Information-Theoretic Secret Sharing From Correlated Gaussian Random Variables and Public Communication

Vidhi Rana, *Graduate Student Member, IEEE*, Rémi A. Chou, *Member, IEEE*, and Hyuck M. Kwon, *Life Senior Member, IEEE*

***Abstract*— In this paper, we study an information-theoretic secret sharing problem, where a dealer distributes shares of a secret among a set of participants under the following constraints: (i) authorized sets of users can recover the secret by pooling their shares, and (ii) non-authorized sets of colluding users cannot learn any information about the secret. We assume that the dealer and participants observe the realizations of correlated Gaussian random variables and that the dealer can communicate with participants through a one-way, authenticated, rate-limited, and public channel. Unlike traditional secret sharing protocols, in our setting, no perfectly secure channel is needed between the dealer and the participants. Our main result is a closed-form characterization of the fundamental trade-off between secret rate and public communication rate.**

***Index Terms*— Secret sharing, information-theoretic security, rate-limited communication, Gaussian sources.**

I. Introduction

SECRET sharing has been introduced in [2], [3]. In basic secret-sharing models, a dealer distributes a secret among a set of participants, with the constraint that only pre-defined sets of participants can recover this secret by pooling their shares, while any other set of colluding participants cannot learn any information about the secret.

In most secret-sharing models, including Shamir's scheme [2], it is assumed that the dealer and each participant can communicate over an information-theoretically secure channel at no cost. While complexity-based cryptography techniques, e.g., [4], could be used to implement secure channels without any other resources than a public channel, it would not provide information-theoretically secure channels. In this paper, we are interested in *another approach that aims at providing a full information-theoretic solution that would not rely on complexity-based cryptography*. In other words, we want to avoid the assumption that information-theoretically secure communication channels are available at no cost. An information-theoretic approach to secret sharing over wireless channels has been introduced in [5] for this purpose. The main idea is to leverage channel noise by remarking that information-theoretic secret sharing over wireless channels is similar to compound wiretap channel models [6]. This information-theoretic approach has also been formulated for source models in [7]–[9], where participants and dealers share correlated random variables. These models are related to compound secret-key generation, e.g., [10], [11], and biometric systems with a multiuser access structure [12], in that multiple reliability and security constraints need to be satisfied simultaneously.

In this paper, we consider the information-theoretic secret sharing model in [8] with Gaussian sources. Specifically, the dealer and the participants observe realizations of correlated Gaussian random variables, and the dealer can communicate with the participants over an authenticated, one-way, rate-limited, and public communication channel. In wireless networks, independently and identically distributed realizations of correlated random variables can, for instance, be obtained from channel gain measurements after appropriate manipulations [13], [14]. Our approach for the achievability part consists in handling the reliability and security requirements separately. Specifically, reliability is obtained via a coding scheme akin to a compound version of Wyner-Ziv coding [15], and security relies on universal hashing via extractors [16]. Interestingly, the converse shows that there is no loss of optimality in decoupling the reliability and security requirements. The achievability is first obtained for discrete random variables and then extended to continuous random variables via fine quantization. In principle, one cannot assume a specific quantization strategy to ensure the security requirement in an information-theoretic manner; hence, the key step in this extension is to show that information-theoretic security holds, provided that the quantization is sufficiently fine. For the converse part, we can partly rely on techniques developed in [17], [18]. However, unlike in [17], [18], our setting involves multiple security constraints that need to be satisfied simultaneously; hence, the main task in the converse is to prove a saddle point property without any degradation assumption on the source model.

The main differences between our work and [8], [10]–[12] are that [8], [10]–[12] consider discrete memoryless sources, whereas we consider Gaussian sources. As described above, handling Gaussian random variables calls for different proof techniques and considerations. Additionally, unlike

Manuscript received October 14, 2020; revised October 4, 2021; accepted October 7, 2021. Date of publication October 27, 2021; date of current version December 23, 2021. The work of Vidhi Rana and Rémi A. Chou was supported by NSF under Grant CCF-1850227 and Grant CCF-2047913. An earlier version of this paper was presented at the 2020 IEEE Information Theory Workshop [1] [DOI: 10.1109/ITW46852.2021.9457636]. *(Corresponding author: Vidhi Rana.)*

The authors are with the Department of Electrical Engineering and Computer Science, Wichita State University, Wichita, KS 67260 USA (e-mail: vxrana@shockers.wichita.edu; remi.chou@wichita.edu; hyuck.kwon@wichita.edu).

Communicated by A. Beimel, Associate Editor for Cryptography.

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TIT.2021.3122808.

Digital Object Identifier 10.1109/TIT.2021.3122808

[8], [10]–[12], it also allows us to derive capacity results without assuming any source degradation properties. We also highlight that unlike [8], [11], we consider rate-limited public communication, and unlike [8], [12], we handle arbitrary access structures.

The main features of our work can be summarized as follows: (i) Our model relies on correlated Gaussian random variables and, similar to [8] but unlike traditional secret-sharing schemes [2], does not rely on the assumption that information-theoretically secure channels between the dealer and the participants are available. (ii) Similar to the model in [8] but unlike traditional secret-sharing models, we consider a model that requires information-theoretic security for the secret with respect to unauthorized sets of participants during the distribution phase, i.e., when the dealer distributes shares of the secret to participants. (iii) We establish a closed-form expression that characterizes the optimal trade-off between secret rate and public communication rate. (iv) The size of the shares in our coding scheme scales linearly with the size of the secret for any access structure similar to the model in [8]. Indeed, a share comprises the public communication from the dealer and n quantized realizations of a Gaussian random variable, which can be shown to both linearly scale with n. The size of the shares does depend on the specific access structure considered but not on the number of participants. Specifically, the public communication must ensure that the set of authorized users with the least amount of information about the secret is able to reconstruct the secret. By contrast, the best-known traditional secret-sharing schemes may require a share size that grows exponentially with the number of the participants for some access structures [19] – note, however, that it is unknown whether or not there exist traditional secret-sharing schemes that require a smaller share size. (v) For threshold access structures, i.e., when a fixed number of participants t is needed to reconstruct the secret (independently from the specific identities of those participants), we establish that the size of the secret that can be exchanged is, in general, *not* a monotonic function of the threshold t.

The remainder of the paper is organized as follows. We set the notation in Section II and formally introduce the problem statement in Section III. We present our main results in Section IV, and proofs in Sections V and VI. Finally, we provide concluding remarks in Section VII.

II. Notation

For any $a, b \in \mathbb{R}$, define $[\![a, b]\!] \triangleq [\lfloor a \rfloor, \lceil b \rceil] \cap \mathbb{N}$. For $x \in \mathbb{R}$, define $[x]^+ \triangleq \max(0, x)$. For a set $\mathcal{S}$, let $2^{\mathcal{S}}$ denote the power set of $\mathcal{S}$. All logarithms are taken in base 2 throughout the paper. Let I_m denote the identity matrix of dimension $m \in \mathbb{N}$. Let $\det(W)$ denote the determinant of a matrix W and $|\mathcal{S}|$ denote the cardinality of a set $\mathcal{S}$. For two random variables X and V, σ_X^2 and σ_{XV} denote $\mathbb{E}[(X - \mathbb{E}[X])^2]$ and $\mathbb{E}[(X - \mathbb{E}[X])(V - \mathbb{E}[V])]$, respectively. $N \sim \mathcal{N}(0, \Sigma)$ indicates that N is a zero-mean Gaussian random vector with covariance matrix Σ. The indicator function is denoted by $\mathbb{1}\{\omega\}$, which is equal to 1 if the predicate ω is true and 0 otherwise. Let $H(X)$ (respectively, $h(X)$) denote the Shannon entropy (respectively, the differential entropy) of a discrete (respectively continuous), random variable X. Also, let $I(X;Y)$ denote the mutual information between X and Y, which are either continuous or discrete random variables.

III. Problem Statement

Consider a dealer and L participants. Define $\mathcal{L} \triangleq [\![1, L]\!]$, $\mathcal{X} \triangleq \mathbb{R}$, and $\mathcal{Y} \triangleq \mathbb{R}$. Consider a Gaussian memoryless source model $(\mathcal{X} \times \mathcal{Y}_{\mathcal{L}}, p_{XY_{\mathcal{L}}})$, where $Y_{\mathcal{L}} \triangleq (Y_l)_{l \in \mathcal{L}}$, and $(X, Y_{\mathcal{L}})$ are jointly Gaussian random variables with a non-singular covariance matrix. Let $\mathbb{A}$ be a set of subsets of $\mathcal{L}$ such that for any $\mathcal{T} \subseteq \mathcal{L}$, if $\mathcal{T}$ contains a set that belongs to $\mathbb{A}$, then $\mathcal{T}$ also belongs to $\mathbb{A}$, i.e., $\mathbb{A}$ is a monotone access structure [20]. We also define $\mathbb{U} \triangleq 2^{\mathcal{L}} \backslash \mathbb{A}$ as the set of all colluding subsets of users who must not learn any information about the secret. In the following, for any $\mathcal{A} \in \mathbb{A}$ and for any $\mathcal{U} \in \mathbb{U}$, we use the notation $Y_{\mathcal{A}}^n \triangleq (Y_l^n)_{l \in \mathcal{A}}$ and $Y_{\mathcal{U}}^n \triangleq (Y_l^n)_{l \in \mathcal{U}}$. Moreover, we assume that the dealer can communicate with the participants over an authenticated, one-way, rate-limited, noiseless, and public communication channel.

Definition 1: A $(2^{nR_s}, R_p, \mathbb{A}, n)$ secret-sharing strategy is defined as follows:

- The dealer observes X^n and Participant $l \in \mathcal{L}$ observes Y_l^n.
- The dealer sends over the public channel the message M to the participants with the bandwidth constraint $H(M) \leq nR_p$.
- The dealer computes a secret $S \in \mathcal{S} \triangleq [\![1, 2^{nR_s}]\!]$ from X^n.
- Any subset of participants $\mathcal{A} \in \mathbb{A}$ can compute an estimate $\widehat{S}(\mathcal{A})$ of S from their observations $(Y_l^n)_{l \in \mathcal{A}}$ and M.

Definition 2: A rate pair (R_p, R_s) is achievable if there exists a sequence of $(2^{nR_s}, R_p, \mathbb{A}, n)$ secret-sharing strategies such that

$$\lim_{n \to \infty} \max_{\mathcal{A} \in \mathbb{A}} \mathbb{P}[\widehat{S}(\mathcal{A}) \neq S] = 0, \tag{1}$$

$$\lim_{n \to \infty} \max_{\mathcal{U} \in \mathbb{U}} I(S; M, Y_{\mathcal{U}}^n) = 0, \tag{2}$$

$$\lim_{n \to \infty} \log |\mathcal{S}| - H(S) = 0. \tag{3}$$

(1) means that any subset of participants in $\mathbb{A}$ is able to recover the secret, (2) means that any subset of participants in $\mathbb{U}$ cannot obtain information about the secret, while (3) means that the secret is nearly uniform and that its entropy is nearly equal to its length.

Remark 1: The uniformity condition (3) ensures that a secret-sharing strategy that maximizes the length of the secret, will also maximize the entropy of the secret. Without this condition, maximizing the length of the secret would not be meaningful as one could always increase the length of the secret by adding redundancy to it. This is the same reason why in secret-key generation, one requires uniformity of the secret key [21], [22].

The secret capacity region is defined as

$$\mathcal{R}(p_{XY_{\mathcal{L}}}, \mathbb{A}) \triangleq \{(R_p, R_s) : (R_p, R_s) \text{ is achievable}\}.$$

Moreover, for a fixed R_p, the supremum of secret rates R_s such that $(R_p, R_s) \in \mathcal{R}(p_{XY_{\mathcal{L}}}, \mathbb{A})$ is called the secret capacity and is denoted by $C_s(\mathbb{A}, R_p)$.

Additionally, one can write for any $\mathcal{A} \in \mathbb{A}$ and for any $\mathcal{U} \in \mathbb{U}$ (see Appendix A for the derivation)

$$Y_{\mathcal{A}} = H_{\mathcal{A}} X + W_{Y_{\mathcal{A}}}, \tag{4}$$

$$Y_{\mathcal{U}} = H_{\mathcal{U}} X + W_{Y_{\mathcal{U}}}, \tag{5}$$

where $H_{\mathcal{A}} \in \mathbb{R}^{|\mathcal{A}|\times 1}$, $H_{\mathcal{U}} \in \mathbb{R}^{|\mathcal{U}|\times 1}$, $W_{Y_{\mathcal{A}}} \sim \mathcal{N}(0, I_{|\mathcal{A}|})$, and $W_{Y_{\mathcal{U}}} \sim \mathcal{N}(0, I_{|\mathcal{U}|})$.

IV. Main Results

A. Results for General Access Structures

For a given access structure $\mathbb{A}$, define

$$\mathcal{A}^\star \in \arg\min_{\mathcal{A}\in\mathbb{A}} H_{\mathcal{A}}^T H_{\mathcal{A}}, \quad \mathcal{U}^\star \in \arg\max_{\mathcal{U}\in\mathbb{U}} H_{\mathcal{U}}^T H_{\mathcal{U}}.$$

Theorem 1: For any access structure $\mathbb{A}$ and public communication rate $R_p \geq 0$, the secret capacity $C_s(\mathbb{A}, R_p)$ is

$$C_s(\mathbb{A}, R_p) = \left[\frac{1}{2}\log\frac{\sigma_X^2 H_{\mathcal{U}^\star}^T H_{\mathcal{U}^\star} 2^{-2R_p} + \sigma_X^2 H_{\mathcal{A}^\star}^T H_{\mathcal{A}^\star}(1-2^{-2R_p})+1}{\sigma_X^2 H_{\mathcal{U}^\star}^T H_{\mathcal{U}^\star}+1}\right]^+.$$

Proof: The converse and achievability are proved in Sections V and VI, respectively. □

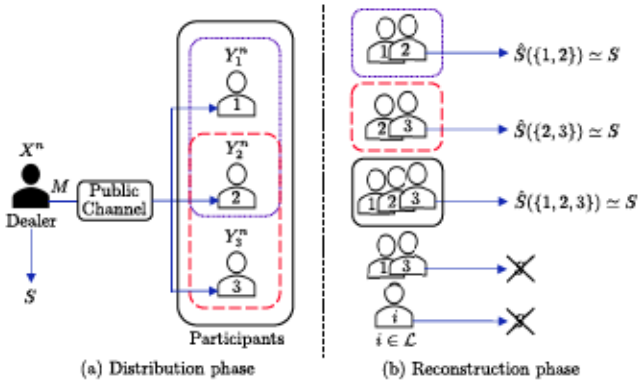
From Theorem 1, we obtain the following corollary when the public communication is rate-unlimited.

