can be seen as a secret-sharing problem where perfect reconstruction of the secret is relaxed to an approximate reconstruction, and the perfect security requirement is relaxed to controlled information leakage. Our main result is the characterization of the optimal trade-off between the source compression rate, the desired distortion, and the information leakage for this problem. We note that characterizing this trade-off when the source is a vector Gaussian random variable is an open problem.

Appendix A
Proof of Equation (2)

For the sake of completeness, we present the following theorem from [28, Th. 3.5.2], which is essential in our proof.

Theorem 5 [28]: Let $\mathbf{X}$ and $\mathbf{Y}$ be zero-mean, jointly Gaussian, and jointly non-singular. Then $\mathbf{X}$ can be expressed as $\mathbf{X} = \mathbf{G}\mathbf{Y} + \mathbf{V}$, where $\mathbf{V}$ is statistically independent of $\mathbf{Y}$ and

$$\mathbf{G} = \mathbf{K}_{XY}\mathbf{K}_Y^{-1}$$
$$\mathbf{K}_V = \mathbf{K}_X - \mathbf{K}_{XY}\mathbf{K}_Y^{-1}\mathbf{K}_{XY}^{\intercal}.$$

For every $\mathcal{A} \in \mathbb{A}$, by Theorem 5, we have

$$\mathbf{Y}_{\mathcal{A}} = \boldsymbol{\Sigma}_{X\mathbf{Y}_{\mathcal{A}}}\sigma_X^{-2}X + \mathbf{N}'_{\mathcal{A}}, \tag{22}$$

where $\boldsymbol{\Sigma}_{\mathbf{N}'_{\mathcal{A}}} \triangleq \boldsymbol{\Sigma}_{\mathbf{Y}_{\mathcal{A}}} - \boldsymbol{\Sigma}_{X\mathbf{Y}_{\mathcal{A}}}\sigma_X^{-2}\boldsymbol{\Sigma}_{X\mathbf{Y}_{\mathcal{A}}}^{\intercal}$ and $\boldsymbol{\Sigma}_{\mathbf{N}'_{\mathcal{A}}} \succ 0$ from [28, Eq. (3.43)], since the covariance matrix $\boldsymbol{\Sigma}_{\mathbf{N}'_{\mathcal{A}}}$ is invertible. Next, we normalize (22) as follows. From Cholesky decomposition, there exists an invertible matrix $\mathbf{C} \in \mathbb{R}^{|\mathcal{A}|\times|\mathcal{A}|}$ such that $\boldsymbol{\Sigma}_{\mathbf{N}'_{\mathcal{A}}} = \mathbf{C}\mathbf{C}^{\intercal}$, therefore, we can rewrite (22) as follows

$$\mathbf{Y}'_{\mathcal{A}} = \mathbf{h}_{\mathcal{A}}X + \mathbf{N}''_{\mathcal{A}},$$

where $\mathbf{Y}'_{\mathcal{A}} \triangleq \mathbf{C}^{-1}\mathbf{Y}_{\mathcal{A}}$, $\mathbf{h}_{\mathcal{A}} \triangleq \mathbf{C}^{-1}\boldsymbol{\Sigma}_{X\mathbf{Y}_{\mathcal{A}}}\sigma_X^{-2}$, and $\mathbf{N}''_{\mathcal{A}} \sim \mathcal{N}(0, \mathbf{I}_{|\mathcal{A}|})$. Similarly, for every $\mathcal{B} \in \mathbb{B}$, one can show that

$$\mathbf{Y}'_{\mathcal{B}} = \mathbf{h}_{\mathcal{B}}X + \mathbf{N}''_{\mathcal{B}},$$

where $\mathbf{Y}'_{\mathcal{B}} \triangleq \mathbf{C}^{-1}\mathbf{Y}_{\mathcal{B}}$, $\mathbf{h}_{\mathcal{B}} \triangleq \mathbf{C}^{-1}\boldsymbol{\Sigma}_{X\mathbf{Y}_{\mathcal{B}}}\sigma_X^{-2}$, and $\mathbf{N}''_{\mathcal{B}} \sim \mathcal{N}(0, \mathbf{I}_{|\mathcal{B}|})$.

Appendix B
Proof of Theorem 2 and Theorem 3

We first show that, there exist sets of authorized users $\mathcal{A}_t^\star \in \mathrm{argmin}_{\mathcal{A}\in\mathbb{A}_t}\mathrm{tr}\left(\boldsymbol{\Sigma}_{\mathcal{A}}^{-1}\right)$ and unauthorized users $\mathcal{B}_t^\star \in \mathrm{argmax}_{\mathcal{B}\in\mathbb{B}_t}\mathrm{tr}\left(\boldsymbol{\Sigma}_{\mathcal{B}}^{-1}\right)$ such that for any $t \in \llbracket 1 : L-1\rrbracket$, $\mathcal{A}_t^\star \subset \mathcal{A}_{t+1}^\star$ and $\mathcal{B}_t^\star \subset \mathcal{B}_{t+1}^\star$. Then, by using Theorem 1, we remark that $\mathcal{A}_t^\star$ and $\mathcal{B}_t^\star$ also correspond to the sets that appear in the expression of the optimal compression and the leakage rates for the threshold access structure $\mathbb{A}_t$. Ultimately, using the monotonicity of the sets $\left(\mathcal{A}_t^\star\right)_{t\in\llbracket 1\,:\,L\rrbracket}$ and $\left(\mathcal{B}_t^\star\right)_{t\in\llbracket 1\,:\,L\rrbracket}$ and Theorem 1, we compute necessary and sufficient conditions to determine whether the optimal compression and leakage rates increase or decrease with the threshold t.