Corollary 1: For any access structure $\mathbb{A}$, and an unlimited public communication rate, the secret capacity is given by

$$C_s(\mathbb{A}, R_p = +\infty) \triangleq \lim_{R_p\to+\infty} C_s(\mathbb{A}, R_p) = \left[\frac{1}{2}\log\frac{\sigma_X^2 H_{\mathcal{A}^\star}^T H_{\mathcal{A}^\star}+1}{\sigma_X^2 H_{\mathcal{U}^\star}^T H_{\mathcal{U}^\star}+1}\right]^+.$$

Note that in Theorem 1 and Corollary 1, the length of the public communication scales linearly with the length of the secret by construction and corresponds to a compressed version of the n source observations of the dealer via a compound version of Wyner-Ziv coding. Hence, the size of the share of each participant, which comprises the public communication and n quantized observations of a Gaussian random variable, scales linearly with the length of the secret – as explained in the proof of Theorem 1, the number of bits needed to store quantized realizations of Gaussian random variables is negligible compared to the number of source observations n in our achievability scheme. Note that, unlike traditional secret-sharing models, which separately consider the share-creation phase and the share-distribution phase, we allow a joint design of these two phases in our setting. This is made possible by considering correlated random variables (at the participants and the dealer) and public communication instead of information-theoretically secure channels as in traditional secret-sharing models. The following example illustrates Theorem 1 and Corollary 1.

Example 1: Consider a dealer and three participants who observe independently and identically distributed realizations of correlated Gaussian random variables as depicted in Figure 1. Define the access structure $\mathbb{A} \triangleq \{\{1,2\},\{2,3\},\{1,2,3\}\}$ and define $\mathbb{U} \triangleq \{\{1,3\},\{1\},\{2\},\{3\}\}$ such that (i) the sets of participants in $\mathbb{A}$ can recover the secret using their observations and the public message M, and (ii) the sets of participants in $\mathbb{U}$ cannot learn information about the secret. For $s \in [\![1, L]\!]$, let $H_{\mathcal{L}}(s)$ denote the s-th component of $H_{\mathcal{L}}$, and assume that $\sigma_X^2 \triangleq 2$, $H_{\mathcal{L}} \triangleq [0.5, 1, 0.8]^T$, and for any $\mathcal{S} \subseteq \mathcal{L}$, $H_{\mathcal{S}} = (H_{\mathcal{L}}(s))_{s\in\mathcal{S}}$. Then, one can compute the secret capacity using Theorem 1 and Corollary 1, as shown in Figure 2.



(a) Distribution phase (b) Reconstruction phase

Fig. 1. Secret-sharing setting when $\mathbb{A} = \{\{1,2\},\{2,3\},\{1,2,3\}\}$ and $\mathbb{U} = \{\{1,3\},\{1\},\{2\},\{3\}\}$. Dashed, dotted, and solid contour lines represent the subsets of participants that are authorized to reconstruct the secret.

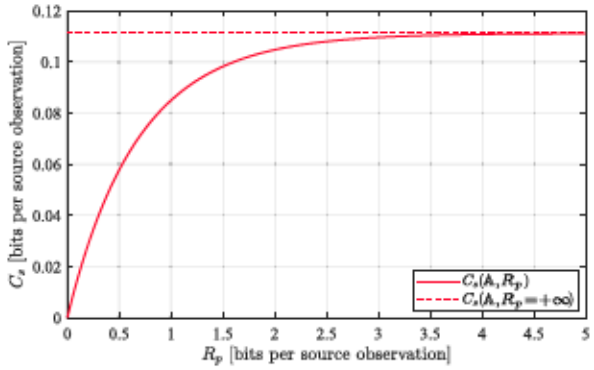


Fig. 2. Secret capacity for example 1.

B. Results for Threshold Access Structures

We now consider a special kind of access structure called threshold access structure [2]. A threshold access structure with threshold $t \in [\![1, L]\!]$ is defined as

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

The complement of $\mathbb{A}_t$ is defined as $\mathbb{U}_t \triangleq 2^{\mathcal{L}} \backslash \mathbb{A}_t = \{\mathcal{A} \subseteq \mathcal{L} : |\mathcal{A}| < t\}$. In other words, the threshold access structure is defined such that any set of t participants can reconstruct the secret, but no set of fewer than t participants can learn information about the secret.

The following result provides necessary and sufficient conditions to determine whether the secret capacity increases or decreases as the threshold t increases.

Theorem 2: Assume that for any $\mathcal{S} \subseteq \mathcal{L}$, $H_{\mathcal{S}} = (H_{\mathcal{L}}(s))_{s\in\mathcal{S}}$. For any $t \in [\![1, L]\!]$, consider $\mathcal{A}_t^\star \in \arg\min_{\mathcal{A}\in\mathbb{A}_t} H_{\mathcal{A}}^T H_{\mathcal{A}}$, and $\mathcal{U}_t^\star \in \arg\max_{\mathcal{U}\in\mathbb{U}_t} H_{\mathcal{U}}^T H_{\mathcal{U}}$. For any communication rate $R_p \geq 0$, for any $t \in [\![1, L]\!]$, we have

$$C_s(\mathbb{A}_1, R_p) \geq C_s(\mathbb{A}_t, R_p),$$

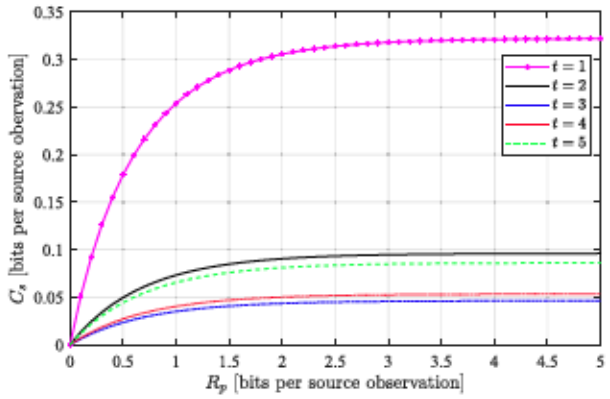


Fig. 3. Secret capacity for threshold access structure.

and for any $t \in [\![1, L]\!]$ and $i \in [\![1, L-t]\!]$,

$$C_s(\mathbb{A}_t, R_p) \geq C_s(\mathbb{A}_{t+i}, R_p) \iff \frac{H_{\mathcal{U}_{t+i}^\star}^T H_{\mathcal{U}_{t+i}^\star} - H_{\mathcal{U}_t^\star}^T H_{\mathcal{U}_t^\star}}{H_{\mathcal{A}_{t+i}^\star}^T H_{\mathcal{A}_{t+i}^\star} - H_{\mathcal{A}_t^\star}^T H_{\mathcal{A}_t^\star}} \geq \frac{1+\sigma_X^2 H_{\mathcal{U}_t^\star}^T H_{\mathcal{U}_t^\star}}{1+\sigma_X^2 H_{\mathcal{A}_t^\star}^T H_{\mathcal{A}_t^\star}}.$$

Proof: See Appendix B. □

Theorem 2 illustrates the fact that the secret capacity is not necessarily a monotonic decreasing function of the threshold t.

Example 2: Consider a dealer and five participants. Assume that $\sigma_X^2 \triangleq 2$, $H_{\mathcal{L}} \triangleq [1, 0.85, 0.9, 0.95, 0.75]^T$, and for any $\mathcal{S} \subseteq \mathcal{L}$, $H_{\mathcal{S}} = (H_{\mathcal{L}}(s))_{s\in\mathcal{S}}$. Then, one can compare the secret capacities for different thresholds using Theorem 2, as shown in Figure 3.

From the definition of $\mathcal{A}_t^\star$ and $\mathcal{U}_t^\star$, we have $H_{\mathcal{A}_1^\star} = [0.75]^T$, $H_{\mathcal{A}_2^\star} = [0.75, 0.85]^T$, $H_{\mathcal{A}_3^\star} = [0.75, 0.85, 0.9]^T$, $H_{\mathcal{A}_4^\star} = [0.75, 0.85, 0.9, 0.95]^T$, $H_{\mathcal{A}_5^\star} = [0.75, 0.85, 0.9, 0.95, 1]^T$, $H_{\mathcal{U}_2^\star} = [1]^T$, $H_{\mathcal{U}_3^\star} = [1, 0.95]^T$, $H_{\mathcal{U}_4^\star} = [1, 0.95, 0.9]^T$, and $H_{\mathcal{U}_5^\star} = [1, 0.95, 0.9, 0.85]^T$.

For example, putting $H_{\mathcal{A}_4^\star}^T H_{\mathcal{A}_4^\star} = 2.9975$, $H_{\mathcal{U}_4^\star}^T H_{\mathcal{U}_4^\star} = 2.7125$, $H_{\mathcal{A}_5^\star}^T H_{\mathcal{A}_5^\star} = 3.9975$, and $H_{\mathcal{U}_5^\star}^T H_{\mathcal{U}_5^\star} = 3.4350$ in Theorem 2 with $t = 4$ and $i = 1$, we get $C_s(\mathbb{A}_4, R_p) \leq C_s(\mathbb{A}_5, R_p)$ for any $R_p \geq 0$.

V. Converse Proof of Theorem 1

To prove the converse, we first derive an upper bound on the secret capacity $C_s(\mathbb{A}, R_p)$ by considering a worst-case scenario in terms of a secret-key generation problem. This upper bound takes the form of a minimax optimization problem. We then derive a closed-form expression of this upper bound by proving a minimax theorem.

Define for $\mathcal{A} \in \mathbb{A}$, $\mathcal{U} \in \mathbb{U}$, $O_{\mathcal{A}} \triangleq H_{\mathcal{A}}^T H_{\mathcal{A}}$, and $O_{\mathcal{U}} \triangleq H_{\mathcal{U}}^T H_{\mathcal{U}}$. Consider V an auxiliary random variable jointly Gaussian with X, and let $\sigma_{X|V}^2$ be the conditional variance of X given V. Consider also $\mathcal{A}^\star \in \arg\min_{\mathcal{A}\in\mathbb{A}} O_{\mathcal{A}}$ and $\mathcal{U}^\star \in \arg\max_{\mathcal{U}\in\mathbb{U}} O_{\mathcal{U}}$. Provided that $\sigma_{X|V}^2 \neq 0$, for $\mathcal{A} \in \mathbb{A}$, $\mathcal{U} \in \mathbb{U}$, define

$$I_p(\sigma_{X|V}^2, \mathcal{A}) \triangleq \frac{1}{2}\log\frac{\sigma_X^2}{\sigma_{X|V}^2} - \frac{1}{2}\log\frac{\sigma_X^2 O_{\mathcal{A}} + 1}{\sigma_{X|V}^2 O_{\mathcal{A}} + 1},$$
$$I_s(\sigma_{X|V}^2, \mathcal{A}, \mathcal{U}) \triangleq \frac{1}{2}\log\frac{\sigma_X^2 O_{\mathcal{A}} + 1}{\sigma_{X|V}^2 O_{\mathcal{A}} + 1} - \frac{1}{2}\log\frac{\sigma_X^2 O_{\mathcal{U}} + 1}{\sigma_{X|V}^2 O_{\mathcal{U}} + 1}.$$

We will also use the following lemmas.

Lemma 1 (Weinstein–Aronszajn Identity, e.g., [23, Appendix B]): For any $\sigma^2 \in \mathbb{R}^+$ and $A \in \mathbb{R}^{q\times 1}$, we have

$$\det(A\sigma^2 A^T + I_q) = A^T A \sigma^2 + 1.$$

Lemma 2: Let $c, d \in \mathbb{R}_+$ such that $c \geq d$. Then, the function $f_{c,d}$ is non-decreasing, where

$$f_{c,d} : \mathbb{R}_+ \to \mathbb{R}, \quad x \mapsto \frac{1}{2}\log\frac{cx+1}{dx+1}.$$

Proof: The derivative of $f_{c,d}$ at $x \in \mathbb{R}_+$ is $f'_{c,d}(x) = \frac{1}{2\ln 2}\frac{c-d}{(cx+1)(dx+1)} \geq 0$. □

We now prove the converse of Theorem 1 through a series of lemmas.

Lemma 3: Let $R_p \in \mathbb{R}_+$. An upper bound on the secret capacity $C_s(\mathbb{A}, R_p)$ for the Gaussian source model $(\mathcal{X} \times \mathcal{Y}_{\mathcal{L}}, p_{XY_{\mathcal{L}}})$ is given by

$$C_s(\mathbb{A}, R_p) \leq \min_{\mathcal{A}\in\mathbb{A}} \min_{\mathcal{U}\in\mathbb{U}} \max_{\substack{0<\sigma_{X|V}^2\leq\sigma_X^2 \\ \text{s.t. } I_p(\sigma_{X|V}^2,\mathcal{A})\leq R_p}} I_s(\sigma_{X|V}^2, \mathcal{A}, \mathcal{U}). \tag{6}$$

Proof: Fix $\mathcal{A} \in \mathbb{A}$, $\mathcal{U} \in \mathbb{U}$. We first consider the secret-key generation model in [17] consisting of a transmitter (Alice), a receiver (Bob), and an eavesdropper (Eve), who observe X^n, Y^n, and Z^n, respectively, independently and identically distributed according to a Gaussian source $((\mathcal{X} \times \mathcal{Y} \times \mathcal{Z}), p_{XYZ})$, where $\mathcal{X} \triangleq \mathbb{R}$, $\mathcal{Y} \triangleq \mathbb{R}^{|\mathcal{A}|}$, $\mathcal{Z} \triangleq \mathbb{R}^{|\mathcal{U}|}$. In this model, a secret-key rate R_k is achievable if after the transmission from Alice to Bob of message M such that $H(M) \leq nR_p$ over an authenticated noiseless public channel, a secret key $K \in [\![1, 2^{nR_k}]\!]$ is generated by Alice, and an estimate $\widehat{K}$ of K is generated by Bob such that (i) $\lim_{n\to\infty} \mathbb{P}[K \neq \widehat{K}] = 0$ (reliability), (ii) $\lim_{n\to\infty} I(K; Z^n M) = 0$ (security), and $\lim_{n\to\infty} \log\lceil 2^{nR_k}\rceil - H(K) = 0$ (uniformity). Moreover, the capacity region of this model is defined as $\mathcal{R}(p_{XYZ}, \mathcal{A}, \mathcal{U}) \triangleq \{(R_p, R_k) : (R_p, R_k) \text{ is achievable}\}$.