Lemma 4: There exist sets $\left(\mathcal{A}_t^\star\right)_{t\in\llbracket 1\,:\,L\rrbracket}$ and $\left(\mathcal{B}_t^\star\right)_{t\in\llbracket 1\,:\,L\rrbracket}$ such that, for any $t \in \llbracket 1 : L-1\rrbracket$, we have $\mathcal{A}_t^\star \subset \mathcal{A}_{t+1}^\star$ and $\mathcal{B}_t^\star \subset \mathcal{B}_{t+1}^\star$, and for any $t \in \llbracket 1 : L\rrbracket$, $\mathcal{A}_t^\star \in \mathrm{argmin}_{\mathcal{A}\in\mathbb{A}_t}\mathrm{tr}\left(\boldsymbol{\Sigma}_{\mathcal{A}}^{-1}\right)$ and $\mathcal{B}_t^\star \in \mathrm{argmax}_{\mathcal{B}\in\mathbb{B}_t}\mathrm{tr}\left(\boldsymbol{\Sigma}_{\mathcal{B}}^{-1}\right)$.

Proof: We write $\boldsymbol{\Sigma}_{\mathcal{L}}$ as $\mathrm{diag}(\sigma_1^2, \ldots, \sigma_L^2)$. Without loss of generality, suppose that $\sigma_1^2 \geq \sigma_2^2 \geq \cdots \geq \sigma_L^2$. For $t \in \llbracket 1 : L-1\rrbracket$, let $\mathcal{A}_t^\star \triangleq \llbracket 1 : t\rrbracket$ and $\mathcal{B}_t^\star \triangleq \llbracket L-t+2 : L\rrbracket$, since $\mathcal{A}_t^\star \in \mathrm{argmin}_{\mathcal{A}:|\mathcal{A}|=t}\sum_{i\in\mathcal{A}}\sigma_i^{-2}$ and $\mathcal{B}_t^\star \in \mathrm{argmax}_{\mathcal{B}:|\mathcal{B}|<t}\sum_{i\in\mathcal{B}}\sigma_i^{-2}$ we have $\mathcal{A}_t^\star \subset \mathcal{A}_{t+1}^\star$ and $\mathcal{B}_t^\star \subset \mathcal{B}_{t+1}^\star$. ■

When $t = L$, from Lemma 4 we have $\mathrm{tr}\left(\boldsymbol{\Sigma}_{\mathcal{A}_L^\star}^{-1}\right) > \mathrm{tr}\left(\boldsymbol{\Sigma}_{\mathcal{B}_L^\star}^{-1}\right)$, therefore, the optimal leakage rate in Theorem 1 is,

$$\Delta(D, \mathbb{A}_L) = \frac{1}{2}\log\frac{\sigma_X^2}{D} - \frac{1}{2}\log\left(1+\frac{\sigma_X^2}{\mathrm{tr}(\boldsymbol{\Sigma}_{\mathcal{A}_L^\star}^{-1})^{-1}}\right)$$
$$+\frac{1}{2}\log\left(1+\frac{\sigma_X^2}{\mathrm{tr}(\boldsymbol{\Sigma}_{\mathcal{B}_L^\star}^{-1})^{-1}}\right) \tag{23a}$$

and for $t \in \llbracket 1 : L-1\rrbracket$ and $\mathrm{tr}\left(\boldsymbol{\Sigma}_{\mathcal{A}_t^\star}^{-1}\right) \geq \mathrm{tr}\left(\boldsymbol{\Sigma}_{\mathcal{B}_t^\star}^{-1}\right)$,

$$\Delta(D, \mathbb{A}_t) = \frac{1}{2}\log\frac{\sigma_X^2}{D} - \frac{1}{2}\log\left(1+\frac{\sigma_X^2}{\mathrm{tr}(\boldsymbol{\Sigma}_{\mathcal{A}_t^\star}^{-1})^{-1}}\right)$$
$$+\frac{1}{2}\log\left(1+\frac{\sigma_X^2}{\mathrm{tr}(\boldsymbol{\Sigma}_{\mathcal{B}_t^\star}^{-1})^{-1}}\right). \tag{23b}$$

By (23a), (23b), and monotonicity of the log function, we have

$$\begin{aligned}\Delta(D, \mathbb{A}_L) &\leq \Delta(D, \mathbb{A}_t)\\ &\Leftrightarrow \frac{\sigma_X^{-2} + \mathrm{tr}\Big(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_t^\star}\Big)}{\sigma_X^{-2} + \mathrm{tr}\Big(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_t^\star}\Big)} \leq \frac{\sigma_X^{-2} + \mathrm{tr}\Big(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_L^\star}\Big)}{\sigma_X^{-2} + \mathrm{tr}\Big(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_L^\star}\Big)}. \quad (23c)\end{aligned}$$

Next, for $t \in [\![1 : L]\!]$, and $\mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_t^\star}\right) \leq \mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_t^\star}\right)$,

$$\Delta(D, \mathbb{A}_t) = \frac{1}{2}\log\left(\frac{\sigma_X^2}{D} + \frac{\mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_t^\star})}{\sigma_X^{-2}} - \frac{\mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_t^\star})}{\sigma_X^{-2}}\right). \quad (23d)$$

Using (23a), (23d), and monotonicity of the log function, we have

$$\begin{aligned}\Delta(D, \mathbb{A}_L) &\leq \Delta(D, \mathbb{A}_t)\\ &\Leftrightarrow \frac{1}{2}\log\left[\frac{\sigma_X^2\Big(\sigma_X^{-2} + \mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_L^\star})\Big)}{D\Big(\sigma_X^{-2} + \mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_L^\star})\Big)}\right]\\ &\leq \frac{1}{2}\log\left(\frac{\sigma_X^2}{D} + \frac{\mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_t^\star})}{\sigma_X^{-2}} - \frac{\mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_t^\star})}{\sigma_X^{-2}}\right)\\ &\Leftrightarrow \mathrm{tr}\Big(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_L^\star}\Big) - \mathrm{tr}\Big(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_L^\star}\Big)\\ &\leq D\Big(\sigma_X^{-2} + \mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_L^\star})\Big)\Big(\mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_t^\star}) - \mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_t^\star})\Big), \quad (23e)\end{aligned}$$

which is always true since the RHS (23e) is positive and the left-hand side of (23e) is negative because $\mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_L^\star}\right) \leq \mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_L^\star}\right)$.

Next, for $i \in [\![1 : L - t]\!]$, by Theorem 1 and using that the log function is increasing, we have

$$R(D, \mathbb{A}_t) \geq R(D, \mathbb{A}_{t+i}) \Leftrightarrow \mathrm{tr}\Big(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_t^\star}\Big) \leq \mathrm{tr}\Big(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_{t+i}^\star}\Big), \quad (24)$$

and (24) is always true by Lemma 4. Note that (24) also proves that for any $t \in [\![1 : L]\!]$, $R(D, \mathbb{A}_t) \geq R(D, \mathbb{A}_L)$.

We now prove Theorem 3. Let $i \in [\![1 : L - t]\!]$. We consider four cases. First, when $\mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_t^\star}\right) \leq \mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_t^\star}\right)$ and $\mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_{t+i}^\star}\right) \leq \mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_{t+i}^\star}\right)$, we have

$$\begin{aligned}\Delta(D, \mathbb{A}_t) &\geq \Delta(D, \mathbb{A}_{t+i})\\ &\Leftrightarrow \frac{1}{2}\log\left(\frac{\sigma_X^2}{D} + \frac{\mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_t^\star})}{\sigma_X^{-2}} - \frac{\mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_t^\star})}{\sigma_X^{-2}}\right)\\ &\geq \frac{1}{2}\log\left(\frac{\sigma_X^2}{D} + \frac{\mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_{t+i}^\star})}{\sigma_X^{-2}} - \frac{\mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_{t+i}^\star})}{\sigma_X^{-2}}\right)\\ &\Leftrightarrow \mathrm{tr}\Big(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_{t+i}^\star}\Big) - \mathrm{tr}\Big(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_t^\star}\Big) \geq \mathrm{tr}\Big(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_{t+i}^\star}\Big) - \mathrm{tr}\Big(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_t^\star}\Big).\\ &\qquad (25)\end{aligned}$$

Second, when $\mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_t^\star}\right) \geq \mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_t^\star}\right)$ and $\mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_{t+i}^\star}\right) \geq \mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_{t+i}^\star}\right)$, we have

$$\begin{aligned}\Delta(D, \mathbb{A}_t) &\geq \Delta(D, \mathbb{A}_{t+i})\\ &\Leftrightarrow \frac{1}{2}\log\left(\frac{\sigma_X^{-2} + \mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_t^\star})}{\sigma_X^{-2} + \mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_t^\star})}\right)\\ &\geq \frac{1}{2}\log\left(\frac{\sigma_X^{-2} + \mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_{t+i}^\star})}{\sigma_X^{-2} + \mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_{t+i}^\star})}\right)\\ &\Leftrightarrow \frac{\sigma_X^{-2} + \mathrm{tr}\Big(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_t^\star}\Big)}{\sigma_X^{-2} + \mathrm{tr}\Big(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_t^\star}\Big)} \geq \frac{\sigma_X^{-2} + \mathrm{tr}\Big(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_{t+i}^\star}\Big)}{\sigma_X^{-2} + \mathrm{tr}\Big(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_{t+i}^\star}\Big)}. \quad (26)\end{aligned}$$

Third, when $\mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_t^\star}\right) \geq \mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_t^\star}\right)$ and $\mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_{t+i}^\star}\right) \leq \mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_{t+i}^\star}\right)$, we have,

$$\begin{aligned}\Delta(D, \mathbb{A}_t) &\geq \Delta(D, \mathbb{A}_{t+i})\\ &\Leftrightarrow \frac{1}{2}\log\left[\frac{\sigma_X^2\Big(\sigma_X^{-2} + \mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_t^\star})\Big)}{D\Big(\sigma_X^{-2} + \mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_t^\star})\Big)}\right]\\ &\geq \frac{1}{2}\log\left(\frac{\sigma_X^2}{D} + \frac{\mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_{t+i}^\star})}{\sigma_X^{-2}} - \frac{\mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_{t+i}^\star})}{\sigma_X^{-2}}\right)\\ &\Leftrightarrow \mathrm{tr}\Big(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_t^\star}\Big) - \mathrm{tr}\Big(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_t^\star}\Big)\\ &\geq D\Big(\sigma_X^{-2} + \mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_t^\star})\Big)\Big(\mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_{t+i}^\star}) - \mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_{t+i}^\star})\Big), \quad (27)\end{aligned}$$

since $\mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_t^\star}\right) - \mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_t^\star}\right) \leq 0$ and $\mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_{t+i}^\star}\right) - \mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_{t+i}^\star}\right) \geq 0$ the inequality in the RHS of (27) is never satisfied and $\Delta(D, \mathbb{A}_t) \leq \Delta(D, \mathbb{A}_{t+i})$. Fourth, when $\mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_t^\star}\right) \leq \mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_t^\star}\right)$ and $\mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_{t+i}^\star}\right) \geq \mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_{t+i}^\star}\right)$, we have,

$$\begin{aligned}\Delta(D, \mathbb{A}_t) &\geq \Delta(D, \mathbb{A}_{t+i})\\ &\Leftrightarrow \frac{1}{2}\log\left(\frac{\sigma_X^2}{D} + \frac{\mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_t^\star})}{\sigma_X^{-2}} - \frac{\mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_t^\star})}{\sigma_X^{-2}}\right)\\ &\geq \frac{1}{2}\log\left[\frac{\sigma_X^2\Big(\sigma_X^{-2} + \mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_{t+i}^\star})\Big)}{D\Big(\sigma_X^{-2} + \mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_{t+i}^\star})\Big)}\right]\\ &\Leftrightarrow D\Big(\sigma_X^{-2} + \mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_{t+i}^\star})\Big)\Big(\mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_t^\star}) - \mathrm{tr}(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_t^\star})\Big)\\ &\geq \mathrm{tr}\Big(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_{t+i}^\star}\Big) - \mathrm{tr}\Big(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_{t+i}^\star}\Big), \quad (28)\end{aligned}$$