Consider now the secret-sharing problem described in Section III and the rate pair $(R_p, R_s) \in \mathcal{R}(p_{XY_{\mathcal{L}}}, \mathbb{A})$. Then, by conditions (1), (2), and (3), the rate pair (R_p, R_s) also belongs to $\mathcal{R}(p_{XY_{\mathcal{A}}Y_{\mathcal{U}}}, \mathcal{A}, \mathcal{U})$ for any $\mathcal{A} \in \mathbb{A}$, $\mathcal{U} \in \mathbb{U}$. Therefore, by [17, Theorem 2], we have for any $\mathcal{A} \in \mathbb{A}$, $\mathcal{U} \in \mathbb{U}$,

$$R_s \leq \frac{1}{2}\log\left[\frac{\det(H_{\mathcal{A}}\sigma_X^2 H_{\mathcal{A}}^T + I)}{\det(H_{\mathcal{A}}\sigma_{X|V}^2 H_{\mathcal{A}}^T + I)}\frac{\det(H_{\mathcal{U}}\sigma_{X|V}^2 H_{\mathcal{U}}^T + I)}{\det(H_{\mathcal{U}}\sigma_X^2 H_{\mathcal{U}}^T + I)}\right],$$
$$R_p \geq \frac{1}{2}\log\frac{\sigma_X^2}{\sigma_{X|V}^2} - \frac{1}{2}\log\frac{\det(H_{\mathcal{A}}\sigma_X^2 H_{\mathcal{A}}^T + I)}{\det(H_{\mathcal{A}}\sigma_{X|V}^2 H_{\mathcal{A}}^T + I)},$$

for some $\sigma_{X|V}^2 \in (0, \sigma_X^2]$. Finally, using Lemma 1 and the definition of $O_{\mathcal{A}}$, $\mathcal{A} \in \mathbb{A}$ and $O_{\mathcal{U}}$, $\mathcal{U} \in \mathbb{U}$, we have (6). □

Lemma 4: Let $R_p \in \mathbb{R}_+$. Let $\mathcal{A} \in \mathbb{A}$, $\mathcal{U} \in \mathbb{U}$, and assume that $O_{\mathcal{A}} \geq O_{\mathcal{U}}$. Then, we have

$$\max_{\substack{0<\sigma_{X|V}^2\leq\sigma_X^2 \\ \text{s.t. } I_p(\sigma_{X|V}^2,\mathcal{A})\leq R_p}} I_s(\sigma_{X|V}^2, \mathcal{A}, \mathcal{U}) = \frac{1}{2}\log\frac{\sigma_X^2 O_{\mathcal{U}} 2^{-2R_p} + \sigma_X^2 O_{\mathcal{A}}(1-2^{-2R_p}) + 1}{\sigma_X^2 O_{\mathcal{U}} + 1}. \tag{7}$$

Proof: Fix $\mathcal{A} \in \mathbb{A}$ and $\mathcal{U} \in \mathbb{U}$. Let $\sigma^{2\star}_{X|V}(\mathcal{A},\mathcal{U})$ be an optimal solution on the left-hand side of (7). By writing $I_s(\sigma^2_{X|V},\mathcal{A},\mathcal{U})$ as

$$I_s(\sigma^2_{X|V},\mathcal{A},\mathcal{U}) = \frac{1}{2}\log\frac{\sigma^2_X O_{\mathcal{A}}+1}{\sigma^2_X O_{\mathcal{U}}+1} - \frac{1}{2}\log\frac{\sigma^2_{X|V} O_{\mathcal{A}}+1}{\sigma^2_{X|V} O_{\mathcal{U}}+1},$$

we have that $I_s(\sigma^2_{X|V},\mathcal{A},\mathcal{U})$ is a non-increasing function of $\sigma^2_{X|V}$ by Lemma 2 because $O_{\mathcal{A}} \geq O_{\mathcal{U}}$. Hence, $\sigma^{2\star}_{X|V}(\mathcal{A},\mathcal{U})$ must be the smallest $\sigma^2_{X|V} \in (0,\sigma^2_X]$ that satisfies the constraint $I_p(\sigma^2_{X|V},\mathcal{A}) \leq R_p$. However, $I_p(\sigma^2_{X|V},\mathcal{A})$ is a non-increasing function of $\sigma^2_{X|V}$; thus, we must have $I_p(\sigma^{2\star}_{X|V}(\mathcal{A},\mathcal{U}),\mathcal{A}) = R_p$, i.e.,

$$R_p = \frac{1}{2}\log\frac{\sigma^2_X}{\sigma^{2\star}_{X|V}(\mathcal{A},\mathcal{U})} - \frac{1}{2}\log\frac{\sigma^2_X O_{\mathcal{A}}+1}{\sigma^{2\star}_{X|V}(\mathcal{A},\mathcal{U})O_{\mathcal{A}}+1},$$

which gives

$$\sigma^{2\star}_{X|V}(\mathcal{A},\mathcal{U}) = \frac{\sigma^2_X}{\sigma^2_X O_{\mathcal{A}}(2^{2R_p}-1)+2^{2R_p}}. \tag{8}$$

Plugging in this value for $\sigma^{2\star}_{X|V}(\mathcal{A},\mathcal{U})$ in $I_s(\sigma^{2\star}_{X|V}(\mathcal{A},\mathcal{U}),\mathcal{A},\mathcal{U})$ gives (7). □

Lemma 5: Assume that for any $\mathcal{A} \in \mathbb{A}$, $\mathcal{U} \in \mathbb{U}$, we have $O_{\mathcal{A}} \geq O_{\mathcal{U}}$. Let $R_p \in \mathbb{R}_+$. Then, we have

$$\begin{aligned}&\min_{\mathcal{A}\in\mathbb{A}}\min_{\mathcal{U}\in\mathbb{U}} \max_{\substack{0<\sigma^2_{X|V}\leq\sigma^2_X \\ \text{s.t. } I_p(\sigma^2_{X|V},\mathcal{A})\leq R_p}} I_s(\sigma^2_{X|V},\mathcal{A},\mathcal{U}) \\ &= \max_{\substack{0<\sigma^2_{X|V}\leq\sigma^2_X \\ \text{s.t. } I_p(\sigma^2_{X|V},\mathcal{A}^\star)\leq R_p}} \min_{\mathcal{A}\in\mathbb{A}}\min_{\mathcal{U}\in\mathbb{U}} I_s(\sigma^2_{X|V},\mathcal{A},\mathcal{U}). \end{aligned} \tag{9}$$

Proof: By Lemma 2, we have for any $\sigma^2_{X|V} \in (0,\sigma^2_X]$, $\mathcal{A} \in \mathbb{A}$, $\mathcal{U} \in \mathbb{U}$,

$$\begin{aligned}&\frac{1}{2}\log\frac{\sigma^2_X O_{\mathcal{A}}+1}{\sigma^2_{X|V} O_{\mathcal{A}}+1} \geq \frac{1}{2}\log\frac{\sigma^2_X O_{\mathcal{A}^\star}+1}{\sigma^2_{X|V} O_{\mathcal{A}^\star}+1}, \\ &-\frac{1}{2}\log\frac{\sigma^2_X O_{\mathcal{U}}+1}{\sigma^2_{X|V} O_{\mathcal{U}}+1} \geq -\frac{1}{2}\log\frac{\sigma^2_X O_{\mathcal{U}^\star}+1}{\sigma^2_{X|V} O_{\mathcal{U}^\star}+1};\end{aligned}$$

hence, $I_s(\sigma^2_{X|V},\mathcal{A},\mathcal{U}) \geq I_s(\sigma^2_{X|V},\mathcal{A}^\star,\mathcal{U}^\star)$, and we conclude that for any $\sigma^2_{X|V} \in (0,\sigma^2_X]$,

$$\min_{\mathcal{A}\in\mathbb{A}}\min_{\mathcal{U}\in\mathbb{U}} I_s(\sigma^2_{X|V},\mathcal{A},\mathcal{U}) = I_s(\sigma^2_{X|V},\mathcal{A}^\star,\mathcal{U}^\star). \tag{10}$$

Then, we have

$$\begin{aligned}&\min_{\mathcal{A}\in\mathbb{A}}\min_{\mathcal{U}\in\mathbb{U}} \max_{\substack{0<\sigma^2_{X|V}\leq\sigma^2_X \\ \text{s.t. } I_p(\sigma^2_{X|V},\mathcal{A})\leq R_p}} I_s(\sigma^2_{X|V},\mathcal{A},\mathcal{U}) \\ &\overset{(a)}{=} \min_{\mathcal{A}\in\mathbb{A}}\min_{\mathcal{U}\in\mathbb{U}} I_s(\sigma^{2\star}_{X|V}(\mathcal{A},\mathcal{U}),\mathcal{A},\mathcal{U}) \\ &\overset{(b)}{=} I_s(\sigma^{2\star}_{X|V}(\mathcal{A}^\star,\mathcal{U}^\star),\mathcal{A}^\star,\mathcal{U}^\star) \\ &= \max_{\substack{0<\sigma^2_{X|V}\leq\sigma^2_X \\ \text{s.t. } I_p(\sigma^2_{X|V},\mathcal{A}^\star)\leq R_p}} I_s(\sigma^2_{X|V},\mathcal{A}^\star,\mathcal{U}^\star) \\ &\overset{(c)}{=} \max_{\substack{0<\sigma^2_{X|V}\leq\sigma^2_X \\ \text{s.t. } I_p(\sigma^2_{X|V},\mathcal{A}^\star)\leq R_p}} \min_{\mathcal{A}\in\mathbb{A}}\min_{\mathcal{U}\in\mathbb{U}} I_s(\sigma^2_{X|V},\mathcal{A},\mathcal{U}),\end{aligned}$$

where in (a) we have defined for $\mathcal{A} \in \mathbb{A}$, $\mathcal{U} \in \mathbb{U}$,

$$\sigma^{2\star}_{X|V}(\mathcal{A},\mathcal{U}) \triangleq \operatorname*{arg\,max}_{\substack{0<\sigma^2_{X|V}\leq\sigma^2_X \\ \text{s.t. } I_p(\sigma^2_{X|V},\mathcal{A})\leq R_p}} I_s(\sigma^2_{X|V},\mathcal{A},\mathcal{U}),$$

(b) holds because for any $\mathcal{A} \in \mathbb{A}$, $\mathcal{U} \in \mathbb{U}$, we have $I_s(\sigma^{2\star}_{X|V}(\mathcal{A},\mathcal{U}),\mathcal{A},\mathcal{U}) \geq I_s(\sigma^{2\star}_{X|V}(\mathcal{A},\mathcal{U}),\mathcal{A}^\star,\mathcal{U}^\star) \geq I_s(\sigma^{2\star}_{X|V}(\mathcal{A}^\star,\mathcal{U}^\star),\mathcal{A}^\star,\mathcal{U}^\star)$, where the first inequality holds by (10), and the second inequality holds because $I_s(\sigma^{2\star}_{X|V}(\mathcal{A},\mathcal{U}),\mathcal{A}^\star,\mathcal{U}^\star)$ is a non-increasing function of $\sigma^{2\star}_{X|V}(\mathcal{A},\mathcal{U})$ by Lemma 2, and $\sigma^{2\star}_{X|V}(\mathcal{A}^\star,\mathcal{U}^\star) \geq \sigma^{2\star}_{X|V}(\mathcal{A},\mathcal{U})$ by (8) in the proof of Lemma 4, and (c) holds by (10). □

Next, we remark that if there exist $\mathcal{A} \in \mathbb{A}$ and $\mathcal{U} \in \mathbb{U}$ such that $O_{\mathcal{A}} < O_{\mathcal{U}}$, then $C_s(\mathbb{A},R_p) = 0$ by Lemma 3 and Lemma 2 applied to $f_{\sigma^2_X,\sigma^2_{X|V}}$. Thus, we obtain the converse of Theorem 1 by combining Lemmas 3, 4, and 5.

VI. Achievability Proof of Theorem 1

To prove the achievability part of Theorem 1, we first prove an achievability result for discrete random variables in Section VI-A and then extend our result to Gaussian random variables by a quantization argument in Section VI-B.

A. Discrete Case

Our coding scheme decouples the requirements (1) (reliability) and (2) (security with respect to unauthorized groups of colluding users). Specifically, as described next, we repeat $q \in \mathbb{N}$ times a reconciliation step to handle (1) via a compound version of Wyner-Ziv coding and then perform a privacy amplification step to handle (2) via universal hashing implemented with extractors. Note that Wyner-Ziv coding is a key component to handle rate-limited communication constraints as in rate-limited secret-key generation [24] and biometric secrecy system models, e.g., [25]–[29], which rely on rate-limited secret-key generation. Here, unlike in [25]–[29], we employ a compound version of Wyner-Ziv coding because unlike in [25]–[29], we simultaneously consider multiple reliability constraints due to the presence of an access structure.