since $\mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_t^\star}\right) - \mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_t^\star}\right) \geq 0$ and $\mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{B}_{t+i}^\star}\right) - \mathrm{tr}\left(\boldsymbol{\Sigma}^{-1}_{\mathcal{A}_{t+i}^\star}\right) \leq 0$, the inequality in the RHS of (28) is always satisfied and $\Delta(D, \mathbb{A}_t) \geq \Delta(D, \mathbb{A}_{t+i})$.

APPENDIX C
DISTORTION CONSTRAINT IN THEOREM 4

We have,

$$\begin{aligned}D \quad &\geq \frac{1}{n}\sum_{i=1}^{n}\mathbb{E}\Big(X_i - \mathbb{E}\big[X_i|\mathbf{Y}^n_{\mathcal{A}}, f(X^n)\big]\Big)^2 &(29a)\\ &= \frac{1}{n}\sum_{i=1}^{n}\mathbb{E}\Big[\sigma^2_{X_i|\mathbf{Y}^n_{\mathcal{A}}, f(X^n)}\Big] &(29b)\\ &\overset{(a)}{\geq} \frac{1}{n}\sum_{i=1}^{n}\mathbb{E}\Big[\sigma^2_{X_i|\mathbf{Y}_{\mathcal{A},i}, \mathbf{Y}^n_{\mathcal{A}\sim i}, f(X^n), \mathbf{Y}^{i-1}_{\mathcal{B}}, X^{i-1}}\Big] &(29c)\\ &\overset{(b)}{=} \frac{1}{n}\sum_{i=1}^{n}\mathbb{E}_{\mathbf{Y}_{\mathcal{A},i}, V_i}\Big[\sigma^2_{X_i|\mathbf{Y}_{\mathcal{A},i}, V_i}\Big] &(29d)\end{aligned}$$

$$\overset{(c)}{=} \sum_{i=1}^{n} \mathbb{P}(Q=i)\mathbb{E}_{\mathbf{Y}_{\mathcal{A},Q},V_Q|Q=i}\left[\sigma^2_{X_Q|\mathbf{Y}_{\mathcal{A},Q},V_Q,Q=i}\right] \tag{29e}$$

$$= \mathbb{E}_{\mathbf{Y}_{\mathcal{A},Q},V_Q,Q}\left[\sigma^2_{X_Q|\mathbf{Y}_{\mathcal{A},Q},V_Q,Q}\right] \tag{29f}$$

$$\overset{(d)}{=} \mathbb{E}_{\mathbf{Y}_{\mathcal{A}},V}\left[\sigma^2_{X|\mathbf{Y}_{\mathcal{A}},V}\right], \tag{29g}$$

where

- (a) follows since conditioning reduces MMSE [13, Lemma 13];
- (b) follows by defining $V_i \triangleq \left(\mathbf{Y}^n_{\mathcal{A}\sim i}, f(X^n), \mathbf{Y}^{i-1}_{\mathcal{B}}, X^{i-1}\right)$, which is consistent with the definition of V_i in the proof of [9, Theorem 3];
- (c) holds with Q uniformly distributed over $[\![1:n]\!]$;
- (d) follows by defining $X \triangleq X_Q$, $\mathbf{Y}_{\mathcal{A}} \triangleq \mathbf{Y}_{\mathcal{A},Q}$, and $V \triangleq (V_Q, Q)$ which is consistent with the definitions of these random variables in the proof of [9, Th. 3].

Appendix D
Proof of Lemma 2

We prove the first statement of Lemma 2 as follows. By [28, Chapter 3], we have

$$\begin{aligned}\sigma^2_{X|Y} &= \sigma^2_X - \frac{\sigma^2_{XY}}{\sigma^2_Y}\\ &\overset{(a)}{=} \sigma^2_X - \frac{h^2\sigma^4_X}{h^2\sigma^2_X+\sigma^2_N}\\ &= \frac{\sigma^2_N}{h^2} - \sigma^4_N\left(h^4\sigma^2_X + h^2\sigma^2_N\right)^{-1}.\end{aligned} \tag{30}$$

where (a) follows by calculating $\sigma_{XY} = h\sigma^2_X$ and $\sigma^2_Y = h^2\sigma^2_X + \sigma^2_N$. Hence, by (30), the constraint $D \leq \sigma^2_{X|Y}$ can be expressed as

$$D \leq \frac{\sigma^2_N}{h^2} - \sigma^4_N\left(h^4\sigma^2_X + h^2\sigma^2_N\right)^{-1},$$

which can be rewritten as

$$0 < \sigma^4_N\left(h^4\sigma^2_X + h^2\sigma^2_N\right)^{-1} \leq \frac{\sigma^2_N}{h^2} - D. \tag{31}$$