1) Reconciliation Step: Let $n \in \mathbb{N}$ and $\epsilon > 0$. For a probability mass function p_X, denote the set of ϵ-letter typical sequences [30] (see also [31]) with respect to p_X by $\mathcal{T}^n_\epsilon(X)$, and define $supp(p_X) \triangleq \{x \in \mathcal{X} : p_X(x) > 0\}$ and $\mu_X \triangleq \min_{x\in supp(p_X)} p_X(x)$. Define $\epsilon_1 \triangleq \frac{1}{2}\epsilon$.

a) Code construction: Fix a joint probability distribution $p_{VXY_{\mathcal{L}}}$ on $\mathcal{V}\times\mathcal{X}\times\mathcal{Y}_{\mathcal{L}}$, where V is an auxiliary random variable such that $V - X - Y_{\mathcal{L}}$ forms a Markov chain. Define $R_v \triangleq \max_{\mathcal{A}\in\mathbb{A}} H(V|Y_{\mathcal{A}}) - H(V|X) + 6\epsilon H(V)$, $R'_v \triangleq H(V) - \max_{\mathcal{A}\in\mathbb{A}} H(V|Y_{\mathcal{A}}) - 3\epsilon H(V)$. Generate $2^{n(R_v+R'_v)}$ codewords, labeled $v^n(\omega,\nu)$ with $(\omega,\nu) \in [\![1,2^{nR_v}]\!] \times [\![1,2^{nR'_v}]\!]$, by generating the symbols $v_i(\omega,\nu)$ for $i \in [\![1,n]\!]$ and $(\omega,\nu) \in [\![1,2^{nR_v}]\!] \times [\![1,2^{nR'_v}]\!]$ independently according to p_V.

b) Encoding: Given x^n, find a pair (ω,ν) such that $(x^n, v^n(\omega,\nu)) \in \mathcal{T}^n_\epsilon(XV)$. If there are several pairs, choose one (according to the lexicographic order); otherwise, set $(\omega,\nu) = (1,1)$. Define $v^n \triangleq v^n(\omega,\nu)$, and transmit $m \triangleq \omega$.

c) Decoding: Let $\mathcal{A} \in \mathbb{A}$. Given $y_{\mathcal{A}}^n$ and m, find $\tilde{\nu}_{\mathcal{A}}$ such that $(y_{\mathcal{A}}^n, v^n(\omega, \tilde{\nu}_{\mathcal{A}})) \in \mathcal{T}_\epsilon^n(Y_{\mathcal{A}}V)$. If there is one or more $\tilde{\nu}_{\mathcal{A}}$, then choose the smallest; otherwise, set $\tilde{\nu}_{\mathcal{A}} = 1$. Define $\widehat{v}_{\mathcal{A}}^n \triangleq v^n(\omega, \tilde{\nu}_{\mathcal{A}})$.

d) Probability of error: The random variable that represents the randomly generated code is denoted by C_n. As shown in Appendix C, there exists a codebook $\mathcal{C}_n^\star$ such that

$$\max_{\mathcal{A}\in\mathbb{A}} \mathbb{P}[V^n \neq \widehat{V}_{\mathcal{A}}^n] \leq |\mathbb{A}| \max_{\mathcal{A}\in\mathbb{A}} \delta(n,\epsilon,\mathcal{A}), \tag{11}$$

where

$$\begin{aligned}\delta(n,\epsilon,\mathcal{A}) \triangleq\ & 2|\mathcal{X}||\mathcal{Y}_{\mathcal{A}}|e^{-n\epsilon_1^2\mu_{XY_{\mathcal{A}}}} + 2^{-n\epsilon H(V)} \\ & + \exp(-(1-2|\mathcal{V}||\mathcal{X}|e^{-n\frac{(\epsilon-\epsilon_1)^2}{1+\epsilon_1}}\mu_{VX})2^{\epsilon n H(V)}) \\ & + 2|\mathcal{V}||\mathcal{X}||\mathcal{Y}_{\mathcal{A}}|e^{-n\frac{(\epsilon-\epsilon_1)^2}{1+\epsilon_1}\mu_{VXY_{\mathcal{A}}}}.\end{aligned}$$

2) Privacy Amplification Step: Let $q, n \in \mathbb{N}$, and define $N \triangleq nq$. The reconciliation step is repeated q times such that the dealer has $V^N = (V^n)^q$ and the participants in $\mathcal{A} \in \mathbb{A}$ have $(\widehat{V}_{\mathcal{A}}^n)^q$. Note that the total public communication $M \in \mathcal{M}$ is such that $\frac{H(M)}{N} \leq \frac{\log|\mathcal{M}|}{N} = \max_{\mathcal{A}\in\mathbb{A}} I(X;V|Y_{\mathcal{A}}) + 6\epsilon H(V)$. Next, another round of reconciliation with negligible communication is performed to ensure that $\max_{\mathcal{A}\in\mathbb{A}} \mathbb{P}[(V^n)^q \neq (\widehat{V}_{\mathcal{A}}^n)^q] \leq \delta(q)$, where $\lim_{q\to\infty}\delta(q) = 0$ when n is fixed. Finally, the dealer computes $S = g(V^N, U_d)$, while the participants in $\mathcal{A} \in \mathbb{A}$ compute $\widehat{S}(\mathcal{A}) = g(\widehat{V}_{\mathcal{A}}^N, U_d)$, where U_d is a sequence of d (to be defined later) uniformly distributed random bits, and $g : \{0,1\}^N \times \{0,1\}^d \to \{0,1\}^k$ is to be defined later.

3) Analysis of Reliability: The secrets computed by the dealer and the participants in $\mathcal{A} \in \mathbb{A}$ are asymptotically the same for a fixed n as q goes to infinity.

$$\mathbb{P}[\widehat{S}(\mathcal{A}) \neq S] \leq \mathbb{P}[(\widehat{V}_{\mathcal{A}}^n)^q \neq (V^n)^q] \leq \delta(q).$$

4) Analysis of Security: Let the min-entropy of a discrete random variable X, defined over $\mathcal{X}$ with probability mass function p_X, be denoted by $H_\infty(X) \triangleq -\log(\max_{x\in\mathcal{X}} p_X(x))$. We will use the following lemmas:

Lemma 6 (Adapted from [32]): Let $E_{\mathcal{U}}$ be the random variable that represents the total knowledge about V^N available to participants in $\mathcal{U} \in \mathbb{U}$. Let $e_{\mathcal{U}}$ be a particular realization of $E_{\mathcal{U}}$. If $H_\infty(V^N|E_{\mathcal{U}} = e_{\mathcal{U}}) \geq \gamma N$, for some $\gamma \in [0,1]\backslash\{0,1\}$, then there exists an extractor $g : \{0,1\}^N \times \{0,1\}^d \to \{0,1\}^k$ with $d \leq N\delta(N)$ and $k \geq N(\gamma - \delta(N))$, where $\delta(N)$ is such that $\lim_{N\to+\infty}\delta(N) = 0$. Moreover,

$$H(S|U_d, E_{\mathcal{U}} = e_{\mathcal{U}}) \geq k - \delta^\star(N),$$

with $\delta^\star(N) = 2^{-\sqrt{N}/\log N}(k + \sqrt{N}/\log N)$.

Lemma 7 ([32], See Also [33]): Consider a discrete memoryless source $(\mathcal{X}\times\mathcal{Y}, p_{XY})$ and define

$$\Theta \triangleq \mathbb{1}\{(X^q, Y^q) \in \mathcal{T}_{2\epsilon}^q(XY)\}\mathbb{1}\{Y^q \in \mathcal{T}_\epsilon^q(Y)\}.$$

Then, $\mathbb{P}[\Theta = 1] \geq 1 - (2|S_X|e^{-\epsilon^2 q\mu_X/3} + 2|S_{XY}|e^{-\epsilon^2 q\mu_{XY}/3})$, with $S_{XY} \triangleq supp(p_{XY})$ and $S_Y \triangleq supp(p_Y)$. Moreover, if $y^q \in \mathcal{T}_\epsilon^q(Y)$, then

$$\begin{aligned}&H_\infty(X^q|Y^q = y^q, \Theta = 1) \\ &\geq q(1-\epsilon)H(X|Y) + \log(1 - 2|S_{XY}|e^{-\epsilon^2 q\mu_{XY}/6}).\end{aligned}$$

Define for any $\mathcal{U} \in \mathbb{U}$, the random variables

$$\Theta_{\mathcal{U}} \triangleq \mathbb{1}\{(V^N, Y_{\mathcal{U}}^N) \in \mathcal{T}_{2\epsilon}^q(V^n Y_{\mathcal{U}}^n)\}\mathbb{1}\{Y_{\mathcal{U}}^N \in \mathcal{T}_\epsilon^q(Y_{\mathcal{U}}^n)\}, \tag{12}$$

$$\begin{aligned}\Upsilon_{\mathcal{U}} \triangleq \mathbb{1}\{&H_\infty(V^N|Y_{\mathcal{U}}^N = y_{\mathcal{U}}^N, \Theta_{\mathcal{U}} = 1) \\ &- H_\infty(V^N|Y_{\mathcal{U}}^N = y_{\mathcal{U}}^N, M = m, \Theta_{\mathcal{U}} = 1) \\ &\leq \log|\mathcal{M}| + \sqrt{N}\}.\end{aligned} \tag{13}$$

For any $\mathcal{U} \in \mathbb{U}$, $\mathbb{P}[\Theta_{\mathcal{U}} = 1] \geq 1 - \delta_\epsilon^0(n,\mathcal{U})$, where $\delta_\epsilon^0(n,\mathcal{U}) \triangleq 2|S_{V^n}|e^{-\epsilon^2 q\mu_{V^n}/3} + 2|S_{V^n Y_{\mathcal{U}}^n}|e^{-\epsilon^2 q\mu_{V^n Y_{\mathcal{U}}^n}/3}$ by Lemma 7 applied to the discrete memoryless source model $(\mathcal{V}^n \times \mathcal{Y}_{\mathcal{U}}^n, p_{V^n Y_{\mathcal{U}}^n})$, and $\mathbb{P}[\Upsilon_{\mathcal{U}} = 1] \geq 1 - 2^{-\sqrt{N}}$ by [32, Lemma 10]. Hence,

$$\mathbb{P}[\Upsilon_{\mathcal{U}} = 1, \Theta_{\mathcal{U}} = 1] \geq 1 - \delta_\epsilon^0(n,\mathcal{U}) - 2^{-\sqrt{N}}. \tag{14}$$

Then, for any $\mathcal{U} \in \mathbb{U}$, we have

$$\begin{aligned}H(S|U_d Y_{\mathcal{U}}^N M) &\overset{(a)}{\geq} H(S|U_d Y_{\mathcal{U}}^N M \Theta_{\mathcal{U}} \Upsilon_{\mathcal{U}}) \\ &\geq \min_{\mathcal{U}\in\mathbb{U}} H(S|U_d Y_{\mathcal{U}}^N M \Theta_{\mathcal{U}} \Upsilon_{\mathcal{U}}) \\ &\geq \min_{\mathcal{U}\in\mathbb{U}} \mathbb{P}[\Theta_{\mathcal{U}} = 1, \Upsilon_{\mathcal{U}} = 1] \\ &\qquad \times H(S|U_d Y_{\mathcal{U}}^N M, \Theta_{\mathcal{U}} = 1, \Upsilon_{\mathcal{U}} = 1) \\ &\geq \min_{\mathcal{U}\in\mathbb{U}} \mathbb{P}[\Theta_{\mathcal{U}} = 1, \Upsilon_{\mathcal{U}} = 1] \\ &\quad \times \min_{\mathcal{U}\in\mathbb{U}} H(S|U_d Y_{\mathcal{U}}^N M, \Theta_{\mathcal{U}} = 1, \Upsilon_{\mathcal{U}} = 1) \\ &\overset{(b)}{\geq} \left(1 - \max_{\mathcal{U}\in\mathbb{U}} \delta_\epsilon^0(n,\mathcal{U}) - 2^{-\sqrt{N}}\right) \\ &\quad \times \min_{\mathcal{U}\in\mathbb{U}} H(S|U_d Y_{\mathcal{U}}^N M, \Theta_{\mathcal{U}} = 1, \Upsilon_{\mathcal{U}} = 1),\end{aligned} \tag{15}$$

where (a) holds because conditioning reduces entropy and (b) holds by (14). To lower bound $\min_{\mathcal{U}\in\mathbb{U}} H(S|U_d Y_{\mathcal{U}}^N M, \Theta_{\mathcal{U}} = 1, \Upsilon_{\mathcal{U}} = 1)$ in (15) with Lemma 6, we now lower bound $\min_{\mathcal{U}\in\mathbb{U}} H_\infty(V^N|Y_{\mathcal{U}}^N = y_{\mathcal{U}}^N, M = m, \Theta_{\mathcal{U}} = 1, \Upsilon_{\mathcal{U}} = 1)$. We have for any $\mathcal{U} \in \mathbb{U}$,

$$\begin{aligned}&H_\infty(V^N|Y_{\mathcal{U}}^N = y_{\mathcal{U}}^N, M = m, \Theta_{\mathcal{U}} = 1, \Upsilon_{\mathcal{U}} = 1) \\ &\overset{(a)}{\geq} H_\infty(V^N|Y_{\mathcal{U}}^N = y_{\mathcal{U}}^N, \Theta_{\mathcal{U}} = 1) - \log|\mathcal{M}| - \sqrt{N} \\ &\overset{(b)}{\geq} q(1-\epsilon)H(V^n|Y_{\mathcal{U}}^n) - \delta_\epsilon^1(q,n,\mathcal{U}) - N(\max_{\mathcal{A}\in\mathbb{A}} I(V;X|Y_{\mathcal{A}}) \\ &\qquad + 6\epsilon H(V)) - \sqrt{N} \\ &\overset{(c)}{\geq} N[I(X;V|Y_{\mathcal{U}}) - \max_{\mathcal{A}\in\mathbb{A}} I(V;X|Y_{\mathcal{A}}) - \delta_\epsilon^2(q,n,\mathcal{U})] \\ &\geq N[\min_{\mathcal{U}\in\mathbb{U}} I(X;V|Y_{\mathcal{U}}) - \max_{\mathcal{A}\in\mathbb{A}} I(V;X|Y_{\mathcal{A}}) - \max_{\mathcal{U}\in\mathbb{U}} \delta_\epsilon^2(q,n,\mathcal{U})] \\ &\overset{(d)}{=} N[\min_{\mathcal{A}\in\mathbb{A}} I(V;Y_{\mathcal{A}}) - \max_{\mathcal{U}\in\mathbb{U}} I(V;Y_{\mathcal{U}}) - \max_{\mathcal{U}\in\mathbb{U}} \delta_\epsilon^2(q,n,\mathcal{U})],\end{aligned} \tag{16}$$

where (a) holds by (13), (b) holds by Lemma 7 with $\delta_\epsilon^1(q,n,\mathcal{U}) \triangleq -\log(1 - 2|S_{V^n Y_{\mathcal{U}}^n}|e^{-\epsilon^2 q\mu_{V^n Y_{\mathcal{U}}^n}/6})$, (c) holds with $\delta_\epsilon^2(q,n,\mathcal{U}) \triangleq \epsilon I(X;V|Y_{\mathcal{U}}) + (1-\epsilon)[2\epsilon H(X|Y_{\mathcal{U}}V) + 2n^{-1} + \log|\mathcal{X}|(4|\mathcal{V}||\mathcal{X}|e^{-n\epsilon^2\mu_{XV}} + 2|\mathcal{V}||\mathcal{X}||\mathcal{Y}_{\mathcal{U}}|$