Next, we prove the second statement of Lemma 2. Since (V, X, Y) are jointly Gaussian and V is independent of N, $\sigma^2_{X|V,Y}$ is given by [28, Chapter 3]

$$\sigma^2_{X|V,Y} = \sigma^2_X - \begin{bmatrix}\sigma_{XV} & h\sigma^2_X\end{bmatrix}\begin{bmatrix}\sigma^2_V & h\sigma_{XV}\\ h\sigma_{XV} & \sigma^2_Y\end{bmatrix}^{-1}\begin{bmatrix}\sigma_{XV} & h\sigma^2_X\end{bmatrix}^{\intercal},$$

where $\begin{bmatrix}\sigma^2_V & h\sigma_{XV}\\ h\sigma_{XV} & \sigma^2_Y\end{bmatrix}^{-1}$ is provided at the bottom of this page, in which (a) follows since

$$\begin{aligned}\sigma_V^{-2}\left(\sigma^2_V\sigma^2_Y - h^2\sigma^2_{XV}\right) &= \sigma^2_Y - h^2\sigma_V^{-2}\sigma^2_{XV}\\ &= h^2\sigma^2_X - h^2\sigma_V^{-2}\sigma^2_{XV} + \sigma^2_N\\ &= h^2\sigma^2_{X|V} + \sigma^2_N,\end{aligned}$$

where the last equality holds since $\sigma^2_{X|V} = \sigma^2_X - \sigma_V^{-2}\sigma^2_{XV}$. Hence,

$$\sigma^2_{X|V,Y} = \frac{\sigma^2_N\sigma^2_{X|V}}{h^2\sigma^2_{X|V}+\sigma^2_N}. \tag{32}$$

Then, by (32), the constraint $\sigma^2_{X|V,Y} \leq D$ can be expressed as follows:

$$\frac{\sigma^2_N\sigma^2_{X|V}}{h^2\sigma^2_{X|V}+\sigma^2_N} \leq D,$$

and, since $\frac{\sigma^2_N}{h^2} - D > 0$ by (31), we have

$$\sigma^2_{X|V} \leq \frac{\sigma^2_N D}{\sigma^2_N - h^2 D}.$$

The last statement of the lemma holds because if $D = \sigma^2_{X|V,Y}$, then

$$D = \frac{\sigma^2_N\sigma^2_{X|V}}{h^2\sigma^2_{X|V}+\sigma^2_N}, \tag{33}$$

where (33) follows from (32), and solving (33) for $\sigma^2_{X|V}$ results to $\sigma^2_{X|V} = \frac{\sigma^2_N D}{\sigma^2_N - h^2 D}$.

Appendix E
Proof of Lemma 3

Here, we show that for a given feasible V, we can construct a feasible Gaussian random variable $\bar{V}$ such that $C(V) = C(\bar{V})$. Thus, this implies that restricting V to be Gaussian does not change the optimum value of the optimization problem. Next, to study the difference of the two differential entropy in (18), we need the following properties of the Fisher information and the differential entropy.

Definition 3 [33, Definition 1]: Let X and U be random variables with well-defined densities, and $f_{X|U}$ be the corresponding conditional density. The conditional Fisher information of X is defined by

$$\mathbb{J}(X|U) = \mathbb{E}\left[\left(\frac{\partial \log f_{X|U}(x|u)}{\partial x}\right)^2\right],$$

$$\begin{aligned}\begin{bmatrix}\sigma^2_V & h\sigma_{XV}\\ h\sigma_{XV} & \sigma^2_Y\end{bmatrix}^{-1} &= \left(\sigma^2_V\sigma^2_Y - h^2\sigma^2_{XV}\right)^{-1}\begin{bmatrix}\sigma^2_Y & -h\sigma_{XV}\\ -h\sigma_{XV} & \sigma^2_V\end{bmatrix}\\ &\overset{(a)}{=} \begin{bmatrix}\sigma_V^{-2}\left(h^2\sigma^2_{X|V}+\sigma^2_N\right)^{-1}\left(h^2\sigma^2_X+\sigma^2_N\right) & -h\sigma_V^{-2}\sigma_{XV}\left(h^2\sigma^2_{X|V}+\sigma^2_N\right)^{-1}\\ -h\sigma_V^{-2}\sigma_{XV}\left(h^2\sigma^2_{X|V}+\sigma^2_N\right)^{-1} & \left(h^2\sigma^2_{X|V}+\sigma^2_N\right)^{-1}\end{bmatrix}\end{aligned}$$

where the expectation is over (U, X).

Lemma 5 [13, Lemma 18]: Let (V, X, G_1, G_2) be random variables such that (V, X) and (G_1, G_2) are independent, and let G_1 and G_2 be Gaussian random variables with variance $0 < \sigma_1^2 \le \sigma_2^2$. Then, we have

$$\mathbb{J}(X + G_2|V)^{-1} - \sigma_2^2 \ge \mathbb{J}(X + G_1|V)^{-1} - \sigma_1^2.$$

From [33, Lemma 3], we have

$$\mathbb{h}\left(\frac{1}{h_\mathcal{B}}\tilde{Y}_\mathcal{B}|V\right) - \mathbb{h}(X|V) = \frac{1}{2}\int_0^{\frac{\tilde{\sigma}_\mathcal{B}^2}{h_\mathcal{B}^2}} \mathbb{J}(X + N|V)d\sigma_N^2, \tag{34}$$

where N is a zero-mean Gaussian random variable with covariance $\sigma_N^2 \ge 0$. We now outer region (34) by substituting $G_1 \leftarrow \emptyset$ and $G_2 \leftarrow N$ in Lemma 5 as follows,

$$\mathbb{J}(X + N|V) \le \left(\mathbb{J}(X|V)^{-1} + \sigma_N^2\right)^{-1}. \tag{35}$$

Substituting (35) in (34), we have,

$$\mathbb{h}\left(\frac{1}{h_\mathcal{B}}\tilde{Y}_\mathcal{B}|V\right) - \mathbb{h}(X|V) \le \frac{1}{2}\log\frac{\mathbb{J}(X|V)^{-1} + \frac{\tilde{\sigma}_\mathcal{B}^2}{h_\mathcal{B}^2}}{\mathbb{J}(X|V)^{-1}}. \tag{36}$$