$e^{-\epsilon^2 n\mu_{VXY_{\mathcal{U}}}/8})] + N^{-1}\delta_\epsilon^1(q,n,\mathcal{U}) + 6\epsilon H(V) + N^{-1/2}$ because, as shown in Appendix D, we have

$$\begin{aligned} H(V^n|Y_{\mathcal{U}}^n) \geq n(H(X|Y_{\mathcal{U}}) - H(X|Y_{\mathcal{U}}V)(1+2\epsilon)) \\ -2 - n\log|\mathcal{X}|(4|\mathcal{V}||\mathcal{X}|e^{-n\epsilon^2\mu_{XV}} \\ +2|\mathcal{V}||\mathcal{X}||\mathcal{Y}_{\mathcal{U}}|e^{-\epsilon^2 n\mu_{VXY_{\mathcal{U}}}/8}), \end{aligned} \tag{17}$$

and (d) holds because $V - X - (Y_{\mathcal{A}}, Y_{\mathcal{U}})$.

Next, we set the output size k of the extractor to be less than the lower bound in (16) by $\sqrt{N}$, i.e.,

$$\begin{aligned} k \triangleq \lfloor N[\min_{\mathcal{A}\in\mathbb{A}} I(V;Y_{\mathcal{A}}) - \max_{\mathcal{U}\in\mathbb{U}} I(V;Y_{\mathcal{U}}) - \max_{\mathcal{U}\in\mathbb{U}} \delta_\epsilon^2(q,n,\mathcal{U}) \\ - N^{-1/2}]\rfloor, \end{aligned} \tag{18}$$

Finally, we have

$$\begin{aligned} \max_{\mathcal{U}\in\mathbb{U}} I(S;U_d Y_{\mathcal{U}}^N M) &= H(S) - \min_{\mathcal{U}\in\mathbb{U}} H(S|U_d Y_{\mathcal{U}}^N M) \\ &\overset{(a)}{\leq} k - \left(1 - \max_{\mathcal{U}\in\mathbb{U}} \delta_\epsilon^0(n,\mathcal{U}) - 2^{-\sqrt{N}}\right) \\ &\qquad \times (k - \delta^\star(N)) \\ &\overset{(b)}{\leq} \delta_\epsilon^3(N), \end{aligned} \tag{19}$$

where (a) holds by (15), (16) (valid for any $\mathcal{U}\in\mathbb{U}$), (18), and Lemma 6 with $\delta^\star(N) \triangleq 2^{-\sqrt{N}/\log N}(k+\sqrt{N}/\log N)$ and (b) holds with $\delta_\epsilon^3(N) \triangleq \delta^\star(N) + (\max_{\mathcal{U}\in\mathbb{U}} \delta_\epsilon^0(n,\mathcal{U}) + 2^{-\sqrt{N}})k$.

5) Analysis of Uniformity: Similar to (19), we have

$$\begin{aligned} H(S) &\geq \min_{\mathcal{U}\in\mathbb{U}} H(S|U_d Y_{\mathcal{U}}^N M) \\ &\geq k - \delta_\epsilon^3(N). \end{aligned} \tag{20}$$

6) Public Communication Rate: The public communication rate corresponds to the rate of M plus the rate of U_d, i.e.,

$$\lim_{N\to\infty} R_p = \max_{\mathcal{A}\in\mathbb{A}} I(X;V|Y_{\mathcal{A}}) + 6\epsilon H(V).$$

7) Achievable Secret Rate: The secret rate $R_s \triangleq k/N$ satisfies

$$\begin{aligned} R_s \geq \min_{\mathcal{A}\in\mathbb{A}} I(V;Y_{\mathcal{A}}) - \max_{\mathcal{U}\in\mathbb{U}} I(V;Y_{\mathcal{U}}) - \max_{\mathcal{U}\in\mathbb{U}} \delta_\epsilon^2(q,n,\mathcal{U}) \\ - N^{-1/2} - N^{-1}. \end{aligned} \tag{21}$$

B. Continuous Case

In this section, we extend the achievability result of Section VI-A for discrete random variables to Gaussian random variables by means of quantization. Quantization also allows us to show that the size of the shares linearly scales with the length of the secret. The main issue with quantization is that it might lead to an underestimation of the information that unauthorized sets of participants may learn about the secret. We will, however, show that this issue can be overcome provided that the quantization is fine enough.

We now build upon Section VI-A to show that $(R_p, R_s) \in \mathcal{R}(p_{XY_{\mathcal{C}}}, \mathbb{A})$, where

$$R_p = \frac{1}{2}\log\frac{\sigma_X^2}{\sigma_{X|V}^2} - \frac{1}{2}\log\frac{\sigma_X^2 O_{\mathcal{A}^\star} + 1}{\sigma_{X|V}^2 O_{\mathcal{A}^\star} + 1}, \tag{22}$$

$$R_s = \frac{1}{2}\log\frac{\sigma_X^2 O_{\mathcal{A}^\star} + 1}{\sigma_{X|V}^2 O_{\mathcal{A}^\star} + 1} - \frac{1}{2}\log\frac{\sigma_X^2 O_{\mathcal{U}^\star} + 1}{\sigma_{X|V}^2 O_{\mathcal{U}^\star} + 1}. \tag{23}$$

We use the following lemma to extend Section VI-A to the continuous case by means of quantization.

Lemma 8 ([34]–[36]): Let X and Y be two real-valued random variables with probability distribution $\mathbb{P}_X$ and $\mathbb{P}_Y$, respectively. Let $\mathcal{C}_{\Delta_1} = \{C_i\}_{i\in\mathcal{I}}$, $\mathcal{D}_{\Delta_2} = \{D_j\}_{j\in\mathcal{J}}$ be two partitions of the real line for X and Y such that for any $i\in\mathcal{I}$, $\mathbb{P}_X[C_i] = \Delta_1$, for any $j\in\mathcal{J}$, $\mathbb{P}_Y[D_j] = \Delta_2$, where Δ_1, $\Delta_2 > 0$. Let $X_{\Delta_1}, Y_{\Delta_2}$ be the quantized version of X, Y with respect to the partitions $\mathcal{C}_{\Delta_1}, \mathcal{D}_{\Delta_2}$, respectively. Then, we have

$$I(X,Y) = \lim_{\Delta_1,\Delta_2\to 0} I(X_{\Delta_1}, Y_{\Delta_2}).$$

We first show that a quantization does not affect the security requirement (2).

Proposition 1: A quantization of $Y_{\mathcal{U}}^n, \mathcal{U}\in\mathbb{U}$, might lead to an underestimation of $I(S;M,Y_{\mathcal{U}}^n)$. However, if the quantized version $Y_{\mathcal{U},\Delta}^n$ of $Y_{\mathcal{U}}^n, \mathcal{U}\in\mathbb{U}$, is fine enough, then for any $\delta > 0$

$$\max_{\mathcal{U}\in\mathbb{U}} I(S;MY_{\mathcal{U}}^n) \leq \max_{\mathcal{U}\in\mathbb{U}} I(S;MY_{\mathcal{U},\Delta}^n) + \delta. \tag{24}$$

Proof: For any $\delta > 0$, for any $\mathcal{U}\in\mathbb{U}$, we have

$$\begin{aligned} I(S;MY_{\mathcal{U}}^n) &\leq |I(S;MY_{\mathcal{U}}^n) - I(S;MY_{\mathcal{U},\Delta}^n)| + I(S;MY_{\mathcal{U},\Delta}^n) \\ &\leq \max_{\mathcal{U}\in\mathbb{U}} |I(S;MY_{\mathcal{U}}^n) - I(S;MY_{\mathcal{U},\Delta}^n)| \\ &\qquad + \max_{\mathcal{U}\in\mathbb{U}} I(S;MY_{\mathcal{U},\Delta}^n) \\ &\leq \delta + \max_{\mathcal{U}\in\mathbb{U}} I(S;MY_{\mathcal{U},\Delta}^n), \end{aligned} \tag{25}$$

where the last inequality holds by Lemma 8, if the quantized version $Y_{\mathcal{U},\Delta}^n$ of $Y_{\mathcal{U}}^n$, $\mathcal{U}\in\mathbb{U}$, is fine enough. Since (25) is valid for any $\mathcal{U}\in\mathbb{U}$, we obtain (24). □

For $\mathcal{A}\in\mathbb{A}$ and $\mathcal{U}\in\mathbb{U}$, we quantize $X, Y_{\mathcal{A}}, Y_{\mathcal{U}}$, and V as in Lemma 8 to form $X_\Delta, Y_{\mathcal{A},\Delta}, Y_{\mathcal{U},\Delta}$, and V_Δ such that $\Delta = l^{-1}$ and $|\mathcal{X}_\Delta| = |\mathcal{Y}_{\mathcal{A},\Delta}| = |\mathcal{Y}_{\mathcal{U},\Delta}| = |\mathcal{V}_\Delta| = l$ with $l > 0$. Next, we apply the proof for the discrete case to the random variables $X_\Delta, Y_{\mathcal{A},\Delta}, Y_{\mathcal{U},\Delta}, V_\Delta$. By Lemma 8, we can fix l large enough such that, for any $\mathcal{A}\in\mathbb{A}$, $|I(V_\Delta;Y_{\mathcal{A},\Delta}) - I(V;Y_{\mathcal{A}})| < \delta/2$, for any $\mathcal{U}\in\mathbb{U}$, $|I(V_\Delta;Y_{\mathcal{U},\Delta}) - I(V;Y_{\mathcal{U}})| < \delta/2$, such that (21) becomes

$$\begin{aligned} R_s \geq \min_{\mathcal{A}\in\mathbb{A}} I(V;Y_{\mathcal{A}}) - \max_{\mathcal{U}\in\mathbb{U}} I(V;Y_{\mathcal{U}}) - \max_{\mathcal{U}\in\mathbb{U}} \delta_\epsilon^2(q,n,\mathcal{U}) \\ - N^{-1/2} - N^{-1} - \delta. \end{aligned}$$

Note that $\delta_\epsilon^2(q,n,\mathcal{U})$, $\mathcal{U}\in\mathbb{U}$, in the above equation hides the terms $2\epsilon(1-\epsilon)H(X_\Delta|Y_{\mathcal{U},\Delta}V_\Delta)$ and $6\epsilon H(V_\Delta)$, which do not go to zero as l goes to infinity. Consequently, we choose $\epsilon = n^{-\alpha}$, where $\alpha\in[0,1/2]\backslash\{0,1/2\}$, such that if we choose l large enough, then n large enough, and finally q large enough, then the asymptotic secret rate is as close as desired to

$$\min_{\mathcal{A}\in\mathbb{A}} I(V;Y_{\mathcal{A}}) - \max_{\mathcal{U}\in\mathbb{U}} I(V;Y_{\mathcal{U}}), \tag{26}$$

$\delta_\epsilon^3(N)$ vanishes to zero in (19), (20), and the asymptotic public communication rate is as close as desired to

$$\max_{\mathcal{A}\in\mathbb{A}} I(V;X|Y_{\mathcal{A}}). \tag{27}$$

By taking the auxiliary random variable V jointly Gaussian with X in (26) and (27), we obtain (22) and (23), as shown in Appendix E.

Remark 2: We observe that the size of the shares scales linearly with the secret size. First, note that the size of each share is the sum of the length of the public communication, i.e., NR_p bits, and the length of N quantized observations of a Gaussian random variable. Then, since we achieve the secret rate in (26) by making the quantization parameter l fixed when N grows to infinity, we conclude that the size of the shares scales linearly with N, which is also the case for the length of the generated secret.

VII. Concluding Remarks

We studied information-theoretic secret sharing from Gaussian correlated sources over a one-way rate-limited public channel and characterized its secret capacity, which provides a closed-form expression of the trade-off between public communication and the secret rate. By contrast with a traditional secret-sharing protocol, our setting does not require information-theoretically secure channels between the dealer and participants, and provides information-theoretic security during the distribution phase, where the dealer distributes shares of the secret to the participants. Moreover, we have shown that the size of the shares scales linearly with the size of the secret for any access structure. We also characterized the secret capacity for threshold access structures and showed that the secret capacity is, in general, not a monotone function of the threshold.

While explicit and low-complexity coding schemes have been proposed for information-theoretic secret sharing that rely on discrete channel models [37], [38] and discrete source models [39], developing low-complexity coding schemes that achieve the limits derived in this paper for Gaussian sources remains an open problem.