We can also lower bound the Fisher information in (34) by setting $G_2 \leftarrow \frac{1}{h_\mathcal{B}}\tilde{N}_\mathcal{B}$ and $G_1 \leftarrow N$ in Lemma 5 as follows,

$$\mathbb{J}\left(X + \frac{1}{h_\mathcal{B}}\tilde{N}_\mathcal{B}|V\right)^{-1} - \frac{\tilde{\sigma}_\mathcal{B}^2}{h_\mathcal{B}^2} \ge \mathbb{J}(X + N|V)^{-1} - \sigma_N^2,$$

for all $\sigma_N^2 \le \frac{\tilde{\sigma}_\mathcal{B}^2}{h_\mathcal{B}^2}$, which can be rewritten as

$$\mathbb{J}(X + N|V) \ge \left(\mathbb{J}(X + \frac{1}{h_\mathcal{B}}\tilde{N}_\mathcal{B}|V)^{-1} - \frac{\tilde{\sigma}_\mathcal{B}^2}{h_\mathcal{B}^2} + \sigma_N^2\right)^{-1}. \tag{37}$$

Substituting (37) in (34), we have,

$$\begin{aligned}&\mathbb{h}\left(\frac{1}{h_\mathcal{B}}\tilde{Y}_\mathcal{B}|V\right) - \mathbb{h}(X|V)\\ &\ge \frac{1}{2}\log\frac{\mathbb{J}\left(X + \frac{1}{h_\mathcal{B}}\tilde{N}_\mathcal{B}|V\right)^{-1}}{\mathbb{J}\left(X + \frac{1}{h_\mathcal{B}}\tilde{N}_\mathcal{B}|V\right)^{-1} - \frac{\tilde{\sigma}_\mathcal{B}^2}{h_\mathcal{B}^2}}.\end{aligned} \tag{38}$$

Next, define, for $0 \le t \le 1$,

$$\begin{aligned}g(t) &\triangleq t\mathbb{J}(X|V)^{-1}\\ &\quad + (1 - t)\left[\mathbb{J}\left(X + \frac{1}{h_\mathcal{B}}\tilde{N}_\mathcal{B}|V\right)^{-1} - \frac{\tilde{\sigma}_\mathcal{B}^2}{h_\mathcal{B}^2}\right],\end{aligned} \tag{39}$$

$$f(t) \triangleq \frac{1}{2}\log\frac{g(t) + \frac{\tilde{\sigma}_\mathcal{B}^2}{h_\mathcal{B}^2}}{g(t)}. \tag{40}$$

Hence, (36) and (38) can be expressed as,

$$f(0) \le \mathbb{h}\left(\frac{1}{h_\mathcal{B}}\tilde{Y}_\mathcal{B}|V\right) - \mathbb{h}(X|V) \le f(1).$$

Since f is continuous, from the intermediate value theorem, there exists a $t^\star \in [0, 1]$ such that,

$$\mathbb{h}\left(\frac{1}{h_\mathcal{B}}\tilde{Y}_\mathcal{B}|V\right) - \mathbb{h}(X|V) = f\left(t^\star\right) = \frac{1}{2}\log\frac{g(t^\star) + \frac{\tilde{\sigma}_\mathcal{B}^2}{h_\mathcal{B}^2}}{g(t^\star)}, \tag{41}$$

where $g(t^\star)$ is bounded as follows,

$$\mathbb{J}(X|V)^{-1} \overset{(a)}{\le} g\left(t^\star\right) \overset{(b)}{\le} \mathbb{J}\left(X + \frac{1}{h_\mathcal{B}}\tilde{N}_\mathcal{B}|V\right)^{-1} - \frac{\tilde{\sigma}_\mathcal{B}^2}{h_\mathcal{B}^2} \tag{42a}$$

$$\overset{(c)}{\le} \mathbb{J}\left(X + \frac{1}{h_\mathcal{A}}\tilde{N}_\mathcal{A}|V\right)^{-1} - \frac{\tilde{\sigma}_\mathcal{A}^2}{h_\mathcal{A}^2}, \tag{42b}$$

where

(*a*) and (*b*) follow by (39) and therefore by substituting $G_1 \leftarrow \emptyset$ and $G_2 \leftarrow \frac{1}{h_\mathcal{B}}\tilde{N}_\mathcal{B}$, in Lemma 5, we have,

$$\mathbb{J}\left(X + \frac{1}{h_\mathcal{B}}\tilde{N}_\mathcal{B}|V\right)^{-1} - \frac{\tilde{\sigma}_\mathcal{B}^2}{h_\mathcal{B}^2} \ge \mathbb{J}(X|V)^{-1}; \tag{42c}$$

(*c*) follows by Lemma 5 with $G_1 \leftarrow \frac{1}{h_\mathcal{B}}\tilde{N}_\mathcal{B}$ and $G_2 \leftarrow \frac{1}{h_\mathcal{A}}\tilde{N}_\mathcal{A}$.

Hence, (41) implies that if we choose $\bar{V}$ to be a Gaussian random variable which satisfies $\sigma_{X|\bar{V}}^2 = g(t^\star)$, then $C(\bar{V}) = C(V)$. Now, we show that the Gaussian random variable $\bar{V}$ is feasible, i.e., $\sigma_{X|\bar{V},\tilde{Y}_\mathcal{A}}^2 \le D$. The following lemma connects the conditional covariance with Fisher information.

Lemma 6: Let (V, X) be two arbitrary random variables with finite second moments, and N be a zero-mean Gaussian random variable with variance σ_N^2. Let, $Y = X + N$ and assume that V and X are independent of N. Then we have,

$$\mathbb{E}_{Y,V}\left[\sigma_{X|Y,V}^2\right] = \sigma_N^2 - \sigma_N^4\mathbb{J}(X + N|V).$$

A vector version of this lemma is stated in [13, Lemma 21] without proof. For completeness, we prove Lemma 6 in Appendix F. Using Lemma 6, we have,

$$\sigma_{X|\bar{V},\tilde{Y}_\mathcal{A}}^2 = \tilde{\sigma}_\mathcal{A}^2 - \tilde{\sigma}_\mathcal{A}^4\mathbb{J}\left(\tilde{Y}_\mathcal{A}|\bar{V}\right). \tag{43}$$

Then, we have,

$$\begin{aligned}\mathbb{J}\left(\frac{1}{h_\mathcal{A}}\tilde{Y}_\mathcal{A}|\bar{V}\right) &\overset{(a)}{=} \sigma^{-2}_{\frac{1}{h_\mathcal{A}}\tilde{Y}_\mathcal{A}|\bar{V}}\\ &\overset{(b)}{=} \left(\sigma_{X|\bar{V}}^2 + \frac{1}{h_\mathcal{A}^2}\tilde{\sigma}_\mathcal{A}^2\right)^{-1}\\ &\overset{(c)}{\ge} \left(\mathbb{J}(X + \frac{1}{h_\mathcal{A}}\tilde{N}_\mathcal{A}|V)^{-1} - \frac{\tilde{\sigma}_\mathcal{A}^2}{h_\mathcal{A}^2} + \frac{\tilde{\sigma}_\mathcal{A}^2}{h_\mathcal{A}^2}\right)^{-1}\\ &= \mathbb{J}\left(\frac{1}{h_\mathcal{A}}\tilde{Y}_\mathcal{A}|V\right),\end{aligned} \tag{44}$$

where

(*a*) follows from [33, Lemma 2], which states that for Gaussian random variables $\mathbb{J}(X|U) = \sigma_{X|U}^{-2}$;

(*b*) follows since $(\bar{V}, X)$ and $\tilde{N}_\mathcal{A}$ are independent;

(*c*) follows from (42b) since $\sigma_{X|\bar{V}}^2 = g(t^\star)$.

Next, using Lemma 7 below, (44) becomes

$$\mathbb{J}\left(\tilde{Y}_\mathcal{A}|\bar{V}\right) \ge \mathbb{J}\left(\tilde{Y}_\mathcal{A}|V\right), \tag{45}$$

Lemma 7: Let X and U be arbitrarily correlated random variables with well-defined densities. For any $a \in \mathbb{R}_{++}$,

$$\mathbb{J}(aX|U) = \frac{1}{a^2}\mathbb{J}(X|U).$$

The proof of Lemma 7 is available in Appendix G.

Therefore, combining (43) and (45) results to

$$\begin{aligned}\sigma^2_{X|\bar{V},\tilde{Y}_{\mathcal{A}}} &\le \tilde{\sigma}^2_{\mathcal{A}} - \tilde{\sigma}^4_{\mathcal{A}}\mathbb{J}\big(\tilde{Y}_{\mathcal{A}}|V\big)\\ &\overset{(a)}{=} \sigma^2_{X|V,\tilde{Y}_{\mathcal{A}}}\\ &\overset{(b)}{\le} D,\end{aligned}\tag{46}$$

where

(a) follows from Lemma 6;

(b) follows since we assumed that V is feasible, i.e., $\sigma^2_{X|V,\tilde{Y}_{\mathcal{A}}} \le D$.

Equation (46) means that the constructed Gaussian random variable $\bar{V}$ is feasible, which means that for each feasible V, there exists a feasible Gaussian $\bar{V}$ such that $C(V) = C(\bar{V})$.

Appendix F
Proof of Lemma 6

We have,

$$\begin{aligned}\frac{1}{2}\mathbb{J}(X+N|V=v) &\overset{(a)}{=} \frac{\partial}{\partial\sigma_N^2}\mathbb{h}(X+N|V=v)\\ &= \frac{\partial}{\partial\sigma_N^2}[I(X;X+N|V=v)+\mathbb{h}(X+N|X,V=v)]\\ &\overset{(b)}{=} \frac{\partial}{\partial\sigma_N^2}[I(X;X+N|V=v)+\mathbb{h}(N)]\\ &= \frac{\partial}{\partial\sigma_N^2}[I(X;X+N|V=v)]+\frac{1}{2\sigma_N^2}\\ &\overset{(c)}{=} \frac{\partial}{\partial\sigma_N^2}\Big[I\Big(X;\sigma_N^{-1}X+N'|V=v\Big)\Big]+\frac{1}{2\sigma_N^2}\\ &\overset{(d)}{=} -\sigma_N^{-4}\frac{\partial}{\partial u}\Big[I\Big(X;\sqrt{u}X+N'|V=v\Big)\Big]+\frac{1}{2\sigma_N^2}\\ &\overset{(e)}{=} -\frac{1}{2}\sigma_N^{-4}\mathbb{E}_{Y|V=v}\Big[\sigma^2_{X|Y,V=v}\Big]+\frac{1}{2}\sigma_N^{-2},\end{aligned}\tag{47}$$

where

(a) follows from [33, Lemma 3];

(b) follows since V and X are independent of N;

(c) holds with N' a standard Gaussian random variable;

(d) follows by defining $u \triangleq \sigma_N^{-2}$;

(e) follows from [34, Th. 1], with the input distribution $P_{X|V=v}$.