Appendix A
Derivation of (4), (5)

Let Z and Z' be zero-mean jointly Gaussian and jointly non-singular random vectors with covariance matrices Σ_Z and Σ_Z', respectively. By [40, Theorem 3.5.2], we have

$$Z' = PZ + W, \tag{28}$$

where $P \triangleq \Sigma_{Z'Z}\Sigma_Z^{-1}$ and W is independent of Z with covariance $\Sigma_W \triangleq \Sigma_{Z'} - \Sigma_{Z'Z}\Sigma_Z^{-1}\Sigma_{Z'Z}^T$. Hence, by (28), we have for any $\mathcal{S} \subseteq \mathcal{L}$

$$Y_{\mathcal{S}} = \Sigma_{Y_{\mathcal{S}}X}\sigma_X^{-2}X + W_{Y_{\mathcal{S}}}, \tag{29}$$

where $\Sigma_{W_{Y_{\mathcal{S}}}} \triangleq \Sigma_{Y_{\mathcal{S}}} - \Sigma_{Y_{\mathcal{S}}X}\sigma_X^{-2}\Sigma_{Y_{\mathcal{S}}X}^T$. Then, we normalize (29) as follows. By Cholesky decomposition, there exists an invertible matrix $B \in \mathbb{R}^{|\mathcal{S}|\times|\mathcal{S}|}$ such that $\Sigma_{W_{Y_{\mathcal{S}}}} = BB^T$. Hence, (29) can be rewritten as

$$Y'_{\mathcal{S}} = H_{\mathcal{S}}X + W'_{Y_{\mathcal{S}}},$$

where $Y'_{\mathcal{S}} \triangleq B^{-1}Y_{\mathcal{S}}$, $H_{\mathcal{S}} = B^{-1}\Sigma_{Y_{\mathcal{S}}X}\sigma_X^{-2}$, and $W'_{Y_{\mathcal{S}}} \sim \mathcal{N}(0, I_{|\mathcal{S}|})$.

Appendix B
Proof of Theorem 2

To prove Theorem 2, we proceed as follows. For a threshold access structure $\mathbb{A}_t$, we first prove that there exist sets of authorized and unauthorized participants $\mathcal{A}_t^\star \in \arg\min_{\mathcal{A}\in\mathbb{A}_t} H_{\mathcal{A}}^T H_{\mathcal{A}}$ and $\mathcal{U}_t^\star \in \arg\max_{\mathcal{U}\in\mathbb{U}_t} H_{\mathcal{U}}^T H_{\mathcal{U}}$, respectively, such that for any $t \in [\![1, L-1]\!]$, $\mathcal{A}_t^\star \subset \mathcal{A}_{t+1}^\star$, $\mathcal{U}_t^\star \subset \mathcal{U}_{t+1}^\star$. Then, by Theorem 1, we remark that $\mathcal{A}_t^\star$ and $\mathcal{U}_t^\star$ also correspond to the sets that appear in the expression of the secret capacity for the threshold access structure $\mathbb{A}_t$. Finally, using the monotonicity property (with respect to t) of the sets $(\mathcal{A}_t^\star)_{t\in[\![1,L]\!]}$ and $(\mathcal{U}_t^\star)_{t\in[\![1,L]\!]}$ and Theorem 1, we derive necessary and sufficient conditions to determine whether the secret capacity increases or decreases as the threshold t increases.

We will need the following lemma.

Lemma 9: Let $a, c \in \mathbb{R}_+$ and $R_p \in \mathbb{R}_+$. The function f_{a,c,R_p} is non-increasing

$$f_{a,c,R_p} : \mathbb{R}_+ \to \mathbb{R}, \quad y \mapsto \frac{1}{2}\log\frac{cy2^{-2R_p} + ca(1-2^{-2R_p}) + 1}{cy+1}.$$

Proof: The derivative of f_{a,c,R_p} at $y \in \mathbb{R}_+$ is $f'_{a,c,R_p} = \frac{1}{2\ln 2}\frac{c(1+ca)(2^{-2R_p}-1)}{(cy+1)\left(cy2^{-2R_p}+ca(1-2^{-2R_p})+1\right)} \leq 0$. □

Using Lemma 9, we obtain the following result:

Lemma 10: One can find sets $(\mathcal{A}_t^\star)_{t\in[\![1,L]\!]}$ and $(\mathcal{U}_t^\star)_{t\in[\![1,L]\!]}$ such that for any $t \in [\![1, L-1]\!]$, we have $\mathcal{A}_t^\star \subset \mathcal{A}_{t+1}^\star$, $\mathcal{U}_t^\star \subset \mathcal{U}_{t+1}^\star$, and for any $t \in [\![1, L]\!]$,

$$\{\mathcal{A}_t^\star, \mathcal{U}_t^\star\} \in \arg\min_{\mathcal{A}\in\mathbb{A}_t, \mathcal{U}\in\mathbb{U}_t} \left[f_{H_{\mathcal{A}}^T H_{\mathcal{A}}, \sigma_X^2, R_p}(H_{\mathcal{U}}^T H_{\mathcal{U}})\right]^+, \tag{30}$$

where we have used the notation of Lemma 9.

Proof: For $t \in [\![1, L]\!]$, remark that

$$\arg\min_{\mathcal{A}\in\mathbb{A}_t, \mathcal{U}\in\mathbb{U}_t} \left[f_{H_{\mathcal{A}}^T H_{\mathcal{A}}, \sigma_X^2, R_p}(H_{\mathcal{U}}^T H_{\mathcal{U}})\right]^+ = \left\{\arg\min_{\mathcal{A}\in\mathbb{A}_t} H_{\mathcal{A}}^T H_{\mathcal{A}}, \arg\max_{\mathcal{U}\in\mathbb{U}_t} H_{\mathcal{U}}^T H_{\mathcal{U}}\right\}, \tag{31}$$

because $f_{H_{\mathcal{A}}^T H_{\mathcal{A}}, \sigma_X^2, R_p}(H_{\mathcal{U}}^T H_{\mathcal{U}})$ is an increasing function of $H_{\mathcal{A}}^T H_{\mathcal{A}}$ and is a decreasing function of $H_{\mathcal{U}}^T H_{\mathcal{U}}$ by Lemma 9. Next, write the vector $H_{\mathcal{L}}$ as $H_{\mathcal{L}} = [H_{\mathcal{L}}(1), H_{\mathcal{L}}(2), \ldots, H_{\mathcal{L}}(L)]^T$. By relabelling the participants, if necessary, assume that $|H_{\mathcal{L}}(1)| \leq |H_{\mathcal{L}}(2)| \leq \cdots \leq |H_{\mathcal{L}}(L)|$. For $t \in [\![1, L]\!]$, choose $\mathcal{A}_t^\star \triangleq [\![1, t]\!]$ and $\mathcal{U}_t^\star \triangleq [\![L-t+2, L]\!]$. Clearly, for any $t \in [\![1, L-1]\!]$, we have $\mathcal{A}_t^\star \subset \mathcal{A}_{t+1}^\star$, $\mathcal{U}_t^\star \subset \mathcal{U}_{t+1}^\star$, and by (31), we have that (30) holds for any $t \in [\![1, L]\!]$. □

By Theorem 1 and (30), we have

$$C_s(\mathbb{A}_1, R_p) = \left[\frac{1}{2}\log\left(\sigma_X^2 H_{\mathcal{A}_1^\star}^T H_{\mathcal{A}_1^\star}(1-2^{-2R_p}) + 1\right)\right]^+, \tag{32}$$

and for $t \in [\![2, L]\!]$, we have

$$C_s(\mathbb{A}_t, R_p) = \left[\frac{1}{2}\log\frac{\sigma_X^2 H_{\mathcal{U}_t^\star}^T H_{\mathcal{U}_t^\star} 2^{-2R_p} + \sigma_X^2 H_{\mathcal{A}_t^\star}^T H_{\mathcal{A}_t^\star}(1-2^{-2R_p}) + 1}{\sigma_X^2 H_{\mathcal{U}_t^\star}^T H_{\mathcal{U}_t^\star} + 1}\right]^+. \tag{33}$$

Using (32) and (33), we easily obtain for any $t \in [\![1, L]\!]$

$$\begin{aligned} & C_s(\mathbb{A}_1, R_p) \geq C_s(\mathbb{A}_t, R_p) \\ \iff & \sigma_X^2 H_{\mathcal{A}_1^\star}^T H_{\mathcal{A}_1^\star} H_{\mathcal{U}_t^\star}^T H_{\mathcal{U}_t^\star} + H_{\mathcal{A}_1^\star}^T H_{\mathcal{A}_1^\star} + H_{\mathcal{U}_t^\star}^T H_{\mathcal{U}_t^\star} \\ & \qquad - H_{\mathcal{A}_t^\star}^T H_{\mathcal{A}_t^\star} \geq 0. \end{aligned}$$

From the proof of Lemma 10, there exists $O \geq 0$ such that $O \leq H_{\mathcal{U}_t^\star}^T H_{\mathcal{U}_t^\star}$ and $H_{\mathcal{A}_1^\star}^T H_{\mathcal{A}_1^\star} + O = H_{\mathcal{A}_t^\star}^T H_{\mathcal{A}_t^\star}$. Therefore, $H_{\mathcal{A}_1^\star}^T H_{\mathcal{A}_1^\star} + H_{\mathcal{U}_t^\star}^T H_{\mathcal{U}_t^\star} \geq H_{\mathcal{A}_t^\star}^T H_{\mathcal{A}_t^\star}$, and $C_s(\mathbb{A}_1, R_p) \geq C_s(\mathbb{A}_t, R_p)$.

Next, we have for $i \in [\![1, L-t]\!]$,

$$\begin{aligned} & C_s(\mathbb{A}_t, R_p) \geq C_s(\mathbb{A}_{t+i}, R_p) \\ \iff & \sigma_X^2 H_{\mathcal{A}_t^\star}^T H_{\mathcal{A}_t^\star} H_{\mathcal{U}_{t+i}^\star}^T H_{\mathcal{U}_{t+i}^\star} + H_{\mathcal{A}_t^\star}^T H_{\mathcal{A}_t^\star} + H_{\mathcal{U}_{t+i}^\star}^T H_{\mathcal{U}_{t+i}^\star} \\ & \quad \geq \sigma_X^2 H_{\mathcal{U}_t^\star}^T H_{\mathcal{U}_t^\star} H_{\mathcal{A}_{t+i}^\star}^T H_{\mathcal{A}_{t+i}^\star} + H_{\mathcal{U}_t^\star}^T H_{\mathcal{U}_t^\star} + H_{\mathcal{A}_{t+i}^\star}^T H_{\mathcal{A}_{t+i}^\star} \\ \iff & \sigma_X^2 H_{\mathcal{A}_t^\star}^T H_{\mathcal{A}_t^\star} (H_{\mathcal{U}_{t+i}^\star}^T H_{\mathcal{U}_{t+i}^\star} - H_{\mathcal{U}_t^\star}^T H_{\mathcal{U}_t^\star} + H_{\mathcal{U}_t^\star}^T H_{\mathcal{U}_t^\star}) \\ & \qquad + H_{\mathcal{U}_{t+i}^\star}^T H_{\mathcal{U}_{t+i}^\star} - H_{\mathcal{U}_t^\star}^T H_{\mathcal{U}_t^\star} \\ & \quad \geq \sigma_X^2 H_{\mathcal{U}_t^\star}^T H_{\mathcal{U}_t^\star} (H_{\mathcal{A}_{t+i}^\star}^T H_{\mathcal{A}_{t+i}^\star} - H_{\mathcal{A}_t^\star}^T H_{\mathcal{A}_t^\star} + H_{\mathcal{A}_t^\star}^T H_{\mathcal{A}_t^\star}) \\ & \qquad + H_{\mathcal{A}_{t+i}^\star}^T H_{\mathcal{A}_{t+i}^\star} - H_{\mathcal{A}_t^\star}^T H_{\mathcal{A}_t^\star} \\ \iff & (1 + \sigma_X^2 H_{\mathcal{A}_t^\star}^T H_{\mathcal{A}_t^\star})(H_{\mathcal{U}_{t+i}^\star}^T H_{\mathcal{U}_{t+i}^\star} - H_{\mathcal{U}_t^\star}^T H_{\mathcal{U}_t^\star}) \\ & \quad \geq (1 + \sigma_X^2 H_{\mathcal{U}_t^\star}^T H_{\mathcal{U}_t^\star})(H_{\mathcal{A}_{t+i}^\star}^T H_{\mathcal{A}_{t+i}^\star} - H_{\mathcal{A}_t^\star}^T H_{\mathcal{A}_t^\star}), \end{aligned}$$

where the first equivalence is obtained using (33). Note that, by Lemma 10, one can choose $\mathcal{A}_t^\star \subset \mathcal{A}_{t+i}^\star$ and $\mathcal{U}_t^\star \subset \mathcal{U}_{t+i}^\star$, hence, $H_{\mathcal{A}_{t+i}^\star}^T H_{\mathcal{A}_{t+i}^\star} - H_{\mathcal{A}_t^\star}^T H_{\mathcal{A}_t^\star} \geq 0$ and $H_{\mathcal{U}_{t+i}^\star}^T H_{\mathcal{U}_{t+i}^\star} - H_{\mathcal{U}_t^\star}^T H_{\mathcal{U}_t^\star} \geq 0$.