From (47), we have

$$\mathbb{E}_{Y|V=v}\Big[\sigma^2_{X|Y,V=v}\Big] = \sigma_N^2 - \sigma_N^4\mathbb{J}(X+N|V=v).\tag{48}$$

Now let $F_{V,Y}$ be the cumulative distribution function of (V, Y), therefore, from (48) we have

$$\begin{aligned}\mathbb{E}_{Y,V}\Big[\sigma^2_{X|Y,V}\Big] &= \int\limits_v\int\limits_y \sigma^2_{X|Y=y,V=v}dF_{V,Y}\\ &= \int\limits_v\Big(\sigma_N^2-\sigma_N^4 J(X+N|V=v)\Big)dF_V\\ &= \sigma_N^2-\sigma_N^4\int\limits_v J(X+N|V=v)dF_V\\ &= \sigma_N^2-\sigma_N^4 J(X+N|V).\end{aligned}$$

Appendix G
Proof of Lemma 7

Define $Y \triangleq aX$, then $f_{Y|U}(y|u) = \frac{1}{|a|}f_{X|U}\big(\frac{y}{a}|u\big)$, and from Definition 3 we have

$$\begin{aligned}\mathbb{J}(aX|U) &= \mathbb{J}(Y|U)\\ &= \mathbb{E}\left[\left(\frac{\partial\log f_{Y|U}(y|u)}{\partial y}\right)^2\right]\\ &= \mathbb{E}\left[\left(\frac{\partial}{\partial y}\log(\frac{1}{|a|}f_{X|U}(\frac{y}{a}|u))\right)^2\right]\\ &= \mathbb{E}\left[\left(\frac{\partial}{\partial y}\log(f_{X|U}(\frac{y}{a}|u))\right)^2\right]\\ &\overset{(a)}{=} \mathbb{E}\left[\frac{1}{a^2}\left(\frac{\partial}{\partial z}\log(f_{X|U}(z|u))\right)^2\right]\\ &= \frac{1}{a^2}\mathbb{J}(X|U),\end{aligned}$$

where (a) follows by defining $z \triangleq \frac{y}{a}$.

References

[1] H. ZivariFard and R. A. Chou, "Secure data storage resilient against compromised users via an access structure," in *Proc. IEEE Inf. Theory Workshop (ITW)*, 2022, pp. 404–469.

[2] G. R. Blakley, "Safeguarding cryptographic keys," in *Proc. AFIPS 79th Nat. Comput. Conf.*, New York, NY, USA, 1979, pp. 313–317.

[3] A. Shamir, "How to share a secret," *Commun. ACM*, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[4] T. Berger, *Rate Distortion Theory: A Mathematical Basis for Data Compression*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1971.

[5] A. Beimel, "Secret-sharing schemes: A survey," in *Proc. Int. Conf. Coding Cryptol.*, 2011, pp. 11–46.

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

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

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

[9] J. Villard and P. Piantanida, "Secure multiterminal source coding with side information at the eavesdropper," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 3668–3692, Jun. 2013.

[10] R. Tandon, S. Ulukus, and K. Ramchandran, "Secure source coding with a helper," *IEEE Trans. Inf. Theory*, vol. 59, no. 4, pp. 2178–2187, Apr. 2013.

[11] Y.-K. Chia and K. Kittichokechai, "On secure source coding with side information at the encoder," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Istanbul, Turkey, 2013, pp. 2204–2208.

[12] K. Kittichokechai, Y.-K. Chia, T. J. Oechtering, M. Skoglund, and T. Weissman, "Secure source coding with a public helper," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3930–3949, Jul. 2016.

[13] E. Ekrem and S. Ulukus, "Secure lossy transmission of vector Gaussian sources," *IEEE Trans. Inf. Theory*, vol. 59, no. 9, pp. 5466–5487, Sep. 2013.

[14] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. Hoboken, NJ, USA: Wiley, 2001.

[15] Y. Liang, G. Kramer, and H. V. Poor, "Compound wiretap channels," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, pp. 1–12, Oct. 2009.

[16] E. C. Song, P. Cuff, and H. V. Poor, "A rate-distortion based secrecy system with side information at the decoders," in *Proc. 52th Annu. Allerton Conf. Commun., Control, Comput.*, 2014, pp. 755–762.

[17] C. Schieler and P. Cuff, "Rate-distortion theory for secrecy systems," *IEEE Trans. Inf. Theory*, vol. 60, no. 12, pp. 7584–7605, Oct. 2014.

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

[19] 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.

[20] H. Yamamoto, “Coding theorems for Shannon’s cipher system with correlated source outputs, and common information,” *IEEE Trans. Inf. Theory*, vol. 40, no. 1, pp. 85–95, Jan. 1994.

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

[22] 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.

[23] N. Merhav, “Shannon’s secrecy system with informed receivers and its application to systematic coding for wiretapped channels,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2723–2734, Jun. 2006.

[24] P. Cuff and S. Satpathy, “Gaussian secure source coding and Wyner’s common information,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Hong Kong, China, 2015, pp. 116–120.

[25] R. Vidhi, R. A. Chou, and H. M. Kwon, “Information-theoretic secret sharing from correlated Gaussian random variables and public communication,” *IEEE Trans. Inf. Theory*, vol. 68, no. 1, pp. 549–559, Jan. 2022.

[26] A. El Gamal and Y.-H. Kim, *Network Information Theory*, 1st ed. Cambridge, U.K: Cambridge Univ., 2012.

[27] J. Benaloh and J. Leichter, “Generalized secret sharing and monotone functions,” in *Proc. Conf. Theory Appl. Cryptogr.*, New York, NY, USA, 1988, pp. 27–35.

[28] R. G. Gallager, *Stochastic Processes: Theory for Applications*. Cambridge, U.K: Cambridge Univ., 2013.

[29] P. Parada and R. Blahut, “Secrecy capacity of SIMO and slow fading channels,” in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Adelaide, SA, Australia, 2005, pp. 2152–2155.

[30] J. A. Thomas, “Feedback can at most double Gaussian multiple access channel capacity,” *IEEE Trans. Inf. Theory*, vol. IT-33, no. 5, pp. 711–716, Sep. 1987.

[31] 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, Jul. 2007.

[32] J. Wang and J. Chen, “Vector Gaussian two-terminal source coding,” *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 3693–3708, Jun. 2013.

[33] 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.

[34] D. Guo, S. Shamai, and S. Verdú, “Mutual information and minimum mean-square error in Gaussian channels,” *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1261–1282, Apr. 2005.