Appendix C
Proof of (11)

The probability of error averaged over C_n, i.e., $\mathbb{E}_{C_n}[\mathbb{P}[V^n \neq \widehat{V}_{\mathcal{A}}^n]]$ for any $\mathcal{A} \in \mathbb{A}$ can be upper bounded via the union bound by the four following terms:

1) The probability that $(x^n, y_{\mathcal{A}}^n) \notin \mathcal{T}_{\epsilon_1}^n(XY_{\mathcal{A}})$, which is upper bounded by $2|\mathcal{X}||\mathcal{Y}_{\mathcal{A}}| \exp(-n\epsilon_1^2 \mu_{XY_{\mathcal{A}}})$ [31, Page 272 Equation (1.12)].
2) The probability that the encoder cannot find (ω, ν) such that $(x^n, v^n(\omega, \nu)) \in \mathcal{T}_\epsilon^n(XV)$, given that $(x^n, y_{\mathcal{A}}^n) \in \mathcal{T}_{\epsilon_1}^n(XY_{\mathcal{A}})$, which is upper bounded by

$$\begin{aligned} & \mathbb{E}_{C_n}\Bigg[\sum_{x^n, y_{\mathcal{A}}^n} p_{X^n Y_{\mathcal{A}}^n}(x^n, y_{\mathcal{A}}^n) \mathbb{1}\{\forall(\omega,\nu), (v^n(\omega,\nu), x^n) \\ & \qquad \notin \mathcal{T}_\epsilon^n(VX) \text{ and } (x^n, y_{\mathcal{A}}^n) \in \mathcal{T}_{\epsilon_1}^n(XY_{\mathcal{A}})\}\Bigg] \\ & = \sum_{(x^n, y_{\mathcal{A}}^n) \in T_{\epsilon_1}^n(XY_{\mathcal{A}})} p_{X^n Y_{\mathcal{A}}^n}(x^n, y_{\mathcal{A}}^n) \mathbb{P}[\forall(\omega,\nu), \\ & \qquad (V^n(\omega,\nu), x^n) \notin \mathcal{T}_\epsilon^n(VX)] \\ & = \sum_{(x^n, y_{\mathcal{A}}^n) \in T_{\epsilon_1}^n(XY_{\mathcal{A}})} p_{X^n Y_{\mathcal{A}}^n}(x^n, y_{\mathcal{A}}^n)(1 \\ & \qquad - \mathbb{P}[(V^n(\omega,\nu), x^n) \in \mathcal{T}_\epsilon^n(VX)])^{2^{n(R_v + R_v')}} \\ & \overset{(a)}{\leq} \sum_{(x^n, y_{\mathcal{A}}^n) \in T_{\epsilon_1}^n(XY_{\mathcal{A}})} p_{X^n Y_{\mathcal{A}}^n}(x^n, y_{\mathcal{A}}^n) \exp(-2^{n(R_v + R_v')} \\ & \qquad \times \mathbb{P}[(V^n(\omega,\nu), x^n) \in \mathcal{T}_\epsilon^n(VX)]) \\ & \overset{(b)}{\leq} \sum_{(x^n, y_{\mathcal{A}}^n) \in T_{\epsilon_1}^n(XY_{\mathcal{A}})} p_{X^n Y_{\mathcal{A}}^n}(x^n, y_{\mathcal{A}}^n) \exp\Big(-2^{n(R_v + R_v')} \\ & \qquad \times \Big(1 - \delta_{\epsilon_1,\epsilon}^{(2)}(n)\Big) 2^{-n(I(V;X) + 2\epsilon H(V))}\Big) \\ & \leq \exp\Big(-\Big(1 - \delta_{\epsilon_1,\epsilon}^{(2)}(n)\Big) 2^{\epsilon n H(V)}\Big), \end{aligned}$$

where (a) holds because for any $x \geq 0$ and any $p \in [0,1]$, $(1-p)^x \leq e^{-px}$, and in (b) we have defined $\delta_{\epsilon_1,\epsilon}^{(2)}(n) \triangleq 2|\mathcal{V}||\mathcal{X}| \exp\left(-n\frac{(\epsilon-\epsilon_1)^2}{1+\epsilon_1}\mu_{VX}\right)$.

3) The probability that the decoder finds $\tilde{\nu}_{\mathcal{A}} \neq \nu$ such that $(y_{\mathcal{A}}^n, v^n(\omega, \tilde{\nu}_{\mathcal{A}})) \in \mathcal{T}_\epsilon^n(Y_{\mathcal{A}}V)$, given that $(x^n, y_{\mathcal{A}}^n) \in \mathcal{T}_{\epsilon_1}^n(XY_{\mathcal{A}})$ and the encoder found (ω, ν) such that $(x^n, v^n(\omega,\nu)) \in \mathcal{T}_\epsilon^n(XV)$, which is upper bounded by

$$\begin{aligned} & \sum_{\omega,\nu} p(\omega,\nu) \sum_{\nu'_{\mathcal{A}} \neq \nu} \mathbb{E}_{C_n} \sum_{(x^n, y_{\mathcal{A}}^n) \in T_{\epsilon_1}^n(XY_{\mathcal{A}})} p_{X^n Y_{\mathcal{A}}^n}(x^n, y_{\mathcal{A}}^n) \\ & \qquad \times \mathbb{1}\{y_{\mathcal{A}}^n, (v^n(\omega,\nu'_{\mathcal{A}})) \in \mathcal{T}_\epsilon^n(Y_{\mathcal{A}}V)\} \\ & = \sum_{\omega,\nu} p(\omega,\nu) \sum_{\nu'_{\mathcal{A}} \neq \nu} \sum_{(x^n, y_{\mathcal{A}}^n) \in T_{\epsilon_1}^n(XY_{\mathcal{A}})} p_{X^n Y_{\mathcal{A}}^n}(x^n, y_{\mathcal{A}}^n) \\ & \qquad \times \mathbb{P}[(y_{\mathcal{A}}^n, (V^n(\omega,\nu'_{\mathcal{A}})) \in \mathcal{T}_\epsilon^n(Y_{\mathcal{A}}V)] \\ & \leq \sum_{\omega,\nu} p(\omega,\nu) \sum_{\nu'_{\mathcal{A}} \neq \nu} \sum_{(x^n, y_{\mathcal{A}}^n) \in T_{\epsilon_1}^n(XY_{\mathcal{A}})} p_{X^n Y_{\mathcal{A}}^n}(x^n, y_{\mathcal{A}}^n) \\ & \qquad \times 2^{-n(I(V;Y_{\mathcal{A}}) - 2\epsilon H(V))} \\ & \leq 2^{n(R_v' - I(V;Y_{\mathcal{A}}) + 2\epsilon H(V))} \\ & \leq 2^{-n\epsilon H(V)}. \end{aligned}$$

4) The probability that the decoder cannot find $\tilde{\nu}_{\mathcal{A}}$ such that $(y_{\mathcal{A}}^n, v^n(\omega, \tilde{\nu}_{\mathcal{A}})) \in \mathcal{T}_\epsilon^n(Y_{\mathcal{A}}V)$, given that $(x^n, y_{\mathcal{A}}^n) \in \mathcal{T}_{\epsilon_1}^n(XY_{\mathcal{A}})$ and the encoder found (ω, ν) such that $(x^n, v^n(\omega,\nu)) \in \mathcal{T}_\epsilon^n(XV)$, which is upper bounded with Markov lemma [31, Page 319 Equation (5.1)] by $2|\mathcal{V}||\mathcal{X}||\mathcal{Y}_{\mathcal{A}}| \exp\left(-n\frac{(\epsilon-\epsilon_1)^2}{1+\epsilon_1}\mu_{VXY_{\mathcal{A}}}\right)$.

Hence, for any $\mathcal{A} \in \mathbb{A}$, we have $\mathbb{E}_{C_n}[\mathbb{P}[V^n \neq \widehat{V}_{\mathcal{A}}^n]] \leq \delta(n, \epsilon, \mathcal{A})$. Next, we have

$$\begin{aligned} \mathbb{E}_{C_n}\left[\max_{\mathcal{A} \in \mathbb{A}} \mathbb{P}[\widehat{V}_{\mathcal{A}}^n \neq V^n]\right] & \leq \mathbb{E}_{C_n}\left[\sum_{\mathcal{A} \in \mathbb{A}} \mathbb{P}[\widehat{V}_{\mathcal{A}}^n \neq V^n]\right] \\ & = \sum_{\mathcal{A} \in \mathbb{A}} \mathbb{E}_{C_n}\left[\mathbb{P}[\widehat{V}_{\mathcal{A}}^n \neq V^n]\right] \\ & \leq \sum_{\mathcal{A} \in \mathbb{A}} \delta(n, \epsilon, \mathcal{A}) \\ & \leq |\mathbb{A}| \max_{\mathcal{A} \in \mathbb{A}} \delta(n, \epsilon, \mathcal{A}). \end{aligned}$$

By Markov's inequality, we conclude that there exists a codebook such that $\max_{\mathcal{A} \in \mathbb{A}} \mathbb{P}[\widehat{V}_{\mathcal{A}}^n \neq V^n] \leq |\mathbb{A}| \max_{\mathcal{A} \in \mathbb{A}} \delta(n, \epsilon, \mathcal{A})$.

Appendix D
Proof of (17)

For any $\mathcal{U} \in \mathbb{U}$, we have

$$\begin{aligned} H(V^n|Y_{\mathcal{U}}^n) & \overset{(a)}{\geq} I(X^n; V^n|Y_{\mathcal{U}}^n) \\ & = H(X^n|Y_{\mathcal{U}}^n) - H(X^n|V^n Y_{\mathcal{U}}^n) \\ & \overset{(b)}{=} nH(X|Y_{\mathcal{U}}) - H(X^n|V^n Y_{\mathcal{U}}^n), \end{aligned} \tag{34}$$

where (a) holds by definition of mutual information, and (b) holds because the X_i's and $(Y_{\mathcal{U}})_i$'s are independently and identically distributed. We now lower bound the term $-H(X^n|V^nY_{\mathcal{U}}^n)$. Define for any $\mathcal{U} \in \mathbb{U}$,

$$\Gamma_{\mathcal{U}} \triangleq \mathbb{1}\{(X^n, V^n, Y_{\mathcal{U}}^n) \in \mathcal{T}_{2\epsilon}^n(XVY_{\mathcal{U}})\},$$
$$\Delta_{\mathcal{U}} \triangleq \mathbb{1}\{(X^n, V^n) \in \mathcal{T}_{\epsilon}^n(XV)\},$$

so that,

$$\begin{aligned}
&H(X^n|V^nY_{\mathcal{U}}^n)\\
&\le H(X^n\Gamma_{\mathcal{U}}\Delta_{\mathcal{U}}|V^nY_{\mathcal{U}}^n)\\
&= H(\Gamma_{\mathcal{U}}\Delta_{\mathcal{U}}|V^nY_{\mathcal{U}}^n) + H(X^n|V^nY_{\mathcal{U}}^n\Gamma_{\mathcal{U}}\Delta_{\mathcal{U}})\\
&\overset{(a)}{\le} 2 + \sum_{\delta_{\mathcal{U}},\gamma_{\mathcal{U}}\in\{0,1\}} \mathbb{P}(\Gamma_{\mathcal{U}} = \gamma_{\mathcal{U}}|\Delta_{\mathcal{U}} = \delta_{\mathcal{U}})\mathbb{P}(\Delta_{\mathcal{U}} = \delta_{\mathcal{U}})\\
&\qquad \times H(X^n|V^nY_{\mathcal{U}}^n, \Gamma_{\mathcal{U}} = \gamma_{\mathcal{U}}, \Delta_{\mathcal{U}} = \delta_{\mathcal{U}})\\
&\overset{(b)}{\le} 2 + H(X^n|V^nY_{\mathcal{U}}^n, \Gamma_{\mathcal{U}} = 1, \Delta_{\mathcal{U}} = 1)\\
&\qquad + (2\delta_\epsilon(n) + \delta_\epsilon^2(n,\mathcal{U}))\log|\mathcal{X}|^n\\
&= \sum_{y_{\mathcal{U}}^n, v^n} p(y_{\mathcal{U}}^n, v^n|1,1)\\
&\qquad \times H(X^n|Y_{\mathcal{U}}^n = y_{\mathcal{U}}^n, V^n = v^n, \Gamma_{\mathcal{U}} = 1, \Delta_{\mathcal{U}} = 1)\\
&\qquad + 2 + (2\delta_\epsilon(n) + \delta_\epsilon^2(n,\mathcal{U}))\log|\mathcal{X}|^n\\
&\overset{(c)}{\le} \sum_{y_{\mathcal{U}}^n, v^n} p(y_{\mathcal{U}}^n, v^n|1,1)\log|T_{2\epsilon}^n(X|y_{\mathcal{U}}^n, v^n)|\\
&\qquad + 2 + (2\delta_\epsilon(n) + \delta_\epsilon^2(n,\mathcal{U}))\log|\mathcal{X}|^n\\
&\le \sum_{y_{\mathcal{U}}^n, v^n} p(y_{\mathcal{U}}^n, v^n|1,1)nH(X|Y_{\mathcal{U}}V)(1+2\epsilon)\\
&\qquad + 2 + (2\delta_\epsilon(n) + \delta_\epsilon^2(n,\mathcal{U}))\log|\mathcal{X}|^n\\
&\le nH(X|Y_{\mathcal{U}}V)(1+2\epsilon) + 2 + (2\delta_\epsilon(n) + \delta_\epsilon^2(n,\mathcal{U}))\log|\mathcal{X}|^n.
\end{aligned} \tag{35}$$

where (a) holds because $(\Gamma_{\mathcal{U}}, \Delta_{\mathcal{U}})$ is defined over an alphabet of cardinality equal to four so that $H(\Gamma_{\mathcal{U}}\Delta_{\mathcal{U}}|V^nY_{\mathcal{U}}^n) \le \log 4 = 2$, (b) holds because $\mathbb{P}[\Delta_{\mathcal{U}} = 0] \le \delta_\epsilon(n) \triangleq 2|\mathcal{X}||\mathcal{V}|e^{-n\epsilon^2\mu_{XV}}$ and $\mathbb{P}[\Gamma_{\mathcal{U}} = 0|\Delta_{\mathcal{U}} = 1] \le \delta_\epsilon^2(n,\mathcal{U}) \triangleq 2|\mathcal{V}||\mathcal{X}||\mathcal{Y}_{\mathcal{U}}|e^{-\epsilon^2 n\mu_{VXY_{\mathcal{U}}}/8}$ by Markov Lemma [31, Page 319 Equation (5.1)], and (c) holds because $H(X) \le \log|\mathcal{X}|$ for any discrete random variable X defined over $|\mathcal{X}|$. Combining (34) and (35), we obtain (17).

Appendix E
Proof of (22) and (23)

We rewrite (26) and (27) as

$$R_p = \max_{\mathcal{A}\in\mathbb{A}} \left(h(X) - h(X|V) - h(Y_{\mathcal{A}}) + h(Y_{\mathcal{A}}|V)\right), \tag{36}$$
$$R_s = \min_{\mathcal{A}\in\mathbb{A}} \min_{\mathcal{U}\in\mathbb{U}} \left(h(Y_{\mathcal{A}}) - h(Y_{\mathcal{A}}|V) - h(Y_{\mathcal{U}}) + h(Y_{\mathcal{U}}|V)\right). \tag{37}$$

Let $K_{XV} \triangleq \begin{bmatrix} \sigma_X^2 & \sigma_{XV} \\ \sigma_{VX} & \sigma_V^2 \end{bmatrix}$ be the covariance matrix of (X, V). We have

$$\begin{aligned}
h(X|V) &= h(X,V) - h(V)\\
&= \frac{1}{2}\log(2\pi e)^2\det(K_{XV}) - \frac{1}{2}\log 2\pi e\sigma_V^2\\
&= \frac{1}{2}\log 2\pi e(\sigma_X^2 - \sigma_{XV}\sigma_V^{-2}\sigma_{XV})\\
&= \frac{1}{2}\log 2\pi e\sigma_{X|V}^2,
\end{aligned} \tag{38}$$

where the last equality holds by [41, Proposition 3.13]. Next, for any $\mathcal{A} \in \mathbb{A}$, let $K_{Y_{\mathcal{A}}V} \triangleq \begin{bmatrix} \Sigma_{Y_{\mathcal{A}}} & \Sigma_{Y_{\mathcal{A}}V} \\ \Sigma_{Y_{\mathcal{A}}V}^T & \sigma_V^2 \end{bmatrix}$ be the covariance matrix of $(Y_{\mathcal{A}}, V)$. We have

$$\begin{aligned}
h(Y_{\mathcal{A}}|V) &= \frac{1}{2}\log(2\pi e)^{|\mathcal{A}|}\frac{\det(K_{Y_{\mathcal{A}}V})}{\sigma_V^2}\\
&\overset{(a)}{=} \frac{1}{2}\log(2\pi e)^{|\mathcal{A}|}\frac{\sigma_V^2\det(\Sigma_{Y_{\mathcal{A}}} - \Sigma_{Y_{\mathcal{A}}V}\sigma_V^{-2}\Sigma_{Y_{\mathcal{A}}V}^T)}{\sigma_V^2}\\
&\overset{(b)}{=} \frac{1}{2}\log(2\pi e)^{|\mathcal{A}|}\det(\Sigma_{Y_{\mathcal{A}}|V}),\\
&\overset{(c)}{=} \frac{1}{2}\log(2\pi e)^{|\mathcal{A}|}\det(H_{\mathcal{A}}\sigma_{X|V}^2H_{\mathcal{A}}^T + I),
\end{aligned} \tag{39}$$

where (a) holds by the formula for the determinant of a block matrix, (b) holds by [41, Proposition 3.13], (c) holds by (4) and the definition of the conditional variance $\Sigma_{Y_{\mathcal{A}}|V} \triangleq \mathbb{E}\left[(Y_{\mathcal{A}} - \mathbb{E}[Y_{\mathcal{A}}|V])(Y_{\mathcal{A}} - \mathbb{E}[Y_{\mathcal{A}}|V])^T|V\right] = H_{\mathcal{A}}\mathbb{E}\left[(X - \mathbb{E}[X|V])(X - \mathbb{E}[X|V])^T|V\right]H_{\mathcal{A}}^T + \mathbb{E}\left[W_{Y_{\mathcal{A}}}W_{Y_{\mathcal{A}}}^T\right]$ and $W_{Y_{\mathcal{A}}}$ is a Gaussian noise vector with identity covariance matrix. Similarly, for any $\mathcal{U} \in \mathbb{U}$, we have

$$h(Y_{\mathcal{U}}|V) = \frac{1}{2}\log(2\pi e)^{|\mathcal{U}|}\det(H_{\mathcal{U}}\sigma_{X|V}^2H_{\mathcal{U}}^T + I). \tag{40}$$

Thus, from (36), (37), (38), (39), and (40), we have

$$R_p = \max_{\mathcal{A}\in\mathbb{A}}\left(\frac{1}{2}\log\frac{\sigma_X^2}{\sigma_{X|V}^2} - \frac{1}{2}\log\frac{\det(H_{\mathcal{A}}\sigma_X^2H_{\mathcal{A}}^T + I)}{\det(H_{\mathcal{A}}\sigma_{X|V}^2H_{\mathcal{A}}^T + I)}\right), \tag{41}$$

$$R_s = \min_{\mathcal{A}\in\mathbb{A}}\min_{\mathcal{U}\in\mathbb{U}}\left(\frac{1}{2}\log\frac{\det(H_{\mathcal{A}}\sigma_X^2H_{\mathcal{A}}^T + I)}{\det(H_{\mathcal{A}}\sigma_{X|V}^2H_{\mathcal{A}}^T + I)} - \frac{1}{2}\log\frac{\det(H_{\mathcal{U}}\sigma_X^2H_{\mathcal{U}}^T + I)}{\det(H_{\mathcal{U}}\sigma_{X|V}^2H_{\mathcal{U}}^T + I)}\right). \tag{42}$$

Then, by Lemma 1 and the definition of $O_{\mathcal{A}}$, $\mathcal{A} \in \mathbb{A}$ and $O_{\mathcal{U}}$, $\mathcal{U} \in \mathbb{U}$, we can rewrite (41) and (42) as

$$R_p = \max_{\mathcal{A}\in\mathbb{A}}\left(\frac{1}{2}\log\frac{\sigma_X^2}{\sigma_{X|V}^2} - \frac{1}{2}\log\frac{\sigma_X^2O_{\mathcal{A}} + 1}{\sigma_{X|V}^2O_{\mathcal{A}} + 1}\right), \tag{43}$$

$$R_s = \min_{\mathcal{A}\in\mathbb{A}}\min_{\mathcal{U}\in\mathbb{U}}\left(\frac{1}{2}\log\frac{\sigma_X^2O_{\mathcal{A}} + 1}{\sigma_{X|V}^2O_{\mathcal{A}} + 1} - \frac{1}{2}\log\frac{\sigma_X^2O_{\mathcal{U}} + 1}{\sigma_{X|V}^2O_{\mathcal{U}} + 1}\right). \tag{44}$$

Finally, by Lemma 2, (43) and (44) become (22) and (23).

References

[1] V. Rana, R. A. Chou, and H. Kwon, "Secret sharing from correlated Gaussian random variables and public communication," in *Proc. IEEE Inf. Theory Workshop*, Riva del Garda, Italy, Apr. 2021, pp. 1–5.

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

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

[4] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 6, pp. 644–654, Nov. 1976.

[5] S. Zou, Y. Liang, L. Lai, and S. Shamai (Shitz), "An information theoretic approach to secret sharing," *IEEE Trans. Inf. Theory*, vol. 61, no. 6, pp. 3121–3136, Apr. 2015.

[6] Y. Liang, G. Kramer, H. V. Poor, and S. Shamai (Shitz), "Compound wiretap channels," *EURASIP J. Wireless Commun. Netw.*, vol. 2009, no. 1, pp. 1–12, Oct. 2009.

[7] I. Csiszar and P. Narayan, "Capacity of a shared secret key," in *Proc. IEEE Int. Symp. Inf. Theory*, Jun. 2010, pp. 2593–2596.

[8] R. A. Chou, "Secret sharing over a public channel from correlated random variables," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Vail, CO, USA, Jun. 2018, pp. 991–995.

[9] R. A. Chou, "Distributed secret sharing over a public channel from correlated random variables," 2021, *arXiv:2110.10307*.

[10] N. Tavangaran, H. Boche, and R. F. Schaefer, "Secret-key generation using compound sources and one-way public communication," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 1, pp. 227–241, Jan. 2017.

[11] M. Bloch, "Channel intrinsic randomness," in *Proc. IEEE Int. Symp. Inf. Theory*, Austin, TX, USA, Jun. 2010, pp. 2607–2611.

[12] R. A. Chou, "Biometric systems with multiuser access structures," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Paris, France, Jul. 2019, pp. 807–811.

[13] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 240–254, Jun. 2010.

[14] A. J. Pierrot, R. A. Chou, and M. R. Bloch, "Experimental aspects of secret key generation in indoor wireless environments," in *Proc. IEEE 14th Workshop Signal Process. Adv. Wireless Commun.*, Jun. 2013, pp. 669–673.

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

[16] S. Vadhan, "Extracting all the randomness from a weakly random source," Electron. Colloq. Comput. Complex., Berlin, Germany, Tech. Rep. TR98–047, 1998.

[17] S. Watanabe and Y. Oohama, "Secret key agreement from vector Gaussian sources by rate limited public communication," *IEEE Trans. Inf. Forensics Security*, vol. 6, no. 3, pp. 541–550, Sep. 2011.

[18] S. Watanabe and Y. Oohama, "Secret key agreement from correlated Gaussian sources by rate limited public communication," *IEICE Trans. Fundam. Electron., Commun. Comput. Sci.*, vol. E93-A, no. 11, pp. 1–8, Nov. 2010.

[19] A. Beimel, "Secret-sharing schemes: A survey," in *Proc. Int. Conf. Coding Cryptol.*, Qingdao, China, May/Jun. 2011, pp. 11–46.

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

[21] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.

[22] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. I. Secret sharing," *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.

[23] C. Pozrikidis, *An Introduction to Grids, Graphs, and Networks*. New York, NY, USA: Oxford Univ. Press, 2014.

[24] I. Csiszár and P. Narayan, "Common randomness and secret key generation with a helper," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 344–366, Mar. 2000.

[25] R. A. Chou, M. R. Bloch, and E. Abbe, "Polar coding for secret-key generation," *IEEE Trans. Inf. Theory*, vol. 61, no. 11, pp. 6213–6237, Nov. 2015.

[26] T. Ignatenko and F. M. J. Willems, *Biometric Security From Information-Theoretical Perspective*. Hanover, MA, USA: Now, 2012.

[27] T. Ignatenko and F. Willems, "Privacy leakage in binary biometric systems: From Gaussian to binary data," in *Security and Privacy in Biometrics*. London, U.K.: Springer, 2013, pp. 105–122.

[28] O. Günlü, "Multi-entity and multi-enrollment key agreement with correlated noise," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1190–1202, 2021.

[29] O. Günlü, O. Iscan, V. Sidorenko, and G. Kramer, "Code constructions for physical unclonable functions and biometric secrecy systems," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 11, pp. 2848–2858, Nov. 2019.

[30] A. Orlitsky and J. R. Roche, "Coding for computing," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 903–917, Mar. 2001.

[31] G. Kramer, "Topics in multi-user information theory," *Found. Trends Commun. Inf. Theory*, vol. 4, nos. 4–5, pp. 265–444, 2007.

[32] U. Maurer and S. Wolf, *Information-Theoretic Key Agreement: From Weak to Strong Secrecy for Free*. Berlin, Germany: Springer-Verlag, 2000, pp. 351–368.

[33] R. A. Chou and M. R. Bloch, "Separation of reliability and secrecy in rate-limited secret-key generation," *IEEE Trans. Inf. Theory*, vol. 60, no. 8, pp. 4941–4957, Aug. 2014.

[34] T. Cover and J. Thomas, *Elements of Information Theory*, 2nd ed. Hoboken, NJ, USA: Wiley, 2006.

[35] M. Pinsker, *Information and Information Stability of Random Variables and Processes*. San Francisco, CA, USA: Holden-Day, 1964.

[36] R. Fano, *Transmission of Information: A Statistical Theory of Communications*. Cambridge, MA, USA: MIT Press, 1961.

[37] R. A. Chou, "Unified framework for polynomial-time wiretap channel codes," 2020, *arXiv:2002.01924*.

[38] R. A. Chou, "Explicit codes for the wiretap channel with uncertainty on the eavesdropper's channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2018, pp. 476–480.

[39] R. Sultana and R. A. Chou, "Low-complexity secret sharing schemes using correlated random variables and rate-limited public communication," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jul. 2021, pp. 970–975.

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

[41] M. Eaton, *Multivariate Statistics: A Vector Space Approach*. Hoboken, NJ, USA: Wiley, 1983.

Vidhi Rana (Graduate Student Member, IEEE) received the B.Tech. degree in electronics and telecommunication from the College of Engineering, Roorkee, India, and the M.Tech. degree in digital signal processing from the Govind Ballabh Pant Engineering College, Pauri, India. She is currently pursuing the Ph.D. degree with Wichita State University, Wichita, KS, USA.

Rémi A. Chou (Member, IEEE) received the degree in engineering from Supélec, Gif-sur-Yvette, France, in 2011, and the Ph.D. degree in electrical engineering from the Georgia Institute of Technology, Atlanta, GA, USA, in 2015. From 2015 to 2017, he was a Post-Doctoral Scholar with Pennsylvania State University, University Park, PA, USA. He is currently an Assistant Professor with the Department of Electrical Engineering and Computer Science, Wichita State University, Wichita, KS, USA.

Hyuck M. Kwon (Life Senior Member, IEEE) was born in South Korea, in May 1953. He received the B.S. and M.S. degrees in electrical engineering from Seoul National University, Seoul, South Korea, in 1978 and 1980, respectively, and the Ph.D. degree in computer, information, and control engineering from the University of Michigan, Ann Arbor, MI, USA, in 1984. From 1985 to 1989, he was an Assistant Professor with the Department of Electrical Engineering and Computer Science, University of Wisconsin–Milwaukee, Milwaukee, WI, USA. From 1989 to 1993, he was the Principal Engineer with Lockheed Engineering and Sciences Company, Houston, TX, USA, working on the National Aeronautics and Space Administration space shuttle and space station satellite communication systems. Since 1993, he has been with the Department of Electrical Engineering and Computer Science, Wichita State University, Wichita, KS, USA, where he is currently a Full Professor. His current research interests include wireless, massive multiple-input-multiple-output, millimeter-wave, orthogonal frequency-division multiple-access, cooperative, code-division multiple-access, frequency-hopping spread-spectrum, and satellite communication systems.